АПИНО
ICAIT

11TH INTERNATIONAL CONFERENCE
ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2022

XI МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ
И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ»

2022

СБОРНИК НАУЧНЫХ СТАТЕЙ

APINO.SPBGUT.RU

СПбГУТ)))

ИНФОРМАЦИОННЫЕ ПАРТНЁРЫ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ
ИНФОРМАЦИЯ
КОСМОС

НАУЧНЫЙ ЖУРНАЛ
ТУЗС
«ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ»

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

www.iit.sut.ru
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
научное рецензируемое издание • электронный научный журнал
Telecom IT — ISSN 2307-1303

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. А. В. Шестакова; сост. В. С. Елагин, Е. А. Аникевич. СПб. : СПбГУТ, 2022. Т. 2. 759 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.09.2022.
Вышло в свет 30.09.2022. Формат 60×90 1/8.
Уст. печ. л. 47,44. Заказ № 087-ИТТ-2022.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-266-3

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.912+ 004.932.4
ГРНТИ 20.19.29

ОБЗОР ПОДХОДОВ К МАРКИРОВАНИЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ОСНОВАННЫХ НА СДВИГЕ СЛОВ

М. А. Аверенкова, С. А. Копылов

Академия Федеральной службы охраны Российской Федерации

Развитие информационно-телекоммуникационных сетей позволило перейти к активному внедрению систем электронного документооборота во все сферы взаимодействия. Наличие недостатков и уязвимостей средств защиты указанных систем не позволяет обеспечить требуемый уровень защищенности от утечки текстовых документов. Для повышения защищенности текстовых документов необходимо совершенствовать существующие средства маркирования информации. В статье представлен анализ методов маркирования текстовых документов, основанных на стеганографическом внедрении информации за счет сдвига слов. В процессе анализа приведено описание подходов к маркированию, основанных на горизонтальном сдвиге, осуществлена количественная оценка основных параметров существующих исследований в области маркирования, определены их достоинства и недостатки. Обоснована возможность использования методов стеганографического внедрения информации для повышения защищенности текстовых документов. Определены направления дальнейших исследований.

маркирование, текстовая стеганография, текстовые электронные документы.

Возросшее число инцидентов информационной безопасности, связанных с утечкой текстовых документов из систем электронного документооборота, в значительной степени снижает безопасности таких систем со стороны рядовых пользователей. Для защиты текстовых документов, содержащих конфиденциальную информацию, а также персональные данные пользователей, от утечки используются DLP-системы (*Data Loss/Leak*

Prevention/Protection), основанные на контентном анализе содержимого информации, распространяемой и хранящейся в пределах контролируемого периметра защищаемой сети.

В процессе контентного анализа осуществляется извлечение уникальных характеристик, позволяющих идентифицировать данные или встроенную в них информацию. Уникальная характеристика может представлять собой неповторяемый, для разных файлов одного типа данных, набор свойств и признаков или встроенную сигнатуру (информационную последовательность). При этом среди уникальных характеристик наибольшее распространение получили методы, основанные на скрытом внедрении сигнатуры в исходный текст.

Методы скрытого (стеганографического) внедрения информации в текстовые документы можно разделить на следующие группы [1]:

– лингвистические;

– технические.

Лингвистические методы текстовой стеганографии для встраивания информации используют языковые свойства и структуру текста, сочетая в себе синтаксические, пунктуационные добавления (добавление знаков пунктуации в строго определенные места в тексте) и семантические методы (замена определенных слов в тексте на синонимы, использование кодовых таблиц, словарей сокращений и аббревиатур) [2–5].

К техническим методам относятся методы, осуществляющие форматирование текста и текстового пространства, а именно: пространства интервалов и отступов, внесение дополнительных пробелов и кодирование признаков (замена начертания символов). К техническим методам стетеганографического внедрения информации в текстовые документы относятся подходы, основанные на изменении положения слов, которые реализуют кодирование информации посредством горизонтального сдвига слова (влево или вправо на определенное расстояние) либо увеличения (уменьшения) интервала, как между словами, так и между символами внутри слова [6].

Пример изменения положения слова представлен на рис. 1а, изменения интервала между слова – рис. 1б.

а *б*

Рис. 1. Изменение положения слова:
а) сдвиг слова вправо; б) изменения интервала между словами

Для оценки применимости представленных подходов к внедрению информации на практике проведен сравнительный анализ существующих исследований в области маркирования текстовых документов, основанных на горизонтальном сдвиге слова. В качестве анализируемых исследований выступают работы Ло, Брассила и Максемчука [7–9], Хуанга [10], Кима [11], Алаттара [12] и Пандея [13].

В работах Ло, Максемчука и Брассила [7–9] маркирование текстовых документов основано на горизонтальном смещении влево или вправо среднего (центрального) блока, состоящего из нескольких слов, внутри строки текстового документа.

Предельно достижимая емкость встраивания указанного подхода зависит от используемых значений кегля шрифта и величины межстрочного интервала и ограничена значением в 63 бита (текст формата А4 с кеглем шрифта 10 пт и величиной межстрочного интервала 1).

Минимальная величина сдвига блока слов текстовой строки ограничена величиной в 2 пикселя текста, выводимого на печать с разрешением 300 точек на дюйм. В ходе оценки точности извлечения встроенной информации получены следующие значения: 76 % для текста, набранного кеглем шрифта 8 пт, и 94 % для текста с кеглем шрифта 12 пт.

Подход к маркированию текстовых документов, предложенный Хуангом в [10] основан на использовании свободного пространства (пространства пробелов) между словами. Кодирование информации реализуется посредством преобразования пустого текстового пространства, характеризующегося средним расстоянием между словами в строке, в вид синусоидальной формы.

Емкость встраивания рассмотренного подхода к маркированию характеризуется наличием произвольной длины водяного знака и значением предельно достижимой емкости встраивания для текста, набранного кеглем размером 11 пт (52 строки), составляет 42 бита, зависит от формы и параметров синусоидальной волны.

Результат извлечения характеризуется наличием одиночных ошибок извлечения. Из встроенных в текстовые данные 68 бит информации правильно извлечены 64 бита (≈ 94 %).

Маркирование электронных документов, предложенное Кимом в [11], основано на статистике распределения величин интервалов между словами и разработанном подходе классификации слов. В процессе маркирования осуществляется формирование классов слов по определенным признакам, а также группирование слов в сегменты с последующей классификацией сегментов на основе сформированных классов.

В ходе экспериментальной оценки емкости встраивания получены количественные оценки предельно достижимой емкости встраивания, равные 64 бита информации для двух классовой схемы и 128 бит – для четырех

классовой. Невидимость встроенной информации достигается за счет выбора величины горизонтального смешения слова на значение, не превышающее 3 пикселя (минимальное значение – 1 пиксель).

В работе Алаттара [12] маркирование текстовых документов основано на изменении величины интервала между словами за счет расширения (сжатия) пустого пространства после каждого слова в строке на установленную величину в зависимости от символа кодовой последовательности.

Емкость встраивания зависит от количества текстовой информации, а также от параметров помехоустойчивого кода и кода расширенного спектра. Предельно достижимая емкость встраивания для текста, набранного гарнитурой Times New Roman с кеглем 11 пт, двойным межстрочным интервалом на листе формата Letter, составляет 300 бит. При этом в ходе экспериментальной оценки предложенного алгоритма используемая длина внедряемой последовательности (маркера) составляет 32 бита, из которой только 8 бит, приходится на встраиваемую информацию.

В ходе оценки извлекаемости встроенных данных произведено извлечение встроенной информации из неподписанного текстового документа. Точность извлечения составляет 98,8 %, что свидетельствует о наличии одиночных ошибок в процессе извлечения. Количественная оценка точности извлечения из подписанных электронных и напечатанных на бумаге текстовых документов не представлена. Перцептивная невидимость встроенных данных основана на оценках, приведенных в работах [7–9]. Полученные результаты позволяют отнести разработанный алгоритм маркирования текстовых данных к перцептивным.

В работе Пандея [13] предложен альтернативный подход к маркированию текстовых электронных документов за счет изменения величин интервалов между словами, основанный на содержимом текстового документа и статистике появления слов (символов) в английских текстах.

Экспериментальная оценка емкости встраивания, извлекаемости (точности извлечения) и невидимости разработанного алгоритма маркирования не проводилась.

Результаты сравнительной оценки параметров встраивания и извлечения рассмотренных подходов приведены в таблице 1.

ТАБЛИЦА 1. Основные параметры встраивания и извлечения встроенных данных подходов маркирования

Параметр	Исследование				
	Ло, Брассил [7–9]	Хуанг [10]	Ким [11]	Алаттар [12]	Пандей [13]
Границы перцептивной невидимости	1…2 пикселя	0,1…0,2 амплитуды волны	1…3 пикселя	1…2 пикселя	0,34…0,94 пикселя

Параметр	Исследование				
	Ло, Брассил [7–9]	Хуанг [10]	Ким [11]	Алаттар [12]	Пандей [13]
Емкость встраивания (бит)	63	42	128	300	Данные отсутствуют
Точность извлечения (%)	≥ 94 (скан) ≤ 76 (фото)	≥ 94 (скан)	Данные отсутствуют		
Наличие исходного документа	+	–	–	–	Данные отсутствуют

Полученные результаты проведенного анализа позволяют сделать вывод о наличии небольшой емкости встраивания подходов [8–13], приходящейся на страницу текстового документа, что, в свою очередь не позволяет встраивать достаточно большую сигнатуру. При этом подход, предложенный Алаттаром, лишен указанного недостатка, однако авторами не представлена количественная оценка показателей точности извлечения.

Исходя из полученных результатов, можно сделать вывод о возможности применения методов стеганографического внедрения информации, основанных на сдвиге слова, в текстовые документы для защиты от утечки. В то же время наличие описанных ограничений делает задачу по разработке методов внедрения информации в текстовые документы актуальным направлением исследований. Решению данной задачи посвящены дальнейшие исследования.

Список используемых источников

1. Ahvanooey M. T., Li Q, Shim H. J., Huang Y. A Comparative Analysis of Information Hiding Techniques for Copyright Protection of Text Documents // Security and Communication Networks. Vol 2018, pp 1-22.

2. Shirali-Shahreza M., Shirali-Shahreza M. H. Text steganography in SMS // International Conference on Convergence Information Technology. 2005. pp. 64–74.

3. Бондарчук С. С., Давыдова Е. М., Костюченко Е. Ю. Встраивание цифровых знаков для обеспечения защиты информации // Доклады ТУСУР. 2011. Т. 24, № 2. С. 228–235.

4. Govada S. R. Text steganography with multi level shielding // International Journal of Computer Science Issues. 2012. Vol. 9, no. 5. pp. 401–405.

5. Nagarhalli T. P., J. Bakal W., Jain N. A Survey of Hindi Text Steganography // International Journal of Scientific & Engineering Research. 2016. Vol. 7, no. 3. pp. 55–61.

6. Por L. Y., Delina B. Information hiding: A new approach in text steganography // WSEAS International Conference. Proceedings. Mathematics and Computers ib Science and Engineering. World Scientific, Engineering Academy, Society. 2008. pp. 689–695.

7. Brassil J. T. Electronic marking and identification techniques to discourage document copying // Journal on Selected Areas in Communications. 1995. Vol. 13. pp. 1495–1504.

8. Low S. H. Document Marking and Identification using Both Line and Word Shifting // Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003). 1995. Vol. 2. pp. 853–860.

9. Brassil J. T., Maxemchuk N. F., Low S. H. Copyright protection for the electronic distribution of text documents // Proceedings of the IEEE. 1999. Vol. 87. pp. 1181–1196.

10. Huang D., Yan H. Interword distance changes represented by sine waves for watermarking text images // IEEE Transactions on Circuits and Systems for Video Technology. 2001. Vol. 11, no. 12. pp. 1237–1245.

11. Kim Y.-W., Kim K.-A., Moon I.-S. A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics // Proceedings of the Seventh International Conference on Document Analysis and Recognition. 2003. pp. 75–779.

12. Alattar A. M., Alattar O. M Watermarking electronic text documents containing justified paragraphs and irregular line spacing // Security, Steganography, and Watermarking of Multimedia Contents VI. Vol. 5306. International Society for Optics, Photonics. 2004. pp. 685–696.

13. Pandey N., Nandy S., Choudhury S. S. Alternative Shift Algorithm for Digital Watermarking on Text // International Journal of Scientific and Research Publications. 2012. Vol. 2, no. 10. pp. 1–5.

УДК 004.852
ГРНТИ 50.43.19

ПРОГНОЗИРОВАНИЕ ПАРАМЕТРОВ СОСТОЯНИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

В. С. Авраменко, С. Д. Канчалан, А. А. Ковалев

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В статье предлагается подход к реализации функции автоматического прогнозирования отказов (сбоев) средств вычислительной техники на основе рекуррентных нейронных сетей долгой краткосрочной памяти. В результате работы системы искусственных нейронных сетей формируются прогнозные значения параметров технического состояния отдельных элементов системы, далее определяется степень их соответствия допустимым значениям.

нейросети, прогнозирование, отказ.

В настоящее время к автоматизированным системам предъявляются высокие требования по устойчивости, в том числе и по надежности [1, 2]. Соответственно, возрастает роль контроля технического состояния средств вычислительной техники. Вместе с тем существующие системы контроля

(мониторинга) технического состояния не удовлетворяют современным требованиям по оперативности обнаружения и диагностирования отказов (сбоев) средств вычислительной техники [3].

Одним из путей решения данной проблемы является реализация функции автоматического прогнозирования отказов (сбоев), позволяющей администратору в близком к реальному масштабу времени получить данные о возможном отказе (сбое) на прогнозируемом периоде, а также разработать варианты мероприятий (рекомендации) по их устранению.

Функция прогнозирования может быть реализована на основе подхода, предполагающего использование искусственных нейронных сетей (далее ИНС) [4,5].

Для прогнозирования значений параметров технических и программных средств автоматизации целесообразно использовать рекуррентные нейронные сети (РНС) долгой краткосрочной памяти (LSTM (Long short-term memory)) [6].

В качестве прогнозируемых параметров могут использоваться следующие: температура элементов ЭВМ (центрального процессора, жесткого диска и др.), средняя загруженность оперативной памяти, жесткого диска, процессора и другие.

Для прогнозирования параметров технического состояния средств вычислительной техники строится отдельная LSTM сеть для каждого из этих параметров.

Пример структуры сети для одного параметра состояния *x* представлена на рис. 1.

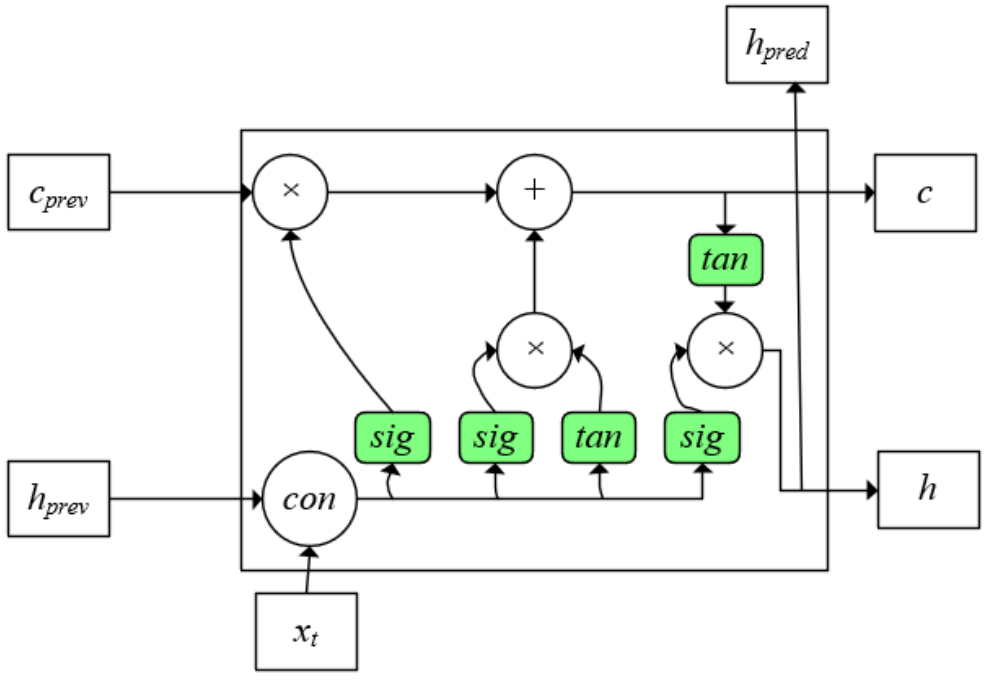


Рис. 1. Структура LSTM сети для одного параметра

На рис. 1:

x_t – последовательность значений температуры процессора;

h_{prev} – результат, получившийся на выходе предыдущей ячейки;

h_{pred} – результат прогноза для следующей ячейки;

h – результат прогноза;

c_{prev} – дополнительный выход предыдущей ячейки;

con – конкатенация;

sig, t*an* – функции активации, сигмоида и тангенсоида соответственно.

Для прогнозирования температуры процессора была создана НС из 64 слоев. Для обучения НС использовался набор данных о температуре процессора, собранных в течение типового сеанса работы пользователя.

Обучающие данные предварительно нормализуются в соответствии с формулой:

$$X_{nnorm} = \frac{X_n - X_{mid}}{\sigma},$$

где $x_{n\ norm}$ – нормированное значение, x_n – элемент выборки, x_{mid} – среднее значение, σ – стандартное отклонение.

На выходе сеть формирует прогнозное значение параметра с заданным прогнозным периодом. Процесс обучения включал 10 эпох.

Решение о техническом состоянии процессора определяется в соответствии с критерием следующего вида:

$$Y_{\text{цп}} = \begin{cases} 1, если\, T_{\text{цп}} \geq T_{\text{цп кр.}} \\ 0, если\, T_{\text{цп}} < T_{\text{цп кр.}} \end{cases},$$

где $Y_{\text{цп}}$ – признак состояния центрального процессора, $T_{\text{цп}}$ – текущая температура центрального процессора, $T_{\text{цп.кр}}$ – критическая температура центрального процессора.

Для сравнительной оценки точности прогноза, помимо прогноза РНС, был осуществлен прогноз температуры процессора методом скользящего среднего. По результатам прогнозирования на период 5 минут метод РНС показал точность на 28 % выше, чем метод скользящего среднего.

Для определения ТС СВТ в целом также может использоваться РНС, при этом на вход нейросети подаются значения нескольких параметров (температура, загруженность ОП и т.д.). Например, при использовании трех параметров состояния структура НС иметь вид, представленный на рис. 2.

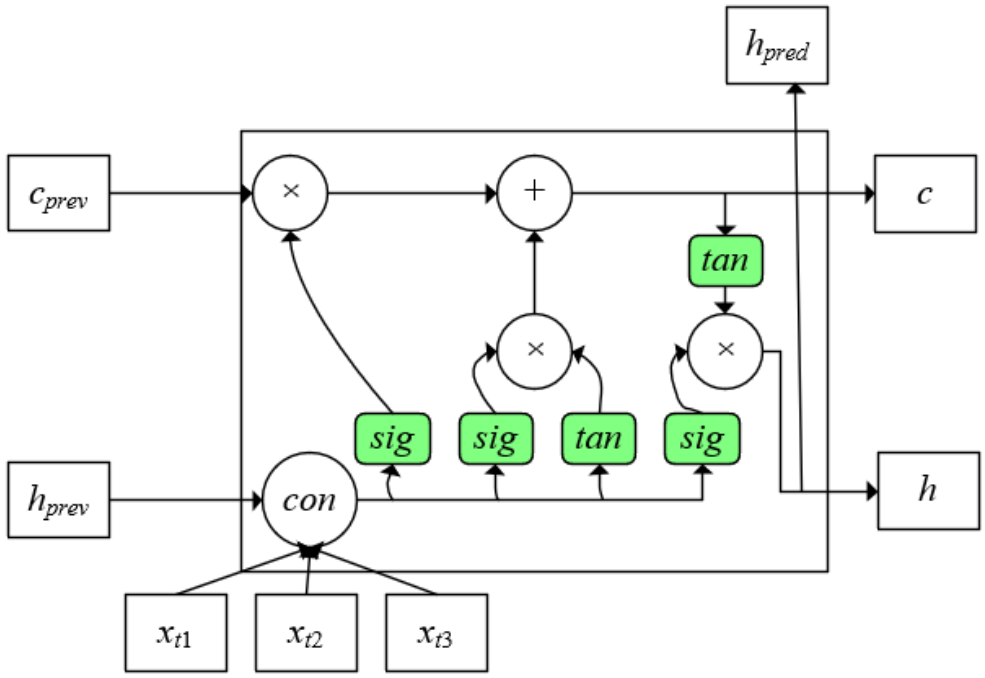


Рис. 2. Структура LSTM сети для 3 параметров

На рис. 2:

x_{t1} – последовательность значений температуры, используемая для обучения;

x_{t2} – последовательность значений текущего состояния СВТ, используемая для обучения;

x_{t3} – последовательность значений загруженности оперативной памяти, используемая для обучения;

h_{prev} – результат, получившийся на выходе предыдущей ячейки;

h_{pred} – результат прогноза для следующей ячейки;

h – результат прогноза;

c_{prev} – дополнительный выход предыдущей ячейки;

con – конкатенация;

sig, t*an* – функции активации, сигмоида и тангенсоида соответственно.

Систему прогнозирования параметров состояния отдельных элементов СВТ и СВТ в целом целесообразно включить в систему мониторинга технических средств связи и автоматизации в качестве подсистемы. В качестве средства сбора данных может использоваться Zabbix – бесплатное программное обеспечение для мониторинга параметров состояния компьютерной сети. Эта система работает на основе триггеров, сигнализирующих о текущем состоянии технических средств.

В результате проведенных экспериментов можно сделать вывод о том, что метод прогнозирования с помощью РНС является достаточно точным для реализации функции автоматического прогнозирования отказов и сбоев средств вычислительной техники.

Таким образом, функция прогнозирования технического состояния элементов СВТ обеспечит администраторам возможность упреждения отказов и сбоев СВТ, позволит своевременно принять меры по обеспечению непрерывности процесса функционирования, целостности хранящейся и обрабатываемой информации, восстановлению СВТ.

Список используемых источников

1. Паращук И. Б., Крюкова Е. С., Михайлеченко А. В. Анализ надежности центров обработки данных и электронных библиотек // VI Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Сборник трудов. Санкт-Петербург, 2021. С. 146–150.

2. Паращук И. Б., Крюкова Е.С., Михайлеченко А. В. Анализ зашумленных и неоднородных данных о значениях параметров надежности дата центров // VI Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Сборник трудов. Санкт-Петербург, 2021. С. 164–172.

3. Ковалев А. А., Авраменко В. С., Иванов Р. М. Анализ проблемы автоматизированного контроля технического состояния комплексов средств автоматизации специального назначения // VI Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Сборник трудов. Выпуск 1. СПб.: ВАС, 2021. С. 55–59.

4. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб.: Питер, 2018. 480 с.

5. Тихонов Э. Е. Методы прогнозирования в условиях рынка: учебное пособие. Невинномысск, 2006. 221 с.

6. Джоши П. Искусственный интеллект с примерами на Python : пер. с англ. СПб.: ООО "Диалектика", 2019. 448 с.

УДК 004.422
ГРНТИ 50.41.25

КОНЦЕПЦИЯ ПРИМЕНЕНИЯ MICROCMS В ОТКРЫТЫХ ЦИФРОВЫХ ЭКОСИСТЕМАХ

С. В. Акимов, Д. О. Амельченко, Г. И. Марзаганов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлена концепция применения микросистемы управления контентом (MicroCMS) в открытых цифровых экосистемах, имеющих микросервисную архитектуру. Микросистема управления контекстом допускает глубокую интеграцию в существующие и проектируемые открытые цифровые экосистемы, освобождая разработчиков микросервисов, формирующих данные экосистемы, от реализации решений по

управлению любыми видами контента – от загрузки и отображения отдельных изображений, до создания многостраничных гипертекстовых документов. В отличие от существующих систем управления контекстом и облачных редакторов документов, у MicroCMS отсутствует избыточная функциональность, допускается глубокая интеграция в цифровые экосистемы, а также имеется возможность использования MicroCMS как стороннего (облачного) сервиса, так и развертывание сервиса MicroCMS на собственных серверах.

микросервисная архитектура, управление контентом, MicroCMS, киберсреда, открытые цифровые экосистемы.

Формирование открытых цифровых экосистем требует наличия различных микросервисов, отвечающих требованиям единичной ответственности, которые реализуют различный функционал [1, 2]. Одной из наиболее распространенных функций является функция управления контентом [3]. Существующие системы либо обладают избыточным функционалом (классические CMS), либо отсутствует возможность их развертывания на собственных серверах (Google Docs, Yandex Документы). Необходима система, в которой отсутствует избыточность, существует возможность бесшовной глубокой интеграции в другие системы, а также возможность использования их в виде сторонних сервисов или в виде сервисов, развернутых на собственных серверах. Данным требованиям отвечает микросистема управления контентом (MicroCMS), что показано на рис. 1.

В настоящий момент времени на рынке программного обеспечения отсутствуют микросистемы управления контентом, допускающие глубокую интеграцию в существующие и проектируемые открытые цифровые экосистемы, освобождающие разработчиков микросервисов от реализации решений по управлению любым контентом – от загрузки и отображения изображений, до создания многостраничных гипертекстовых документов. В данной статье изложена концепция микросистемы управления контентом.

Рис. 1. Различные типы систем управления контентом

MicroCMS состоит из пяти микросервисов (рис. 2.):

– BookKeeper, представляет собой микросервис, назначением которого является создание подшивок тематически объединенных документов, созданных в DockKeeper, и позволяющих работать с ними, как с единым целым;

– DockKeeper: микросервис, позволяющий управлять контентом отдельных документов. Документы могут быть представленным в виде неформатированного текста или HTML-документа. DockKeeper позволяет интегрировать изображения, видеоресурсы и любые другие файлы разрешенного типа, управление которыми осуществляется микросервисами ImageKeeper, VidoKeeper и FileKeeper;

– ImageKeeper, FileKeeper, VidoKeeper – микросервисы, обеспечивающее сохранение и управление изображениями, видеоресурами и файлами любых разрешенных типов, соответственно. Сохранение осуществляется в СУБД GridFS.

Такой подход позволяет распределить функционал управления документами и файлами, интегрированными в эти документы, между отдельными микросервисами. Предложенный набор микросервисов обеспечит программистов, занятых разработкой программного обеспечения киберфизических сред, микросервисами, которые реализуют весь необходимый функционал для создания и управления контентом:

– управление загрузкой и отображением отдельных файлов разрешенных форматов;

– управление загрузкой и отображением статических изображений и видео;

– создание, редактирование и отображение HTML-документов и неформатированного текста;

– создание, редактирование и отображение подшивок HTML-документов.

Внедрение микросистемы управления контентом значительно повысит производительность труда программиста, так как ему не потребуется выполнять реализацию решений по управлению любым контентом – от загрузки и отображения изображений, до создания многостраничных гипертекстовых документов.

Приложение создается на базе подхода DDD (Domain Driven Design), представляющей собой подход к разработке приложений основе модели предметной области (домена). Приложения, в зависимости от сложности бизнес-логики и технической реализации, разбиваются на три слоя: модели предметной области (Domain), инфраструктуры и приложения. Слой домена отвечает за представление сущностей предметной области. Слой инфраструктуры обеспечивает сохранение доменной модели. Основу данного

слоя составляет репозиторий, реализующий CRUD методы. Слой приложения реализует функционал RESTful API.

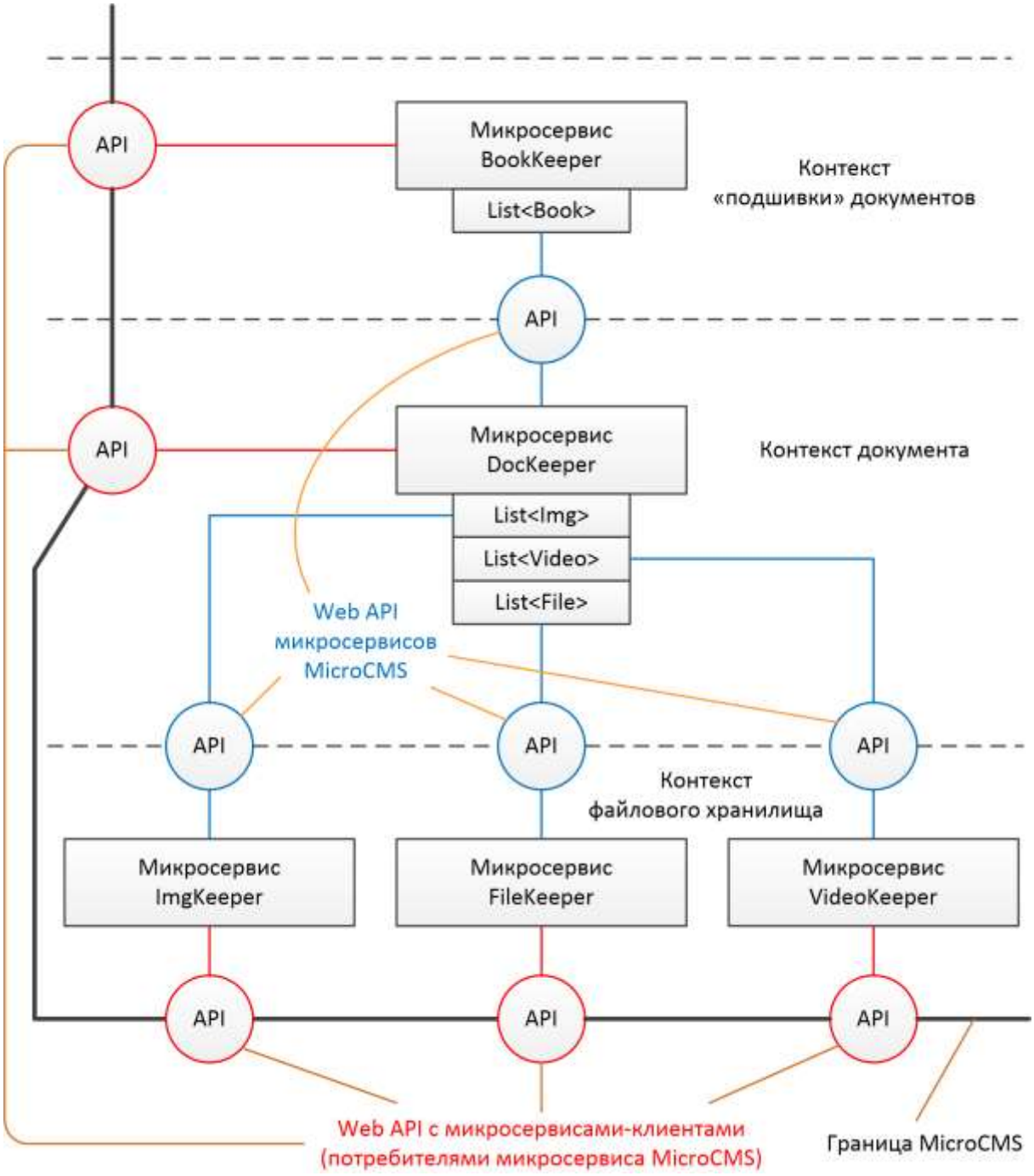


Рис. 2. Микросервисная архитектура встраиваемой системы управления контекстом

На рис. 3 представлен пример графического интерфейса пользователя, выполненного с помощью технологии Blazor [4, 5].

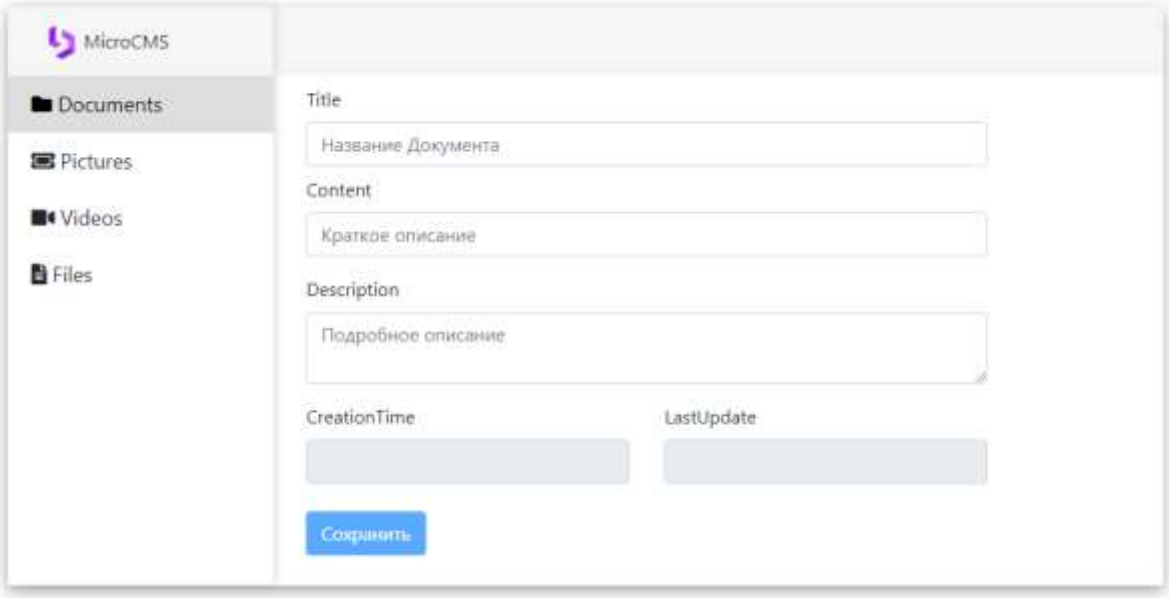


Рис. 4. Реализация графического интерфейса пользователя

Список используемых источников

1. Верхова Г. В., Акимов С. В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // Сборник статей XXIV Международной научной конференции «Волновая электроника и инфокоммуникационные системы». Санкт-Петербург, 2021. С. 34–39.

2. Merson P., Yoder J. Modeling Microservices with DDD. ISBN: Electronic ISBN:978-1-7281-7415-0 Print on Demand (PoD) ISBN:978-1-7281-7416-7. DOI: 10.1109/ICSA-C50368.2020.00010.

3. R. Bose. CMS: a knowledge-based tool for intelligent information systems application development. Print ISBN:0-8186-3730-7. DOI: 10.1109/DMISP.1993.248632. INSPEC Accession Number: 4509164.

4. A. Romano and W. Wang, "WasmView: Visual Testing for WebAssembly Applications," 2020 IEEE/ACM 42nd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), 2020, pp. 13-16.

5. ASP.NET Core Blazor. URL: https://www.elibrary.ru/item.asp?id=43808531 (дата обращения: 26.03.2022)

УДК 616-71
ГРНТИ 76.13.33

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОЧНОЙ ЦИТОМЕТРИИ И АВТОМАТИЧЕСКОЙ МИКРОСКОПИИ ПРИ ИССЛЕДОВАНИИ ОСАДКА МОЧИ

М. И. Алексеева, А. В. Бологова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время существует множество методик диагностики различных заболеваний человека. Особое место в клинической практике занимают лабораторные исследования. В частности, в лечении и прогнозировании патологий мочеполовой системы, большое практическое значение имеет анализ мочи. Анализ мочи широко применяется для мониторинга инфекций мочевыводящих путей, определения причины кровотечений в мочевыделительной системе, заболеваний почек и др. Процесс ручного исследования мочи является длительной, трудоемкой процедурой, что не соответствует текущим потокам в лаборатории и требует достаточно хорошей практической подготовки лаборанта. Учитывая большой поток анализов, процесс исследования стал стремительно автоматизироваться. Это значительно повысило качество диагностики и оптимизировало рабочий процесс за счёт снижения ручного труда в лаборатории. Одним из этапов анализа мочи, имеющем большое практическое значение в клинической диагностике, лечении и прогнозировании патологий мочеполовой системы, является определение форменных элементов в осадке мочи. В этой статье рассматриваются основные преимущества и отличия двух технологий исследования осадка мочи, преобладающих на рынке лабораторного оборудования, таких как проточная цитометрия и автоматическая микроскопия.

микроскопия осадка мочи, проточная цитометрия, автоматическая микроскопия.

Общий клинический анализ мочи наряду с общим клиническим анализом крови является наиболее часто выполняемым видом лабораторных исследований в поликлинике. Анализ мочи в обязательном порядке проводят не только пациентам с заболеваниями почек и мочевыводящих путей, но и всем больным независимо от предполагаемого диагноза на первичном этапе диагностики, а также для оценки течения заболевания и эффективности проводимого лечения. Широкая распространенность данного вида исследования обусловлена несколькими факторами. Во-первых, результаты такого анализа имеют большой объем диагностической информации, как о состоянии почек, так и многих других органов и системах. Во-вторых, методы забора мочи в основном неинвазивные. И, что немаловажно, широкое

применение данного анализа в клинической практике врача обусловлено относительно низкими затратами на выполнение одного анализа [1].

Процесс исследования осадка мочи традиционно заключается в подсчете элементов, которые различаются по определенным признакам (яркость, цвет, геометричность). Исследование мочевого осадка изначально проводилось путем ручного микроскопического исследования, вначале под малым увеличением (× 100), а затем под большим (× 400) увеличением [2, 3]. Данный процесс требует от оператора большой внимательности, что приводит к быстрой утомляемости зрения. Это ограничивает возможность получения достоверной количественной информации об исследуемых объектах. Немаловажным фактором при этом так же являются субъективные и качественные оценки параметров составляющих элементов, которые приводят к низкой точности лабораторной диагностики и сложности обеспечения повторяемости результатов при выполнении научных исследований.

Интенсивное развитие вычислительной техники и повсеместное внедрение цифровых технологий привело к появлению автоматизированных систем для работы с биоматериалами без существенного увеличения стоимости анализа.

В настоящее время на рынке лабораторного оборудования представлено достаточное количество различных по составу и сложности аппаратно-программных систем и комплексов для автоматизации исследования осадка мочи. При выборе модели для исследования элементов мочевого осадка, необходимо учитывать, что в основе прибора может лежать метод проточной цитометрии или автоматической микроскопии.

Принцип работы автоматического анализатора с проточной цитометрией довольно прост. Проба мочи забирается в автоматическом либо ручном режиме, после перемешивания попадает в реакционные камеры и помечается специальным флуоресцентным маркером, связывающимся только с нуклеиновыми кислотами. Тщательно размешивается и отправляется для дальнейшего измерения в проточную кювету. Компоненты мочи выстраиваются в цепочку друг за другом в канале посредством гидродинамического фокусирования, которое обеспечивается разностью давлений между образцом мочи и ламинарным потоком жидкости реактива.

Принципом метода проточной цитометрии является регистрация сигналов светорассеяния и флюоресценции от каждого элемента образца мочи.

После окончания анализа, все жидкости направляются в сливную емкость, для дальнейшей ее утилизации. Далее происходит обработка данных и вывод результатов на экран пользователя [4].

В результате анализа мы получаем скаттерграмму, как изображено на рис. 1. Она далеко не всем доступна для интерпретации результатов.

Все более популярными в лабораториях с небольшим и средним потоком анализов становятся системы автоматизации микроскопического анализа мочевого осадка, основанные на получении качественных микрофотографий с последующей компьютерной обработкой и автоматической идентификацией элементов мочевого осадка.

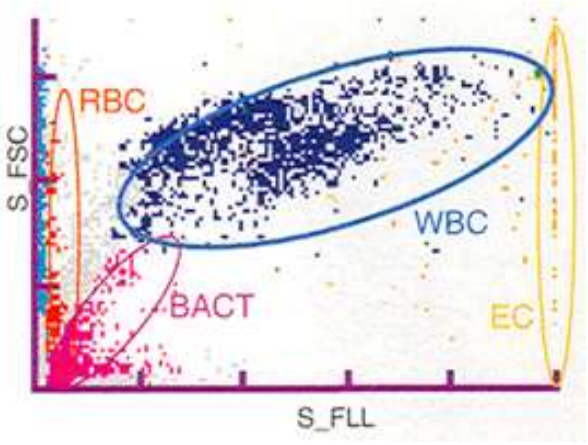


Рис. 1. Скаттерограмма

В основе данный систем лежит метод цифровой микроскопии. Инструментом описываемого метода является цифровой комплекс, который состоит из микроскопа и персонального компьютера с необходимым программным обеспечением [5].

Оптическая система состоит непосредственно из микроскопа и фото- или видео-камеры. Качество полученных изображений можно обеспечить только использованием профессионального оборудования для цифровой микроскопии.

В результате анализа мы получаем количественную оценку состава осадка мочи и изображения полученные в ходе анализа, что дает возможность редактировать и анализировать снимки эксперту. Пример получаемого изображения представлен на рис. 2.

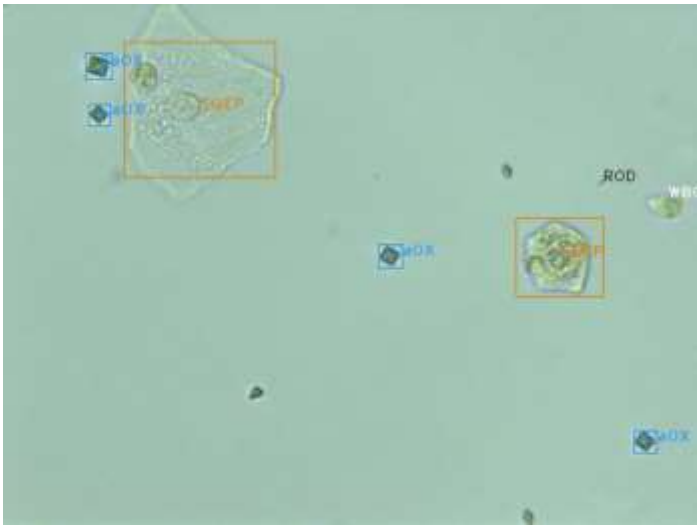


Рис. 2. Обработанное изображение, полученное при помощи камеры

Стоит отметить, что результаты пациента сохраняются в базе данных как при проточной цитометрии, так и при автоматической микроскопии. Это позволяет при необходимости строить карты динамического обследования.

Главное отличие исследуемых методов заключается в том, какие выходные данные мы получаем. В случае автоматической микроскопии это изображения осадка мочи, полученные при помощи камеры, которые эксперт может проанализировать и при необходимость отредактировать результат [6]. В случае с проточной цитометрией, выходными данными является скаттерграмма, которая далеко не всем доступна для визуального восприятия.

Иногда случается так, что при анализе требуется идентификация неоднозначных или непризанных образцов, которые анализатор не смог распознать. При автоматической микроскопии оператор может обратиться к сохраненным изображениям и провести дополнительный анализ, но при проточной цитометрии у исследователя нет возможности визуализировать нераспознанные элементы, поэтому в этом случае требуется проводить дополнительную идентификацию клеток при помощи традиционной ручной микроскопии.

Для любого лечебного учреждения важным является вопрос цены. Аппараты, в основе которых лежит метод проточной цитометрии, имеют достаточно высокую цену, что обусловлено дорогой технологией создания прибора. Помимо этого, при анализе требуются дополнительные расходные материалы, такие как дилюенты, окрашивающие, фокусирующие, контрольные, калибрующие растворы, разбавители, что существенно повышает стоимость одного анализа. Использование метода цифровой микроскопии сокращает количестве расходных материалов до минимума. Все это существенно снижает стоимость анализа.

Подводя итог, хочу отметить, что автоматизация анализа осадка мочи значительно повысила качество диагностики и оптимизировала рабочий процесс за счёт снижения ручного труда в лаборатории.

При выборе того или иного метода, который лежит в основе анализатора необходимо прежде всего опираться на использование современных методик исследования, рекомендованных российскими и зарубежными профессиональными ассоциациями, на потребности и финансовые возможности лаборатории, на постоянный продуктивный диалог врачей клиницистов и врачей-лаборантов, как на этапе назначения анализов, так и их интерпретации.

Рассмотренные методы позволяют быстро и качественно проводить исследования в этой области, но имеют большие различия в работе.

Метод автоматической микроскопии имеет значительное преимущество в том, что оператор может оценить результат визуально, при помощи полученных изображений.

Помимо этого, автоматическая микроскопия позволяет существенно сэкономить на расходных материалах, так как в отличие от проточной цитометрии, скрытые расходы отсутствуют.

Список используемых источников

1. Шибанов А. Н., Куриляк О. А. Лаборатория – клиницисту. Анализ мочи в современной клинике // Медицинский алфавит. 2017. Т. 3. № 33. С. 54–60.
2. Клиническая лабораторная диагностика. Национальное руководство. В 2-х томах. Том 1 / Главные редакторы В. В. Долгов, В. В. Меньшиков. Москва: Изд-во ГЕОТАР-Медиа, 2012. 923 с.
3. Морозова В. Т., Миронова И. И., Марцишевская Р. Л., Романова Л. А. Мочевые синдромы. Лабораторная диагностика. Москва : РМАПО, 2011. 112 с.
4. Кузнецов А. Н., Демин А. Ю. Принцип работы автоматического анализатора мочи с технологией проточной цитометрии // Современные инновации. 2020. № 2(36). С. 28–29.
5. Цифровая микроскопия. URL: https://altami.ru/articles/about_microscopes/digital/ (дата обращения: 25.03.2022)
6. Козлов А. В., Большакова Г. Д., Зимина В. А., Осташова Д. Г. Подходы к стандартизации анализа мочи // Лабораторная диагностика. 2011. № 1 (24).

УДК 004.051
ГРНТИ 50.41.29

АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДОВ ПОСТРОЕНИЯ ИЗОБРАЖЕНИЯ В ВИДЕОИГРАХ

Д. О. Амельченко, И. В. Гвоздков, С. С. Гоняев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рост системных требований видеоигр и развитие производительности ЭВМ всегда были неразрывно связаны. Но для многих пользователей ПК современные компьютерные комплектующие остаются непозволительной роскошью. Это означает, что успех игры будет напрямую зависеть от её доступности, и для повышения эффективности её работы на слабых ПК необходимо прибегать к оптимизации построения изображения. Некоторые методы такой оптимизации требуют весьма больших временных затрат в процессе разработки, а значит в зависимости от содержания игры нужно сочетать наиболее эффективные для конкретных проектов методы.

оптимизация, видеоигры, компьютерные игры, рендеринг.

Производительность вычислительных устройств в последнее время растёт с огромной скоростью, а вместе с ней и системные требования видеоигр. Но далеко не у каждого пользователя имеется возможность закупать и использовать самое современное оборудование.

В результате вышесказанного можно утверждать, что важным аспектом распространённости и популярности того или иного видеоигрового продукта является его требовательность к производительности компьютера пользователя. Для обеспечения работоспособности проекта на широком спектре вычислительных машин, включая низкопроизводительные, необходимо прибегать к различным методам оптимизации построения изображения.

Под оптимизацией построения изображения понимается процесс повышения скорости отрисовки изображения (рендеринга) с целью улучшения игрового процесса и визуального восприятия. Оптимизация включает в себя огромное количество различных методов, среди которых существуют как применяемые практически повсеместно, так и используемые в соответствии со спецификой конкретного проекта.

Для контроля качества оптимизации рендеринга можно выделить четыре основных критерия:

– Первое, что обязана обеспечивать качественная оптимизация – это стабильность игры. Применённые методы оптимизации построения изображения не должны мешать запуску программного продукта и его нормальной работе без ошибок и со стабильным числом кадров в секунду.

– Второе – доступность. Разработчик не знает, на каком компьютере будет запускаться его конечный продукт. Соответственно, ему необходимо предусмотреть механизмы, которые позволят запускать игры на большом количестве различных ПК. Как утверждают представители польской геймдев компании QLOC – «Показатель хорошей оптимизации – игра, работающая с одинаковой частотой кадров на широкой линейке аппаратных конфигураций, включая низкопроизводительные».

– Третье – качество рендеринга. В основе большого количества различных методов оптимизации лежит принцип удаления и упрощения визуальных эффектов, а также количества и качества окружающих объектов для снижения нагрузки на видеокарту при рендеринге. При этом чрезмерное использование таких методов может навредить игровому процессу и, как следствие, опыту игрока [1]. Поэтому хорошая оптимизация – это баланс между стабильной работой и заданным уровнем детализации рендеринга.

– Четвёртое – стабильность ОС. Нередки случаи, когда требовательные игры, используя избыточное количество вычислительных ресурсов, вызывали сбои в работе ПО, сервисов, служб и ОС в целом, а значит качественная оптимизация рендеринга должна препятствовать нарушению нормальной работы операционной системы.

Оптимизация требует индивидуального подхода к продукту. Способы, которые хорошо работают в одних проектах, в других могут привести к ухудшению производительности и работоспособности [2]. Тем не менее,

существует набор универсальных методов оптимизации построения трёхмерного изображения, которые могут быть использованы в подавляющем большинстве проектов:

Первый из этих методов – минимизация влияния объектов за пределами экрана. Поскольку поле зрения игрока сильно ограничено, и он не способен видеть всё, что находится вокруг него, есть возможность сильно снизить нагрузку на видеокарту, сведя к минимуму объём вычислений для объектов вне зоны видимости. При использовании этого способа оптимизации могут возникнуть проблемы с отслеживанием местоположения и состояния объекта, находящегося за пределами экрана. Чтобы избежать этого необходимо делить объекты в архитектуре проекта на два слоя: один слой будет отвечать за визуальное представление объекта и использоваться только тогда, когда находится в поле зрения игрока, а второй слой будет хранить данные и функции объекта для мониторинга позиции и другой информации. Также этот метод оптимизации можно дополнить созданием отдельных процедур, выполняющих упрощённое обновление объекта без анимаций и других алгоритмов, когда этот объект находится вне поля зрения игрока [3].

Согласно информации с сайтов raiseyourskillz.com и escapistmagazine.com в большинстве игр с видом от первого лица поле зрения игрока ограничено углом в 90 градусов, а это означает, что в результате исключения из обработки зон за пределами видимости появляется возможность снизить затрачиваемую вычислительную мощность видеокарты в среднем в 4 раза.

Второй метод – клонирование текстур и объектов. Зачастую на игровых сценах находится множество одинаковых объектов. Чтобы избежать многократной отрисовки одного и того же объекта его можно однократно отрисовать, сохранить и затем несколько раз скопировать на сцену [3]. Большинство современных игровых движков имеют встроенные инструменты для копирования объектов. Примером может служить технология instanced static mesh в Unreal Engine [4].

Третий метод – использование LOD (англ. *Levels Of Detail* – уровни детализации). Этот способ используется для того, чтобы снизить количество ресурсов, затрачиваемое на отрисовку удалённых объектов. Суть метода заключается в создании нескольких копий модели и текстуры более низкой детализации, либо в создании упрощённой модели и нескольких внешних надстроек с деталями для этой модели [3]. Указанные модели с более низкой детализацией будут использоваться на больших расстояниях от игрока, причём при приближении модели будут подменяться (или дополняться) на всё более детализированные.

Для достижения лучшей производительности необходимо комбинировать различные методы оптимизации. В таблице 1 представлено сравнение

производительности нескольких сцен с использованием методов оптимизации построения изображения, и без них.

ТАБЛИЦА 1. Сравнение производительности сцен

Количество объектов на сцене	Количество кадров в секунду без использования методов оптимизации	Количество кадров в секунду при использовании LOD	Количество кадров в секунду при использовании LOD и клонирования объектов
2500	15	75	95
5000	9	40	95
10000	2	20	90
15000	< 1	15	90
20000	< 1	10	90
30000	< 1	9	90
40000	< 1	8	90

Проанализировав таблицу, можно утверждать, что применение LOD позволило увеличить частоту кадров в среднем в 9 раз, а использование комбинации клонирования и LOD дало стабильную отрисовку в 90–95 кадров в секунду, не зависящую от размера сцены.

Исходя из вышесказанного можно отметить, что на текущий момент необходимо использование хотя бы минимальных средств оптимизации рендеринга при создании видеоигр с трёхмерной графикой. Причём если в проектах на готовых игровых движках часть оптимизации выполняет сам игровой движок, то в проектах не использующих готовое ПО для создания игр этому стоит уделить отдельное внимание. Важно отметить, что использование корректных методов и их сочетаний поможет не только улучшить производительность и стабильность игр, но и сэкономить время на их разработку. Так, например, при создании игр с маленькими сценами стоит уделять больше внимания клонированию и удалению объектов за зоной видимости, поскольку создание LOD моделей может занять большое количество времени, но при этом принести незначительный прирост производительности из-за отсутствия больших расстояний в игре.

Список используемых источников

1. Шелл Д. Геймдизайн. Москва: Альпина Паблишер, 2022. 640 с. ISBN: 978-5-9614-1209-3

2. Шрейер Д. Кровь, пот и пиксели Обратная сторона индустрии видеоигр. 2-е изд. Москва: Бомбора, 2021. 384 с. ISBN: 978-5-04-102597-7.

3. Preisz E., Garney B. Video Game Optimization // Cengage Learning PTR; 1st edition (March 1, 2010) 368 p. ISBN-10 : 1598634356

4. Куксон А., Даулингсока Р., Крамплер К. Разработка игр на Unreal Engine 4 за 24 часа. Москва: Бомбора, 2019. 528 с. ISBN: 978-5-04-103162-6.

Статья представлена научным руководителем, кандидатом технических наук, доцентом М. Д. Поведайко.

УДК 004.414.3
ГРНТИ 81.93.29

АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ СИСТЕМ ПЛАНИРОВАНИЯ И ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ ДЛЯ ГОСУДАРСТВЕННЫХ СТРУКТУР НА БАЗЕ ВЕБ-ТЕХНОЛОГИЙ

И. Л. Андреев, А. А. Невров, М. В. Хомичук

Академия Федеральной службы охраны Российской Федерации

В настоящее время уровень автоматизации процесса планирования и организации деятельности в государственных структурах не соответствует потребностям должностных лиц. Задачи по формированию планирующих и отчетных документов госструктур, сбор и обобщение информации о степени их реализации, как правило, решаются без применения специализированных методов и технологических приемов, а также соответствующих средств автоматизации данной деятельности.

информационная безопасность, веб-приложения, веб-сервер, клиент.

В рамках решения задачи по цифровизации деятельности отдельных государственных структур осуществляется внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей [1]. Немаловажным фактором является автоматизация деятельности государственных структур не только с точки зрения конечного потребителя госуслуг, но и внутренних бизнес-процессов организаций. И если по процессу оказания госуслуг в настоящее время достигнуты целевые показатели в области качества, то по организации внутренних процессов госструктур дела обстоят не столь хорошо. Процесс организации и управления собственной деятельностью в государственных структурах требует значительных временных затрат, проведения дополнительных мероприятий по обеспечению необходимой полноты и точности данных.

В связи с этим возникает необходимость в создании информационной системы, которая обеспечит необходимый функционал для эффективной организации и планирования деятельности государственной структуры.

Анализ статистики компьютерных атак за 2019–2022 гг. [2, 3] показывает, что такая система должна быть надежно защищена от действий внешнего и внутреннего нарушителей. То есть остро стоит вопрос создания именно защищенных информационных систем (далее ЗИС) организации и планирования деятельности государственной структуры. Для такой ЗИС необходимо защитить всю информацию, циркулирующую в данной информационной системе, и причём вопрос защиты следует учесть еще на этапе проектирования.

Для обеспечения безопасности рассматриваемой системы следует решить ряд технических и организационных задач, а именно обеспечить безопасности кода, используемого в программном обеспечении, безопасность администрирования системы путем выбора и настройки политик разграничения доступа, создать защищенное информационное хранилище, удовлетворяющее требованиям нормативных документов к системам такого класса.

Технические и организационные меры защиты информации, которые реализуются в ЗИС организации и планирования деятельности, должны быть направлены на обеспечение: конфиденциальности, целостности, доступности [4].

При принятии решении о методах и средствах защиты информации, содержащейся в системе, необходимо определить класс защищенности информационной системы. Класс защищенности определяется в соответствии с приложением к требованиям о защите информации, содержащейся в ЗИС, не составляющей государственную тайну [5].

В связи с этим ЗИС должна обладать рядом сервисов информационной безопасности. Сервисом информационной безопасности называется совокупность механизмов, процедур и других средств управления для снижения рисков, связанных с угрозой утраты или раскрытия данных. На программном уровне они представлены следующими сервисами [5]:

- идентификация и аутентификация пользователей;
- разграничение прав доступа;
- аудит действий пользователей;
- управление событиями информационной безопасности;
- шифрование информационных потоков;
- контроль целостности;
- контроль защищенности.

Данные сервисы информационной безопасности можно реализовать вручную или использовать уже проверенные готовые решения. Также они могу быть включены в выбранные инструменты разработки.

Немаловажным является вопрос выбора архитектуры приложения. Для более широкого использования ЗИС, необходимо, чтобы приложение было кроссплатформенным. Наиболее эффективная и простая архитектура для достижения данной цели – реализация ЗИС в виде веб-приложения. Использование в качестве клиента веб-браузера позволяет создать унифицированный интерфейс. Проведенный ранее анализ позволил сформулировать предложения по использованию программных средств для построения ЗИС: в роли веб-сервера будет использоваться Nginx, а в роли информационного хранилища – система управления базами данных PostgresPro.

Для написания логики работы серверной части веб-приложения необходимо реализовать большое количество функций. С целью облегчения выполнения данной задачи целесообразно использовать веб-фреймворк. В результате анализа многих библиотек в качестве веб-фреймворка был выбран Django. В качестве операционной системы используется ОС Astra Linux SE.

Данные компоненты были выбраны с целью построить устойчивую и безопасную систему. Благодаря такому выбору средств были решены проблемы с обеспечением безопасности информации, циркулирующей в данной ЗИС. Для обеспечения требуемого уровня безопасности были предприняты следующие меры: принудительное использование протокола HTTPS; вывод сервера базы данных в отдельную локальную сеть; настроена политика безопасности.

На рисунке показана структурная схема разработанной ЗИС. Данная структура была реализована в программном обеспечении виртуализации VMware Workstation. Стоит отметить, что тестирование ЗИС с помощью таких инструментов, как: xSpider, nmap, SQLmap, Solar App Screener, Greenbone, Nessus, Scanner-VS, показали хорошие оценки безопасности.

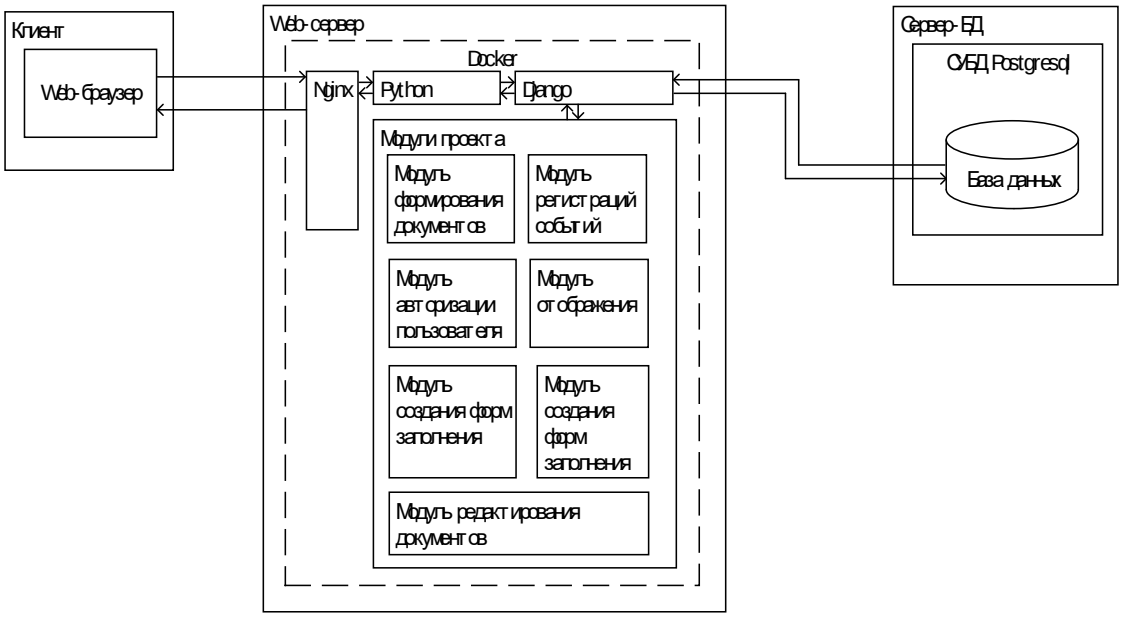


Рисунок. Структурная схема разработанной ЗИС

В результате предложены базовые программные компоненты для построения ЗИС планирования и организации деятельности государственных структур, разработана и верифицирована на соответствие требованиям приказа ФСТЭК России от 11 февраля 2013 г. № 17 архитектура такой ЗИС. Предложенные программные компоненты полностью удовлетворяют требованиям безопасности, предъявляемым к государственным автоматизированным системам данного класса. Получена практическая реализация макета системы планирования и организации деятельности, для которой проведено тестирование на уязвимости и на проникновение, показавшее хорошие результаты, подтверждающие защищенность разработанного макета.

Список используемых источников

1. Паспорт федерального проекта "Цифровое государственное управление" национальной программы "Цифровая экономика Российской Федерации" от 04.06.2019 года. URL: https://digital.ac.gov.ru/upload/iblock/aa1/%D0%9F%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%20%D0%A4%D0%9F%20%D0%A6%D0%93%D0%A3%20%D0%B8%D0%B7%20%D0%93%D0%98%D0%98%D0%A1%20%D0%AD%D0%91%20(%D0%BD%D0%B0%2027_06_2019).docx (дата обращения: 25.11.2021).

2. Актуальные киберугрозы: 1 квартал 2021 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (дата обращения 10.03.2022).

3. Актуальные киберугрозы: итоги 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (дата обращения 10.03.2022).

4. Управление информационной безопасностью телекоммуникационных систем: учебно-методическое пособие / А. Н. Цибуля [и др.]; под общ. ред. А. И. Козачка. Орёл: Академия ФСО России, 2018. 248 с.

5. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

УДК 004.93'11+ 004.932.2
ГРНТИ 20.19.29

ПРИМЕНЕНИЕ ДЕТЕКТОРОВ КЛЮЧЕВЫХ ТОЧЕК ДЛЯ ОБНАРУЖЕНИЯ ТЕКСТОВЫХ ОБЛАСТЕЙ ИЗОБРАЖЕНИЯ

А. А. Арестов, С. А. Копылов

Академия Федеральной службы охраны Российской Федерации

Задача по защите текстовой документов, содержащих конфиденциальную информацию и персональные данные пользователей, является актуальным направлением

исследований. В работе рассмотрены особенности применения детекторов ключевых точек для обнаружения текстовых областей в изображениях, представленных фотографиями и снимками экрана монитора. В ходе экспериментальной оценки извлечения ключевых точек из фотографий и снимков экрана получены количественные значения ключевых точек и их соответствие текстовых областям изображения. Полученные результаты позволяют сделать вывод о возможности применения детекторов ключевых точек для обнаружения текстовых областей на изображениях и защиты текстовых документов от утечки.

В заключении представлены направления дальнейших исследований.

текстовые документы, защита информации от утечки, распознавание образов, алгоритмы детектирования ключевых точек.

В процессе развития систем электронного документооборота, а также систем, осуществляющих обработку, хранение и передачу персональных данных и информации ограниченного доступа, возросло количество инцидентов информационной безопасности. Одним из наиболее часто встречаемых инцидентов является утечка информации [1].

Наибольшее число нарушений приходится на конфиденциальную, платежную информацию и персональные данные, содержащиеся в тестовых документах вне зависимости от формы их представления. Защита текстовой информации от утечки реализуется посредством применения DLP-систем, основанных на применении средств оптического распознавания символов [2, 3]. В то же время отмечается значительный рост инцидентов безопасности, связанных с утечкой как снимков экрана, так и фотографий экрана с выведенным на него текстовым документом.

Наличие ограничений в существующих средствах оптического распознавания символов не позволяет осуществлять правильное извлечение текстовой информации из снимка или фотографии экрана ввиду присутствия как текстовых и графических областей, так и возможного наложения их друг на друга. Указанное ограничение делает задачу по совершенствованию средств защиты текстовой информации, содержащейся в снимках или изображения экрана, от утечки актуальным направлением исследований.

Для решения указанной задачи могут быть применены методы теории распознавания образов, основанные на обнаружении ключевых характеристик изображения. Под ключевой характеристикой (локальным признаком) понимается регион (шаблон) изображения, отличающийся от соседних с ним регионов по установленным критериям [4]. В качестве критериев могут выступать следующие параметры изображения: интенсивность, цвет, текстура и т. д., как по отдельности друг от друга, так и в совокупности.

Все ключевые характеристики (локальные признаки) в зависимости от назначения детектора признаков могут быть разделены [5]:

– ключевые точки – локальные особенности изображения, содержащие ограниченный набор хорошо локализованных и индивидуально идентифицируемых опорных точек;

– края – конкретный тип локальных признаков на изображении, характеризующих специфическую структуру или отдельные области;

– небольшие области изображения – уникальные особенности изображения (сигнатуры), позволяющие распознавать конкретные объекты на изображениях.

Для обнаружения текстовых областей на снимках экрана или фотографиях могут быть применены детекторы, основанные на использовании одновременно всех ключевых характеристик. Результат обнаружения текстовых областей указанными детекторами отличается наличием большого количества ошибок первого и второго рода и не может быть использован для правильного детектирования текстовых областей изображения и обнаружения факта утечки информации.

Детектирование краев позволяет распознать границы отдельных областей и сформировать остовы, соответствующие краям отдельной области или локальной характеристики изображения. В случае наличия дополнительных элементов вблизи контуров текста обнаружение текстовых областей посредством детектора краев нецелесообразно ввиду наличия ошибок детектирования, связанных с пропуском таких областей.

Стоит отметить, что процесс обнаружения текстовых областей в изображениях, полученных посредством фотографирования или создания снимка экрана, характеризуется следующими особенностями [6]:

– в процессе создания снимка экрана осуществляется растеризация изображения с заданным значением разрешения и количества цветов;

– в процессе фотографирования помимо растеризации могут быть осуществлены такие преобразования как искажения, вносимые внешним освещением; искажения, вносимые объективом и искажения, связанные с оптическими особенностями формирования изображения.

Исходя из представленных особенностей, в процессе обнаружения текстовых областей изображения целесообразно использовать детектор ключевых точек. К методам детектирования ключевых точек относятся следующие алгоритмы:

– SIFT (Scale-Invariant Feature Transform) [7];
– SURF (Speeded-Up Robust Features) [8];
– FAST (Features from Accelerated Segment Test) [9];
– BRIEF (Binary Robust Independent Elementary Features) [10];
– ORB (Oriented FAST and Rotated BRIEF) [11].

В процессе извлечения ключевых точек алгоритмом SIFT используется пространственная фильтрация, основанная на гауссовом фильтре, посред-

ством преобразования изображений в масштабно-инвариантные координаты относительно локальных особенностей. Алгоритм SURF осуществляет анализ детерминанта матрицы Гессе, принимающего максимальные значения в областях перепада яркости.

Алгоритмы FAST и BRIEF основаны на использовании методов машинного обучения:

1) FAST использует дерево решений в процессе классификации соседних пикселей по интенсивности цвета относительно анализируемого в изображении;

2) BRIEF детектирует ключевые точки посредством метода случайного леса или наивного Байесовского классификатора.

Алгоритм ORB представляет собой сочетание алгоритмов FAST и BRIEF с определенными модификациями. На первом этапе посредством меры Харриса ключевые точки обнаруживаются по алгоритму FAST. Полученные точки подвергаются серии бинарных сравнений по алгоритму BRIEF для формирования результирующих ключевых точек.

В ходе экспериментальной оценки представленных алгоритмов детектирования ключевых точек проведены эксперименты по извлечению ключевых точек из снимка экрана и фотографии монитора с выведенным текстовым документом. Помимо текстового документа на экран монитора выведено контекстное меню файлового менеджера, файлы с подписями и прочие элементы рабочего стола.

Результаты извлечения количества ключевых точек из снимка экрана и фотографии монитора представлены в таблице 1.

ТАБЛИЦА 1. Извлечение ключевых точек из различных типов изображений

Изображение	Алгоритм детектирования ключевых точек				
	SIRF	SURF	FAST	BRIEF	ORB
Снимок экрана	2510	11959	10933	10593	476
Фотография монитора	15597	31104	9248	9241	494

Анализ полученных результатов позволяет сделать вывод о том, что алгоритм SURF характеризуется наибольшим количеством обнаруженных ключевых точек как на снимке экрана, так и фотографии монитора. Однако визуальный анализ полученных результатов показал, что ключевые точки, обнаруженные посредством указанного алгоритма, соответствуют областям изображения, отличающимся (не соответствующих) по интенсивности цвета (яркости) пикселей от текстовых.

В ходе дальнейшего визуального анализа обнаруженных ключевых точек на анализируемых изображениях установлено, что наиболее точно текстовые области как на снимках, так и на фотографиях детектируются алгоритмами BRIEF и FAST. При этом на ключевые точки алгоритма FAST

приходится больше текстовых областей изображений. Пример извлечения ключевых точек на фотографии экрана алгоритмом FAST представлен на рисунке.

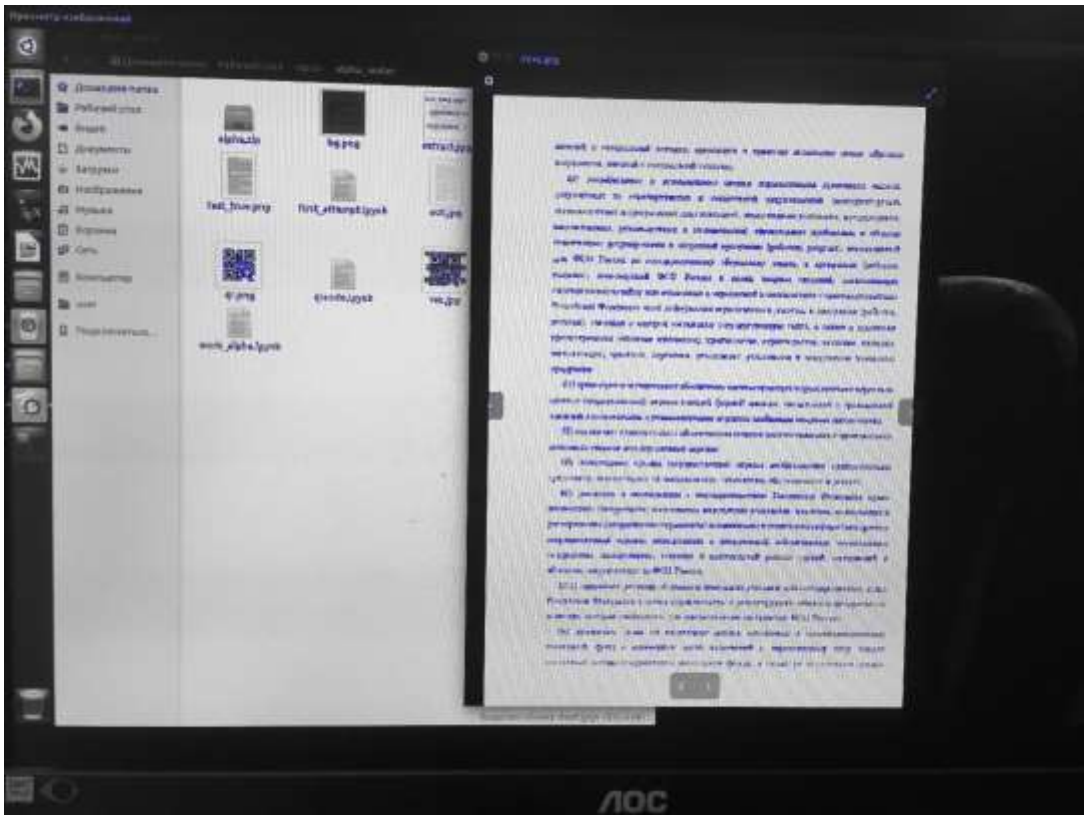


Рисунок. Извлечение ключевых точек из фотографии экрана алгоритмом FAST

Полученные результаты экспериментальных оценок извлечения ключевых точек из изображений, полученных посредством создания снимков экрана и фотографирования, позволяют использовать алгоритм детектирования FAST в процессе обнаружения текстовых областей изображения. В случае практической реализации указанного алгоритма в подсистеме анализа изображений DLP-систем может быть повышена защищенность текстовых документов от утечки за счет детектирования текстовых областей и извлечения содержимого на изображениях с последующим контентным анализом полученного текста на предмет наличия конфиденциальной информации и персональных данных пользователей. Практическая реализация прототипа детектирования и извлечения содержимого текстовых областей изображения, основанного на алгоритме FAST, является направлением дальнейшим исследований.

Список используемых источников

1. Positive Research 2021. Сборник исследований по практической безопасности. 2021. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/ analytics/positive-research-2021-rus.pdf (дата обращения: 31.01.2022).

2. Guha A., Samanta D., Banerjee A., Agarwal D. A Deep Learning Model for Information Loss Prevention From Multi-Page Digital Documents // IEEE Access. 2021. Vol 9. pp. 80451–80465.

3. Stallings W. Data loss prevention as a privacy-enhancing technology // Journal of Data Protection & Privacy. 2020. Vol 3, N 3. pp. 323–333.

4. Tuytelaars T., Mikolajczyk K. Local Invariant Feature Detectors: A Survey // Foundations and Trends in Computer Graphics and Vision. 2007. Vol 3, N 3. pp. 1–38.

5. Бондаренко В. А., Каплинский Г. Э., Павлова В. А., Тупиков В. А. Метод поиска и сопоставления ключевых особенностей изображений для распознавания образов и сопровождения объектов // Известия ЮФУ. Технические науки. 2019. N 1. С. 281–293.

6. Козачок А. В., Горбачев П. Н., Маркин Ю. В., Гайнов А. Е., Кондратьев Б. В. Модель стегосистемы, основанной на текстовом контейнере, устойчивом к преобразованию формата // Защита информации. Инсайд. 2021. N 5 (101). С. 61–67.

7. Lowe D. G. Distinctive Image Features from Scale-Invariant Keypoints // International Journal of Computer Vision. 2004. Vol 60, pp. 91–110.

8. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features // Computer Vision – ECCV 2006 : Proceedings of 9th European Conference on Computer Vision, Graz, Austria, May 7-13. 2006. pp. 404–417.

9. Rosten E., Drummond T. Machine Learning for High-Speed Corner Detection // Computer Vision – ECCV 2006 : Proceedings of 9th European Conference on Computer Vision, Graz, Austria, May 7-13. 2006. pp. 430–443.

10. Calonder M., Lepetit V., Strecha C., Fua P. BRIEF: Binary Robust Independent Elementary Features // Computer Vision – ECCV 2010 : Proceedings of 11th European Conference on Computer Vision, Heraklion, Crete, Greece, September 5-11. 2010. pp. 778–792.

11. Rublee E., Rabaud V., Konolige K., Bradski G. ORB: An efficient alternative to SIFT or SURF // Proceedings of International Conference on Computer Vision, Barcelona, Spain, November 6-13. 2011. pp. 1–8.

УДК 004.056.5
ГРНТИ 78.21.13

АНАЛИЗ ЗАЩИЩЁННОСТИ СОВРЕМЕННЫХ СЕРВИСОВ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

П. А. Архипов, Д. О. Маркин, Н. Д. Сизов

Академия Федеральной службы охраны Российской Федерации

В статье приводится сравнительный анализ современных сервисов обмена мгновенными сообщениями. Предложены критерии оценивания мессенджеров. Проанализированы функциональных возможности расширенного перечня существующих средств мгновенными сообщениями. Сформулированы выводы, обосновывающие выбор наиболее

защищенных технических решений, обеспечивающих защищенный мгновенный мгновенными сообщениями

мессенджер, сервис обмена сообщениями, модель оценки защищенности.

Развитие информационных технологий и мобильных вычислительных систем привело к появлению такого масштабного явления как виртуальные коммункации посредством сервисов обмена мгновенными сообщениями (согласно Федерального закона от 27.07.2006 № 149-ФЗ «Об инфорации, информационных технологиях и о защите информации») или мессенджерами. При этом разработчиками и владельцам мессенджеров доступны внушительные объемы конфиденциальных данных переписок пользователей, аудиовизуальной информации и других сведений, по своей природе требующих серьезного внимания к защите. Вместе с тем, подавляющее большинство пользователей мессенджеров не уделяют необходимого внимания безопасности личных данных и выбору мессенджера в виду недостаточно развитой культуре информационной безопасности и в ряде случаев введению их в заблуждение относительно реальной защищенности используемых ими программ для коммуникаций.

В связи с этим существует объективная потребность во всесторонней оценке наиболее распространенных мессенджеров на предмет защищенности обрабатываемых данных.

В данной работе рассмотрен ряд сервисов обмена мгновенными сообщениями [3] и выполнен сравнительный анализ их защищенности.

В качестве критериев, по которым оценивались мессенджеры [1], отнесены:

Наличие абонентского шифрования (*End-to-End Encryption* или *E2EE*) [2]. Абонентское шифрование значительно повышает обеспечение конфиденциальности переписки и передаваемых данных.

Наличие возможности анонимной регистрации без привязки к электронной почте, номеру телефона и другим сведениям, позволяющим сравнительного легко идентифицировать пользователя. Данный показатель достаточно условен, поскольку современное законодательство РФ (в частности, согласно положениям Федеральных законов «О связи» и «Об инфорации, информационных технологиях и о защите информации») запрещает использование услуг телекоммуникаций для неидентифицированных пользователей;

Наличие централизованного хранения и обработки данных. Централизация обработки данных снижает устойчивость информационных систем к деструктивным воздействиям и повышает риски нарушения конфиденциальности в случаях компрометации и/или взлома. ДЦентрализация позво-

ляет использовать каждое устройство одновременно и как клиент, и как сервер. И, с учетом применения шифрования и других методов защиты информации, повышает устойчивость сервиса в целом.

Использование открытого исходного кода. Считается, что открытый исходный код сервисов способствует их более высокой защищенности. Кроме того, это соответствует принципам построения защищенных криптографических систем О. Керкгоффса, а также способствует более интенсивному поиску и выявлению уязвимостей в программном обеспечении сервиса.

Обеспечение безопасности социального графа. То есть использование механизмов предупреждения и противодействия сбору сведений о социальных контактах (коммуникациях) между пользователями.

Наличие проверка подлинности собеседника.

Наличие систематического аудита исходного кода, в том числе за счет обратной связи с пользователями сервиса.

В таблице 1 ниже представлены результаты проведенного анализа. Использованы следующие условные обозначения:

ОИК – открытый исходный код;

Ц – наличие центализации или централизованный;

ДЦ – децентрализованный;

Ф – федеративный;

ЗСГ – наличие защиты социального графа;

ХС – хранение переписки на сервере;

НТД – нет точных данных;

СР – сообщество разработчиков.

ТАБЛИЦА 1. Сравнительный анализ показателей защищенности сервисов обмена мгновенными сообщениями

Мессенджер	**ОИК**	**Ц**	**Анон. рег.**	**E2EE**	**ЗСГ**	**ХС**	**Владелец**	**Страна**
Telegram	Нет	Ц	Нет	Есть	Нет	Да	Павел Дуров	Россия
Signal	Да	ДЦ	Нет	Есть	Да	Нет	*Open Whisper Systems*	США
Viber	Нет	Ц	Нет	Есть	Нет	Да	*Viber Media.*	Люксенбург
WhatsApp	Нет	Ц	Нет	Есть	Нет	Да	*Meta*	США
Briar	Да	ДЦ	Да	Есть	Да	Нет	СР	Нет
ТамТам	Нет	Ц	Да	Нет	Нет	Да	*Mail.ru Group*	Россия
Вконтакте	Нет	Ц	Нет	Нет	Нет	Да	*VK*	Россия
Facebook Messenger	Нет	Ц	Да	Есть	Нет	Да	*Meta*	США
Wire	Да	Ц	Да	Есть	Да	Нет	Янус Фриис	США
Element	Да	Ф	Да	Есть	Да	Да	*New Vector*	Великобритания

Мессенджер	ОИК	Ц	Анон. рег.	E2EE	ЗСГ	ХС	Владелец	Страна
Status	Да	ДЦ	Да	Есть	Да	Да	НТД	НТД
Threema	Нет	Ц	Да	Есть	Нет	Да	*Threema GmbH*	Швейцария
Wickr me	Нет	Ц	Да	Есть	Да	Да	*Wickr*	США
Session	Да	ДЦ	Да	Есть	Да	Нет	*Loki Foundation*	НТД
Apple iMassage	Нет	Ц	Нет	Есть	Нет	Да	*Apple*	США
Express	Нет	Ф	Нет	Есть	Нет	Да	*Express*	Россия
Surespot	Да	Ц	Да	Есть	Да	Да	*Surespot LLC*	НТД
Kontalk	Да	Ц	Нет	Есть	НТД	Да	*Kontalk devteam*	НТД
Gajim	Да	ДЦ	Да	Есть	НТД	Нет	СР	Нет
Jami	Да	ДЦ	Да	Есть	Да	Нет	*Savoir-faire Linux*	Нет точных данных
VIPole Secure Messenger	Нет	Ц	Нет	Есть	НТД	Да	НТД	НТД
Keybase	Да	Ф	Да	Есть	Да	НТД	*Zoom Video Communications*	США
CoyIM	Да	Ц	Да	Есть	НТД	Да	НТД	НТД
ChatSecure	Да	Ф	Да	Есть	НТД	НТД	НТД	НТД
Xabber	Да	Ф	Да	Есть	Да	Да	*Redsolition OÜ*	Эстония
Antox	Да	ДЦ	Да	Есть	Да	Нет	*Tox Foundation*	НТД
Linphone	Да	Ц	Нет	Есть	Нет	Да	*Belledonne Communications*	Франция
Delta Chat	Да	ДЦ	Да	Есть	Нет	Нет	НТД	НТД
Silence	Да	ДЦ	Нет	Есть	Нет	НТД	НТД	НТД
Q-municate	Да	Ф	Нет	Есть	Нет	Да	*QuickBlox*	США
Confide	Нет	Ц	Да	Есть	Нет	Нет	*Confide*	США
Frisbee	Да	Ц	Нет	Есть	Нет	Да	НТД	Россия
Twinme	Нет	Ц	Да	Есть	НТД	Нет	*twinlife*	Франция

Среди представленных месенджеров по совокупности показателей защищенности особый интерес представляют такие мессенджеры как *Telegram*, *Briar*, *Confide*, *Wickr me* и *Signal*.

Средство *Briar* является лидер среди рассмотренных мессенджеров, поскольку обладает наибольшим перечнем мер защиты пользователей, включая такие достаточно специфические как автоматическое удаление данных приложений, децентрализацией хранения данных, защитой социального графа. Известно, что *Briar* может передавать сообщения без доступа к сети Интернета, используя *Bluetooth* и *Wi-Fi*. При передаче через Интернет сообщение отправляется через сеть веб-браузера *Tor*.

Известный мессенджер *Telegram* в действительности функционирует несколько иначе, чем может показаться при первом знакомстве. Например, абонентское шифрование используется только при использовании функций «секретного чата», а при регистрации необходимо указывать номер телефона, а приложение имеет доступ к вашим контактам.

Средство *Express* отличается тем, что имеет сертификат соответствия ФСТЭК России, абонентское шифрование, авторизованный на территории РФ разработчик. Поддерживает возможность использованиях собственных серверов, трёхуровневое шифрование на эллиптических кривых. Однако к хранящимся на сервере данным имеет доступ администратор.

Выводы

Рынок сервисов обмена мгновенными сообщениями достаточно крупный, однако действительно качественно реализованных средств немного. В то же время развитие современных технологий и средств разработки дает возможность модифицировать известные решения, объединяя в их функциональность наиболее удачные решения с целью получения наиболее защищенных и надежных технических решений.

Список используемых источников

1. Christoph Rottermanner, Peter Kieseberg, Markus Huber, Martin Schmiedecker, Sebastian Schrittwieser Privacy and Data Protection in Smartphone Messengers // iiWAS2015, Brussels, December, 2015. pp. 11–13. URL: https://publications.sba-research.org/publications/paper_drafthp.pdf (дата обращения: 22.03.2022).

2. Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, Matthew Smith Obstacles to the Adoption of Secure Communication Tools // IEEE Symposium on Security and Privacy, 22–26 May 2017. pp. 17. URL: https://jbonneau.com/doc/ASBDNS17-IEEESP-secure_messaging_obstacles.pdf (дата обращения 22.03.2022).

3. Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, Matthew Smith. SoK: Secure Messaging // IEEE Symposium on Security and Privacy, 2015, pp. 25. URL: https://cacr.uwaterloo.ca/techreports/2015/cacr2015-02.pdf (дата обращения: 22.03.2022).

4. Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, Douglas Stebila. A Formal Security Analysis of the Signal Messaging Protocol // IEEE European Symposium on Security and Privacy, 2017. P. 46. URL: https://eprint.iacr.org/2016/1013.pdf (дата обращения: 22.03.2022).

УДК 004.427
ГРНТИ 20.53.21

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЛАСТИ КОЛЛЕКЦИОНИРОВАНИЯ

М. Э. Баранаускас, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены технологии создания Web-приложений, ориентированных на лиц, занимающихся разного рода коллекционированием. Отражены аспекты стратегии разработки подобного рода приложений, которые позволят коллекционерам создавать новую коллекцию и осуществлять различные операции с ней, не тратя на это большое количество времени, кроме того, у пользователя таких приложений уменьшается вероятность совершить какую-то ошибку в процессе коллекционирования. Проанализированы современные технологические средства Web-проектирования. Для создания такого рода информационных систем важно не только знание определённой технологии, но и понимание того, какие достоинства и недостатки она имеет перед другими технологическими решениями, а также подходит ли она для создания системы, которая будет иметь высокую производительность, и не будет затрачивать чрезмерное количество системных ресурсов.

Web-приложение, дизайн-макет, вёрстка, программирование, база данных.

Информационные технологии в современном мире играют огромную роль. Они позволяют общаться на расстоянии, быть всегда в информационном поле, быстро узнавать важные новости, касающиеся не только самих людей, но и всего мира в целом. Но и немаловажно, что информационные технологии позволяют автоматизировать некоторые рутинные процессы, что также позволяет сэкономить большое количество времени. Особенно экономия времени важна для коллекционеров различных вещей, поскольку, чем больше коллекция, тем больше требуется времени на то, чтобы за ней уследить. Также значительно возрастает вероятность допустить какую-либо ошибку, которую впоследствии будет очень трудно найти, и придётся потратить на это большое количество времени. Здесь на помощь и приходят информационные технологии, делающие процесс коллекционирования приятным и малозатратным.

На сегодняшний день существует огромное количество различных Web-сервисов, мобильных и десктоп-приложений и т. д., позволяющих пользователям создавать свои коллекции и манипулировать ими. Такие сервисы или же приложения должны обладать интуитивно понятным и приятным на вид графическим интерфейсом для того, чтобы пользователям было максимально понятно и комфортно в них работать. Также они должны иметь

грамотную и чётко построенную архитектуру, правильно спроектированную и реализованную базу данных и т. д. Всё это сделает систему наиболее эффективной, надёжной и безопасной.

Web-приложения создаются на основе архитектуры «клиент-сервер». Клиент и сервер обмениваются информацией между собой посредством сети Интернет по протоколу HTTP. В качестве клиента выступает браузер, с помощью которого пользователь вводит запрос в адресной строке и отправляет его на Web-сервер, Web-сервер в свою очередь перешлёт его на сервер, где запущено приложение, которое сгенерирует определённую Web-страницу, в соответствии с запросом пользователя, после чего готовая Web-страница забирается сервером, сервер отдаёт её браузеру, и браузер отобразит её пользователю. Такие Web-страницы называются динамическими, поскольку их содержание генерируется в зависимости от запроса пользователя, в отличие от статических Web-страниц, контент которых одинаков для всех посетителей сайта [1].

Создание Web-приложения – это сложный процесс, который требует глубокого комплексного анализа, позволяющего определить критерии, которым должен соответствовать будущий проект. В общем случае процесс создания Web-приложений включает шесть этапов.

1. Определение целей и задач проекта. Здесь формируются бизнес-цели, устанавливаются требования к создаваемому приложению, разрабатывается общая концепция приложения. После определения целей создаётся расширенный план проекта, в котором определяется, сколько времени и средств будет потрачено на разработку.

2. Разработка структуры сайта. Здесь необходимо продумать содержание сайта, из чего он должен состоять, в какой форме должна подаваться информация пользователям, чтобы они не запутались в ней. Необходимо продумать функциональность страниц, сколько их должно быть и каким образом они будут взаимодействовать между собой. Необходимо составить карту сайта, которая представляется в виде блок-схемы, где каждая отдельная Web-страница отображается прямоугольником, а связи между ними иллюстрируют схему переходов между Web-страницами.

3. Разработка дизайн-макетов. Дизайн-макет представляет собой графическое отображение основных элементов сайта и воплощает его визуальную концепцию. Для его создания используют графические программы. Создаётся Web-дизайн сайта в соответствии с общей концепцией. При дизайне сайта важно создать такие графические объекты, которые быстро загружаются и хорошо смотрятся, не учитывая браузер, который используется пользователем.

4. Вёрстка. Здесь разработанный на предыдущем этапе дизайн-макет сайта переносится в html-код, который распознаётся браузером. Самое главное при вёрстке – это добиться корректного отображения Web-страниц при различных параметрах разрешения экрана.

5. Программирование и контроль качества. На этом этапе строятся функциональные инструменты, которые будут обрабатывать данные. Данный этап определяет уровень стабильности и защищённости Web-приложения. Поэтому очень важно правильно определиться с выбором технологий, используемых для разработки конечного продукта.

5. Запуск и сопровождение, SEO-оптимизация. Это последний этап разработки Web-приложений, на нём исправляются ошибки, допущенные в процессе разработки, созданный Web-продукт размещается в Интернете. После этого осуществляется поддерживание стабильности Web-ресурса, которая заключается в обновлении сайта, устранении различных ошибок, выявленных в процессе эксплуатации и т. д. SEO-оптимизация (поисковая оптимизация) – это меры, направленные на то, чтобы увеличить посещаемость Web-ресурса, за счёт повышения его позиций в выдаче поисковых систем по заданному набору целевых запросов [2].

Для создания надёжной и эффективной системы необходимо правильно подойти к выбору соответствующих технологий для её создания.

Существует очень много различных технологий для создания Web-приложений, каждая из которых имеет свои преимущества и недостатки по сравнению с остальными. Для описания содержимого Web-страницы и построения интерфейса пользователя используются следующие инструменты.

1. HTML (Hypertext Markup Language – расширяемый язык разметки), основу которого составляет фиксированный набор тегов и атрибутов, описывающий свойства содержащихся на странице элементов.

2. XML (Extensible Markup Language – расширяемый язык разметки), который также оперирует тегами и атрибутами, но, в отличие от HTML, в котором набор тегов и атрибутов является фиксированным, в XML их число определяется типом создаваемого документа. Существует также язык XHTML (Extensible Hypertext Markup Language – расширяемый язык разметки гипертекста), который создан на базе XML и является аналогом HTML.

3. CSS (Cascading Style Sheets – каскадные таблицы стилей), отвечает за внешний вид Web-страницы, какие стили будут применены к тому или иному элементу. CSS позволяет придать Web-странице более красивый вид, что может помочь расположить пользователя к созданному Web-ресурсу [3].

4. JavaScript – язык программирования, с помощью которого можно добавить анимацию на страницу, сделать её более отзывчивой к действиям пользователя. Например, JavaScript можно использовать при создании меню,

слайдеров и т. д. Чтобы сократить время и использовать больше возможностей JavaScript, для него существуют разнообразные фреймворки, которые представляют собой каркас, объединяющий в себе несколько компонентов, призванных облегчить разработку системы. Одними из самых известных фреймворков для JavaScript являются React, Angular, Vue.

Для создания серверной части приложения, которая реализует логику работы приложения, используются серверные языки программирования и фреймворки. Для написания серверной части используются следующие технологии.

1. PHP (Hypertext PreProcessor, «препроцессор гипертекста»). Основной язык программирования для разработки различных Web-проектов, который создавался именно для этих целей. Задача PHP заключается в выполнении определённого сценария в соответствии с запросом пользователя и генерации готовой Web-страницы, которая будет отображена в браузере. Среди фреймворков для PHP можно выделить: Laravel, Symfony, Yii2, CodeIgniter и др.

2. Java. Является универсальным языком программирования. Java также часто применяется для Web-разработки, поскольку Web-приложения, написанные на Java, являются кроссплатформенными, мультифункциональными, а также надёжными и гибкими. Самым популярным фреймворком для разработки Web-приложений на Java является Spring. Именно на нём делается большинство Web-приложений на Java, так как он является наиболее удобным для этого и основное его преимущество – это возможность разработки Web-приложения в виде набора слабосвязанных компонентов. При этом желательно, чтобы каждый из компонентов обладал минимальными знаниями о другом. Это позволяет очень сильно упростить процесс разработки Web-приложения, а также поддерживать его функциональные возможности в будущем. Конечно, помимо Spring существуют и другие фреймворки для данного языка, такие как JSF, Vaadin, GWT и др., но они не обрели такой популярности как Spring и для Web-разработки ими пользуются реже.

3. Node.js. Представляет собой кроссплатформенную среду, позволяющую выполнить JavaScript-код вне браузера. На сервере Node.js позволяет запустить сценарии, которые обрабатывают динамическое содержание Web-страницы, после чего она отображается в браузере пользователя [4].

4. Python. Для Python также существует много различных фреймворков, а также микрофреймворков. Самым известным фреймворком для Web-разработки на данном языке является Django. Django является open source проектом, то есть свободно распространяемым и с открытым исходным кодом. Он предоставляет разработчикам очень большие возможности для быстрого создания масштабных Web-продуктов. В нём изначально реализована панель администратора, работа с базами данных в виде ORM, кроме того, Django имеет встроенную защиту от атак на сайты. Всё это делает данный

фреймворк одним из самых лучших для разработки больших и сложных решений. Однако данный фреймворк не стоит выбирать в качестве инструмента разработки для создания небольших проектов. Использование Django в этом случае будет избыточно и более рациональным решением будет выбор другого фреймворка, либо же микрофреймворка. Например, для этой задачи отлично подойдёт Flask. Flask позволяет разработчику запускать локальный сервер, обрабатывать поступающие от пользователя запросы, обрабатывать шаблоны и т. д. Преимуществами данного фреймворка является его простота, гибкость, хороший инструментарий для тестирования. Недостатками является то, что фреймворк не поддерживает асинхронность, то есть каждый новый запрос блокирует поток на время, пока он не выполнится. Это может негативно сказаться на работе Web-приложения, в случае, если будет поступать очень много запросов пользователей. Существуют также другие фреймворки для дданного языка, например, Pyramid, Turbo-Gears, Web2py, но они не имеют такой популярности как Django [5].

5. Ruby. Данный язык появился с целью добавить в программирование функциональность и естественность. Для Web-разработки на Ruby используется среда Web-приложений Ruby on Rails. Данный фреймворк стал одним из самых популярных для Web-разработки. Он позволяет программистам быстро создавать Web-приложения различной сложности, поскольку прост и лёгок в процессе разработки. Использует архитектуру MVC и маршрутизацию [6].

Для Web-разработки наиболее распространёнными базами данных являются MySQL, PostgreSQL и MongoDB [4]. Существует ещё очень много различных систем управления базами данных (СУБД), таких как Oracle, Sqlite, Google Cloud Spanner и пр.

Список используемых источников

1. Web-приложение. URL: https://semantica.in/blog/veb-prilozhenie.html (лата обращения: 07.03.2022).

2. Основные этапы разработки web-приложений. URL: http://www.rusnauka.com/16_ADEN_2011/Informatica/3_85389.doc.htm (дата обращения: 07.03.2022).

3. Базовые элементы Web-технологий. URL: http://panda.ispras.ru/~kuliamin/lectures-wtp/Basic%20Web%20Technologies.pdf (дата обращения: 07.03.2022).

4. Алёна Терентьева. Стек технологий для разработки Web-приложений: что важно знать бизнесу. URL: https://www.azoft.ru/blog/web-development-stack/ (дата обращения: 09.03.2022).

5. 10 Web-фреймворков Python, с которыми стоит работать в 2018 году. URL: https://habr.com/ru/company/skillbox/blog/420119/ (дата обращения: 09.03.2022).

6. Web-разработка на Ruby: лучший язык для создания Web-сайтов. URL: https://bestprogrammer.ru/programmirovanie-i-razrabotka/veb-razrabotka-na-ruby-luchshij-yazyk-dlya-sozdaniya-veb-sajtov (дата обращения: 10.03.2022).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной

УДК 004.032.26
ГРНТИ 28.23.37

ОБЗОР И АНАЛИЗ МОДЕЛЕЙ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ ДЛЯ СОЗДАНИЯ УНИКАЛЬНЫХ ОБЪЕКТОВ ИЗОБРАЗИТЕЛЬНОГО ИСКУССТВА

Е. В. Баягантаева, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлен обзор и анализ моделей генеративно-состязательных сетей для создания уникальных объектов изобразительного искусства. Статья содержит описание особенностей их архитектуры, представлены примеры генерируемых изображений, проведен анализ их преимуществ в использовании. Применение данных моделей дает возможность не только для творческого выражения человека, но и для использования сгенерированных объектов в создании рекламной продукции, дизайна книжных изданий, одежды и др.

нейронные сети, генеративно-состязательные сети, генерация изображений.

Генеративно-состязательные сети (ГСС) были впервые описаны Яном Гудфеллоу в 2014 году [1]. Они представляют собой алгоритм машинного обучения без учителя, построенного на комбинации из двух нейронных сетей, одна из которых (сеть G или генератор) создает образцы, а другая (сеть D или дискриминатор) отсеивает те, что не принадлежат к рассматриваемому классу (рис. 1).

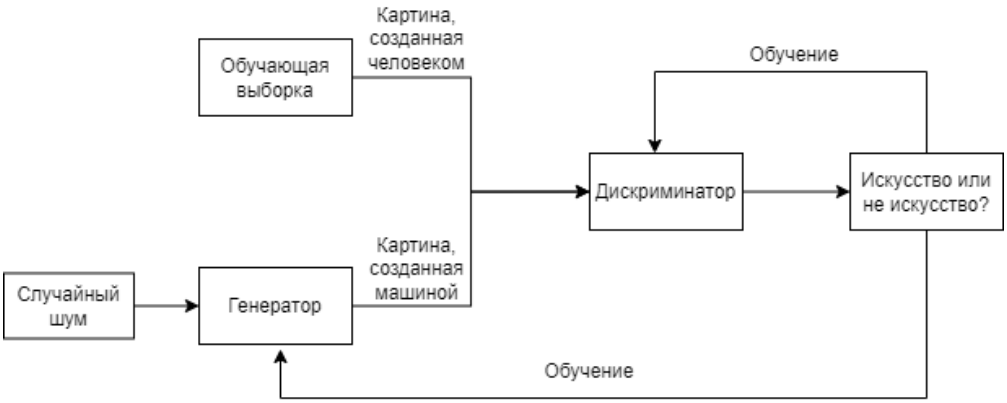


Рис. 1. Схема работы генеративно-состязательной сети

Целью настоящей работы является обзор и анализ моделей генеративно-состязательных сетей для создания уникальных объектов изобразительного искусства.

Объектом исследования являются модели генеративно-состязательных сетей, обладающие различными модификациями.

Задачи исследования:

- Поиск моделей генеративно-состязательных сетей,
- Выбор моделей, специализирующихся на генерации объектов изобразительного искусства,
- Описание выбранных моделей,
- Указание их преимуществ в использовании.

Проблемами классической ГСС являются [2]:

- Схлопывание мод распределения: генератор выдает ограниченное количество разных образцов.
- Проблема стабильности обучения: параметры модели дестабилизируются и не сходятся.
- Проблема запутывания: выявление корреляции в признаках, не связанных (слабо связанных) в реальном мире.

Одной из моделей ГСС, демонстрирующей решение проблемы схлопывания мод распределения, является креативно-состязательная сеть. Она имеет архитектуру, представленную на рис. 2.

Авторами сети являются Эльгаммал А., Лью Б., Элхосейни М. и Мацконе М. [3]. Статья, содержащая описание работы сети, имеет название «CAN: креативно-состязательные сети, генерирующие «Искусство» путем изучения стилей и отклонения от стилевых норм», опубликована 21 июня 2017 г.

Рис. 2. Схема работы креативно-состязательной сети

Основной особенностью генерирования является наличие в архитектуре меток стиля, увеличивающих вариативность создаваемых изображений.

Дискриминатор креативно-состязательной сети имеет доступ к набору произведений искусства, объединенных метками по стилям искусства (Ренессанс, Барокко, Импрессионизм и т. д.), который служит его обучающей выборкой для различения стилей.

Полученные изображения продемонстрированы рис. 3.

Сгенерированные изображения данной нейронной сети и генеративно-состязательной сети были оценены фокус-группой на предмет того, насколько от 1 до 5 она находит их привлекательными, оригинальными и др. Объекты, созданные креативно-состязательная сетью, набрали средний балл равный 3.2, конкурентная сеть – 2.8.

Рис. 3. Сгенерированные изображения креативно-состязательной сети

Следующей рассматриваемой моделью ГСС является модель генеративно-состязательной сети Вассерштайна.

Генеративно-состязательные сети Вассерштайна, или сокращенно ГССВ, были представлены Мартином Аржовски и др. в статье «Wasserstein GAN» в 2017 г. [4].

Используя в качестве функции дивергенции метрику Вассерштейна, данная модель демонстрирует решение проблемы стабильности обучения.

Потенциал применения ГССВ для создания объектов искусства был изучен в магистерской диссертации Бермана А. «Генеративно-состязательные сети для создания объектов искусства», опубликованной 1 января 2020 г. [5].

Пилотное проведение разработанной автором системы оценок сгенерированных изображений было организовано с участием 20 пользователей. ГССВ достигла более высоких оценок качества изображений (рис. 4), чем ГСС.

Рис. 4. Сгенерированные изображения генеративно-состязательной сети Вассерштайна

Решение проблемы запутывания предложено в статье Галаноса Т., Лиаписа А., Яннакакиса Г. «AffectGAN: гене-

ративное искусство, основанное на аффектах, управляемое семантикой», опубликованной 30 сентября 2021 г. [6].

В статье представлен метод создания художественных образов, выражающих определенные аффективные состояния. Используя современные методы глубокого обучения для визуальной генерации, семантические модели из OpenAI и набор данных из энциклопедии изобразительного искусства WikiArt, модель AffectGAN способна генерировать изображения на основе семантических подсказок и предполагаемых аффективных результатов.

Основными компонентами архитектуры являются нейронные сети CLIP и VQGAN (рис. 5).

CLIP (Contrastive Language–Image Pre-training) – мультимодальная сеть, способная оценить изображение и соотнести, подходит ли к ней подпись или наоборот.

VQGAN (Vector Quantized Generative Adversarial Network – это генеративно-состязательная нейросеть, которую используют для создания новых изображений на основе обучающей выборки.

Работая вместе, VQGAN генерирует изображение, а CLIP выступает как ранжировщик, оценивая, насколько изображение подходит тексту.

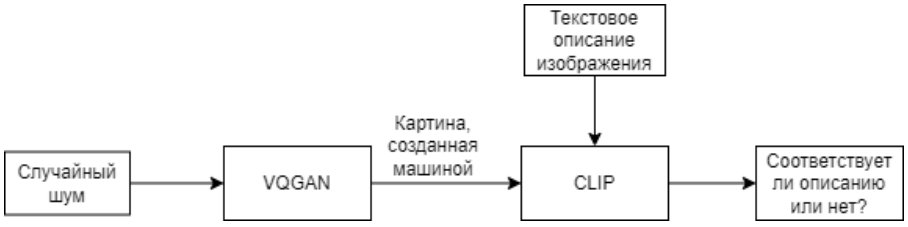


Рис. 5. Схема работы генеративно-состязательной сети AffectGAN

Набор 32 изображений, сгенерированных AffectGAN (рис. 6), оценен 50 участниками с точки зрения эмоций, которые они вызывают. Результаты показывают, что в большинстве случаев предполагаемая эмоция, используемая в качестве подсказки для создания изображения, соответствует ответам участников.

Рис. 6. Сгенерированные изображения генеративно-состязательной сети AffectGAN

В заключение необходимо отметить, что представленные модели генеративно-состяза-

тельных сетей решают основные проблемы классической ГСС. Результат их работы считается приемлемым для применения в рамках темы проводимой исследовательской работы – Алгоритм генерации визуального образа книжных изданий на базе нейронных сетей.

Список используемых источников

1. Генеративно-состязательная сеть // Википедия: свободная энциклопедия. 5 сентября 2021 г. URL: https://ru.wikipedia.org/wiki Генеративно-состязательная_сеть (дата обращения: 01.02.2022).

2. Generative Adversarial Nets (GAN) // Викиконспекты; науч.-метод. архив. Университет ИТМО. 24 января 2021 г. URL: https://neerc.ifmo.ru/wiki/index.php?title=Generative_Adversarial_Nets_(GAN) (дата обращения: 01.02.2022).

3. Elgammal A., Liu B., Mazzone M. CAN: Creative Adversarial Networks, Generating "Art" by Learning About Styles and Deviating from Style Norms // arXiv: науч.-метод. архив. 21 июня 2017 г. URL: https://arxiv.org/pdf/1706.07068.pdf (дата обращения: 10.02.2022).

4. Arjovsky M., Chintala S., Bottou L. Wasserstein GAN // arXiv: науч.-метод. архив. 26 января 2017 г. URL: https://arxiv.org/abs/1701.07875 (дата обращения: 10.02.2022).

5. Berman A. Generative Adversarial Networks for Fine Art Generation // OpenUCT: науч.-метод. архив. 24 января 2020 г. URL: https://open.uct.ac.za/bitstream/handle/11427/32458/thesis_sci_2020_berman_alan.pdf?sequence=1&isAllowed=y (дата обращения: 15.02.2022).

6. Galanos T., Liapis A., Yannakakis G. AffectGAN: Affect-Based Generative Art Driven by Semantics // arXiv: науч.-метод. архив. 30 сентября 2021 г. URL: https://arxiv.org/pdf/2109.14845 (дата обращения: 20.02.2022).

УДК 004
ГРНТИ 20.15.13

ИСПОЛЬЗОВАНИЕ ЧАТ-БОТОВ ДЛЯ АВТОМАТИЗАЦИИ БИЗНЕС ПРОЦЕССОВ

С. Г. Бедняк, А. А. Кузнецова, А. А. Федулова

Поволжский государственный университет телекоммуникаций и информатики

Чат-боты все больше пользуются популярностью среди простых обывателей. Компании все чаще стремятся перевести рутинные процессы в автоматический режим и облегчить ведение бизнеса, отдавая чат-боту хотя бы ответы на часто задаваемые вопросы от клиентов или партнеров. Но чем больше бизнес процессов протекает внутри компании, тем сложнее контролировать все вручную. Тут на помощь и приходят чат-боты.

чат-бот, автоматизация, бизнес.

Регулярно меняющиеся условия рынка, повышенная скорость принятия решений, многозадачность в управлении и потребность снижения рисков заставляют искать современные подходы к организации бизнес процессов. Чат-боты позволяют предприятию куда более качественно располагать временем, ведь какие-то простые или рутинные вопросы возможно уверенно возложить на плечи алгоритмов. Помимо этого, работа с разработанным непосредственно с целью определенного бизнеса ботом во значительном близко работе с умным и хорошо подготовленным личным ассистентом. В настоящее время все большое количество организаций и компаний, в том числе некоммерческих и бюджетных, стремятся внедрить технологию чат-ботов в свои бизнес-процессы, что может оптимизировать процессы сбора информации и позволит сократить штат работников [1, с. 85]. Если потребуется поменять время совещания или встречи, или быть может и вовсе отменить их – чат-бот без труда справится с этой задачей. К тому же, чат-боты могут помочь автоматизировать бизнес-процессы, осуществляя контроль и координируя работу одновременного нескольких отделов предприятия. На сегодняшний день технологии чат-ботов находятся в области пика завышенных ожиданий и зачастую применяются не в силу необходимости, а потому что это тренд, и они не требуют каких-либо существенных затрат [2, с. 159]. Они могут уведомить участников проекта об окончании исполнения установленной проблемы, или возможно запрограммировать их для ответов на часто задаваемые вопросы как клиентами, так и сотрудниками самой компании. С каждым днем возможности чат-ботов только расширяются, все зависит только от потребностей.

Для маленьких компаний или только начинающих предпринимателей не обязательно иметь в штате конкретного человека, который сможет написать программу для требуемого чат-бота, достаточно лишь найти подходящий сервис, где можно самому сконструировать бота даже не имея навыков программирования. Однако, такие боты не могут похвастаться развитым функционалом или способностью выдерживать большие нагрузки. Все же, чем объемнее компания, тем больше ее функций требуют оптимизации и автоматизации.

Функции чат-бота для бизнес-процессов:

1. Поддержка клиентов

Чат-бот сможет помочь сменить неудобный FAQ на сайте, так как пользователь иногда не может сразу найти ответ на свой вопрос. Бот может работать 24 часа в сутки, поможет ответить на типовые вопросы клиентов и разгрузит сотрудников.

2. Клиентский сервис

С помощью чат-бота возможно совершать покупки и запрашивать услуги. С постоянным расширением ассортимента, сложнее искать определенные продукты. После небольшого анализа бот поймет, что интересует клиента, и отправит прямую ссылку.

3. Маркетинг

Чат-бот – это еще один маркетинговый инструмент, который поможет распространять контент, поддерживать клиентов и собирать аналитику. С помощью него возможно совершать рассылки, оповещать покупателей об акциях, собирать комментарии о товарах или услугах, качестве обслуживания.

4. Работа внутри компании

Чат-боты могут помочь оптимизировать в работе такие процессы как: бронирование перемещений для переговоров, оповещение работников о датах отпуска, расписание корпоративного транспорта, сроки зарплаты и многое другое.

Чат-бот практичный и универсальный ассистент, который сбережет кучу рабочего времени и сможет помочь быстрее реагировать на запросы клиентов. Согласно определенным иностранным опросам около 35% потребителей хотели бы, чтобы компании чаще использовали чат-ботов.

Кроме того, чат-боты выполняют множество полезных функций по исполнению рутинных операций, поиску информации, объединению данных, работе с клиентурой. Чат-бот как виртуальный собеседник имеет базу знаний, которая представляет собой наборы возможных вопросов пользователя и соответствующих им ответов. Наиболее распространенными вариантами для получения нужного ответа являются ключевые слова, совпадение фразы, совпадение контекста [3, с. 195].

Плюсы в разработке чат-бота для компании распространяются не только на внутренние бизнес-процессы, но и на индустрию в целом. Так, вскором будущем интегрированные в бизнес чат-боты смогут:

– сократить операционные издержки;
– оптимизировать и повысить эффективность бизнес-процессов;
– снизить рабочее давление;
– непрерывно самосовершенствоваться;
– стать неотъемлемой частью команды.

Чат-боты – это именно тот редкий случай, когда бизнес сам идет навстречу своим клиентам в максимально комфортном и удобном для потребителя формате, и при этом все еще и получает прибыль (рис. 1):

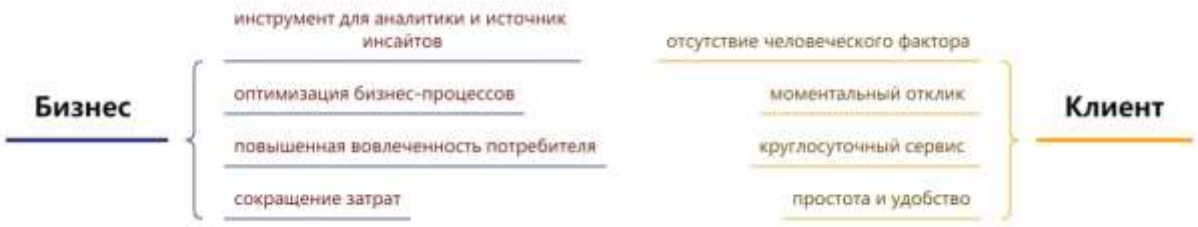


Рис. 1. Чат-бот для бизнеса и для клиента

Существует несколько вариантов классификации чат-ботов, выделим два вида: бизнес-классификация чат-бот приложений (рис. 2) и классификация чат-ботов по техническому типу (рис. 3).

Рис. 2. Бизнес-классификация чат-ботов

Рассмотри каждый тип более подробно:

- Разговорные – созданы для общения, очень похожи на общение с обычным человеком, не имеют конкретной цели.
- Ассистенты – исходя из конкретных целей, из пользовательских ответов извлекают необходимые данные.
- Q&A(вопрос-ответ) – принцип работы: один вопрос – один ответ.

Рис. 3. Техническая классификация чат-ботов

Рассмотрим каждый тип более подробно:

- Основанные на бизнес-правилах.

В этом типе диалог человека и бота предварительно продуман разработчиком и имеет дерево-подобную структуру. Огромное количество клавиш приводит человека к определенному концу. В данном типе вопросов с ответом в свободной форме не существует.

- Основанные на искусственном интеллекте.

Не имеют предопределенную структуру. Путь разговора установлен на базе тестируемых сведений, которые применялись с целью обучения модели машинного обучения. Подобные боты обязаны обладать большим объемом данных для качественной работы.

- Гибридные.

Этот тип включает в себя взаимодействия, основанные на бизнес-правилах и на искусственном интеллекте. Разговор с пользователем ведется по предопределенному пути, но используется искусственный интеллект для определения намерений пользователя, и извлечения данных из переписки.

Подводя итоги всего описанного выше, можно сделать выводы о том, что активное использование чат-ботов для автоматизации бизнес процессов ускоряет работу компании, обеспечивает лучшее взаимодействие как внутри компании, так и с потребителями их продукции, что в настоящее время крайне важно, ведь темп жизни людей не стоит на месте.

Список используемых источников

1. Сметкина О. М., Травин Д. Н. Использование чат-ботов в качестве средства оптимизации бизнес-процессов // Цифровая конвергенция в экономике и управлении: Сборник научных трудов / Под редакцией В. В. Трофимова, В. Ф. Минакова. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2020. С. 83–91.

2. Екатериничев А. Л., Антоненко Н. А., Бабаев А. Б., Наташкина Е. А. Области эффективного применения чат-ботов // Информационные технологии в экономике и управлении: Сборник материалов IV Всероссийской научно-практической конференции (с международным участием), Махачкала, 11–12 ноября 2020 года. Махачкала: Типография ФОРМАТ, 2020. С. 158–162.

3. Тарасова Н. С., Сергеева Н. Ю. Использование чат-ботов в повседневной жизни // Вестник современных исследований. 2017. № 12-1 (15). С. 195–197.

УДК 654.739
ГРНТИ 49.33.29

РЕЛЕВАНТНОСТЬ МОНИТОРОВ С ВЫСОКОЙ ЧАСТОТОЙ, КАК УСТРОЕНО ЧЕЛОВЕЧЕСКОЕ ЗРЕНИЕ

П. А. Берестовский, А. В. Глебов, А. С. Гусев, В. Г. Иванов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Данная статья посвящена разоблачениям популярных заблуждений о работе монитора, принцип работы человеческого глаза, зависимость герцовки экрана и видеокарты компьютера. Влияние использования в играх рассматривается как теория, так и примеры реализации, а, так же анализ дальнейшего развития нейросетей в различных сферах.

мониторы, количество кадров в секунду, работа глаз человека.

В настоящее время большое количество людей до сих пор не разбираются в мониторах, их частоте кадра и зависимости плавности кадра, как от железа, так и от свойств монитора. Основной миф заключается в том, что, если система показывает 60 кадров в секунду в секунду (FPS) в, то и брать монитор выше 60 герц смысла не имеет. Статей на подобную тематику много, но в части из них рассказывают про откровенную ересь, и я решил раз и навсегда разобраться в вопросе, без всяких исторических справок про 24 кадра, как развивалось телевидение, а четко, понятно и с позиции физиологии.

Система взаимодействия между игровым симулятором и восприятием. Данная система состоит из 4 основных составляющих, представленных на рис. 1 [1].

Рис. 1. Элементы системы взаимодействия между игровым симулятором и восприятием

На рис. 1 представлено:

1. Видеокарта генерирует определенное количество FPS.

2. Монитор, отображающий с некоторым количеством герц.

3. Человеческий глаз, который воспринимает, то что показано на мониторе и создаёт нервный импульс.

4. Стриарная кора головного мозга она же зрительная кора.

Есть нюансы, но для данного случая этих данных достаточно. Что бы всё понять разбираться будем в обратном порядке от мозга к видеокарте. У нашего мозга есть условная величина восприятия кадров в секунду, но у неё есть примерная численная характеристика, она показывает кадр какой минимальной продолжительности наш мозг может заметить и распознать, или можно сказать наоборот какая частота кадров в секунду должна быть чтобы наш мозг, в этой череде кадров сумел вычленить хотя бы один. И это не 24 и даже не 120, а где-то 200-250. Многое зависит от условий, того как выглядит то на что мы смотрим, но крупное темное пятно на светлом фоне среднестатистический человек ловит даже при 250 FPS. Профессиональные лётчики могут при такой частоте даже угадать модель самолета, которую им показывают, что наглядно показывает предел FPS человеческой зрительной коры. Данный показатель является индивидуальным и тренируемым, но практически не существует людей, которые не различали 1 кадр из 150, так же существуют люди, которые способны улавливать 1 кадр из 400 [2].

Спускаемся на следующую ступень системы человеческий глаз. Вот тут в научно-популярной литературе возникает больше всего ошибок, часто пишут, что FPS глаза примерно 50-100. Фоторецептор нашего глаза палочки и колбочки представлены на рисунке 2.

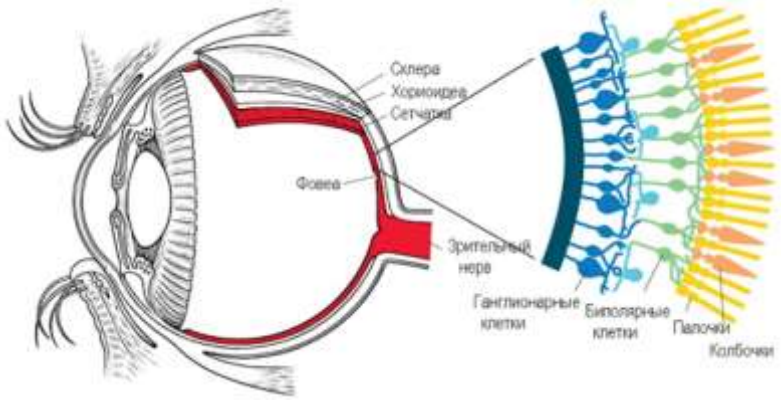


Рис. 2. Расположение фоторецепторов глаза

Палочки и колбочки расположены на сетчатке имеют период рефрактерности или если хотите инертность – это время которое приходит от одного перехода возбуждения фоторецептора до другого. Это время примерно равно 20 миллисекундам. Люди берут делят 1 000 миллисекунд из которых состоит секунда, вот на эти самые 20 миллисекунд задержки и получают как

раз 50 кадров в секунду который якобы может распознать наш глаз. А теперь необходимо осознать важнейшую вещь, это работа не целого глаза, а лишь одного рецептора, а в каждом глазу таких рецепторов около 140 миллионов, 7–8 миллионов колбочек и в районе 130 миллионов палочек. Все эти элементы работают не одновременно как затвор фотоаппарата, а в абсолютный разнобой, при поступлении фотонов света палочка или колбочка гиперполяризовалась, сгенерировала импульс, и отправила его по нейрону дальше. Наш глаз, а точнее наша сетчатка с чудовищной частотой создаёт нервные импульсы, каждый импульс – это лишь мельчайший фрагмент целого изображения. Между рецепторами есть горизонтальные связи, есть дополнительные глиальные клетки и в итоге мозг поступает конечно не 140 миллионов сигналов, от каждой колбочки, а примерно раз в 50–100 меньше, но все ровно в наш мозг в секунду прилетает сильно больше миллиона импульсаций из каждого глаза, и на их основе строится уже полноценное изображение. Иными словами, FPS глаза – это очень условная величина, так как глаз не затвор фотоаппарата, он работает совсем иначе, но при этом если говорить об FPS глаза, то он на столько огромен что во всей системе передачи изображения от видеокарты до мозга, он является самым широким местом. В тысячи больше раз больше чем другие элементы поэтому в рамках это системы можно сказать, что глаза вообще нету привычных нам кадров в секунду, а передается по сути непрерывный поток информации без какой-либо разбивки по кадрам [3].

Следующая ступень это одно из самых узких мест нашей фотосистемы, монитор. Монитор всегда показывает ровно вот то число кадров в секунду, которая написана в руководстве, в FPS совпадает с количеством герц. Сколько бы FPS не генерировала бы видеокарта. В этом и заключается следующее заблуждение строиться по следующим суждениям. Раз монитор может показывать только 60 кадров, значит не нужно что бы игра генерировала больше кадров потому что упрется в пределы возможности монитора. Да больше монитор не покажет, но что именно монитор покажет в случае, когда видеокарта показывает 30, 60 и 120 FPS, будет очень сильно отличаться. Так как есть задержка изображения.

Например, монитор показывает 60 FPS, то есть между двумя кадрами 1/60 FPS, представим этот кусок как отрезок если видеокарта будет создавать 30 FPS, то внутри отрезка 1/60 секунды может вообще не попасть не одного нового кадра, и монитор покажет два одинаковых кадра. В случае если видеокарта создает 60 FPS, то каждый то на 1 кадр монитора 100% попадёт 1 кадр с видеокарты, но он может стоять в самом начале временного интервала. Разница между количеством FPS от герцовки монитора показана на рис. 3 [4].

Рис. 3. Разница изображений между мониторами с разным количеством герц

И отобразиться только через 1/60 секунды. Если 120 FPS, то во внутрь интервала попадет уже 2 кадра, но все равно, второй кадр может стоять в центре временного промежутка и до его отображения пройдет 1/120 секунды, и чем больше FPS создаёт игра, тем большее число кадров анимации попадает в интервал между двумя кадрами на мониторе, интервал как бы разбит, но большое число кадров анимации и значит каждое следующее обновление изображение на мониторе будет содержать или актуальную картинку сгенерированной игрой, и возникает логичный вопрос если у монитора 60 кадров, какая разница, на вид её нельзя заметить и спорить тут бессмысленно, для наблюдателя со взгляда со стороны на этот экран будет выдаваться практически одна и та же картинка. Но для пользователя она вполне ощутимо в первую очередь это сказывается на ощущение в симуляторе стрельбы. [5].

В играх от первого лица можно с помощью мыши без проблем сделать 2 оборота вокруг своей оси, и на эти 2 оборота у нас будет всего 60 кадров анимации, картинка в каждом кадре будет сильно отличатся и мозг это прекрасно почувствует, но подстроится и создаст вам плюс-минус плавную картинку, а вот под что ваш мозг не подстроиться, это под отставание кадра от движения руки, при быстрых движениях можно очень четко осознать, что картинка немножко запаздывает, в худшем случае вот на 1/60 секунды. Вроде бы это мало, но мозг может спокойно различать кадры длиной в 1/200 секунды, это временной интервал, с которым наш мозг вполне умеет работать, и чем более быстрое движение мы совершаем в игре. Чем на чем на большую дистанцию смещается курсор, тем больше нам больше будет казаться, что картинка запаздывает по отношению к движению мышки. Если за 1/60 секунды мы плавно сместили курсор на пару миллиметров, то монитор покажет близкие друг к другу кадры и будет казаться, что отставания почти нету. А вот если мы постоянно с большой скоростью изменяем положение курсора, то при низких FPS симулятора у пользователя будет постоянное ощущение отставания движения картинки от движения руки, это почто то же самое ощущение, как при включенной вертикальной синхронизации. Вроде бы на экране все плавно, но при резком отведении мыши в

сторону картинка сильно смазывается «будто в молоке», движение большое, а смещение меньше чем мы ожидали. Для наблюдающего же со стороны никакой разницы на экране нет всё плавно и при 60 и при 120 кадрах, а вот игрок руками всё прекрасно чувствует так как есть задержка между движением мышки и картинкой на экране потому что визуальная разница между тем где, по нашему мнению, должен быть курсор или прицел, и тем где он находиться тем больше, чем с большей скоростью мы смещаемся.

Исходя из выше изложенных фактов, киберспортсмены рвутся за максимальным FPS и максимальной герцовке монитора, ведь это действительно влияет на геймплей. А если учесть, что до сих пор есть симуляторы где действия завязаны на числе кадров секунду то все упирается в железо персонального компьютера. Нужно ли всем гнаться за FPS и герцами? нет! Если вы играете в спокойные игры и не вертите там со «скоростью звука» мышкой, переплачивать за дорогую технику бессмысленно разницу можно будет почувствовать, но для этих задач это будет не критичной и не обязательной. А вот в симуляторах стрельбы и прочих быстрых играх, то разница уже критична она может влиять на результат вашей игры и еще не забывайте, что у монитора есть время между нажатием кнопки и отображением результата на экране.

Список используемых источников

1. Сайт исследования Nvidia – FPS и герцы влияют на вашу игру. URL: https://rbkgames.com/publications/articles/fps-hz-nvidia-research/ (дата обращения: 15.01.2022)

2. Сайт Мониторы с частотой 144, 240, 360 Гц: дают ли они реальные преимущества. URL: https://yandex.ru/turbo/ichip.ru/s/sovety/pokupka/vysokogercovye-monitory-v-igrah-i-video-739872 (дата обращения: 16.01.2022)

3. Сайт Правда, мифы и особенности игровых мониторов. URL: https://www.iguides.ru/main/other/razbiraemsya_s_igrovymi_monitorami_chastoty_vremya_otklika_freesync_i_g_sync/ / (дата обращения: 17.01.2022)

4. Сайт мифы о мониторах 144-240 Гц на примере LG 27GK750F. URL: https://investgazeta.ru/tehno-cifra/na-chto-vliyaet-gercovka.htm (дата обращения: 18.01.2022)

5. Сайт ЭЛТ-монитор в 2021 году. URL: https://habr.com/ru/company/kaspersky/blog/569856/ (дата обращения: 19.01.2022)

УДК 004.89
ГРНТИ 28.23.37

АНАЛИЗ ВОЗМОЖНОСТЕЙ БИБЛИОТЕКИ PYAUDIO НА ПРИМЕРЕ СОЗДАНИЯ МОДЕЛИ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ ГОЛОСА

П. П. Бовшик, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель работы – исследовать возможности библиотеки PyAudio на примере создания модели глубокого обучения для распознавания голоса. В последнее время машинное обучение имеет большую популярность, модели глубокого обучения используют во многих сферах жизнедеятельности человека, например, для минимизации рисков, простоев и выявления угроз безопасности на предприятиях и не только, для распознавания объектов на камерах видеонаблюдения, распознавания голоса при создании мобильного оператора-бота или голосового ассистента, такого как Siri или Алиса. В данном докладе рассмотрена одна из самых популярных и простых в применении библиотек глубокого обучения PyAudio. На базе данной библиотеки создана простейшая модель по распознаванию объектов на языке Python.

глубокое машинное обучение, распознавание голоса, Python, библиотека PyAudio.

Современные системы распознавания могут распознавать речь от нескольких носителей и имеют огромный словарный запас на разных языках. При этом речь должна быть преобразована из физического звука в электрический сигнал с помощью микрофона, а затем цифровые данные можно использовать для транскрибирования аудио в текст. Рассмотрим необходимые для этого библиотеки.

В **PyPI** существует несколько пакетов для распознавания речи. Некоторые из этих пакетов, например, wit и apiai [1, 2], предлагают встроенные функции, такие как обработка на естественном языке для определения намерений говорящего, которые выходят за рамки базового распознавания речи. Другие, такие как google-cloud-speech, сосредоточены исключительно на преобразовании речи в текст. Существует также один пакет, который отличается простотой использования – SpeechRecognition.

Для распознавания речи требуется аудиовход, а SpeechRecognition делает его очень простым. Вместо того, чтобы создавать сценарии для доступа к микрофонам и обработки аудиофайлов с нуля, SpeechRecognition обеспечит работу всего за несколько минут.

Библиотека SpeechRecognition [4] действует как оболочка для нескольких популярных речевых API и, таким образом, является чрезвычайно гибкой. Гибкость и простота использования пакета SpeechRecognition делают его отличным выбором для любого проекта Python.

Преобразование текста в речь (TTS) – это своего рода синтез речи, который преобразует набранный текст в слышимый человеческий голос.

Существует несколько синтезаторов речи, которые можно использовать с Python. В рамках данного доклада рассмотрим Google Text-to-Speech(gTTS).

gTTS – это библиотека Python и инструмент CLI для взаимодействия с API преобразования текста в речь Google Translate [5]. Записывает произносимые mp3 данные в файл, файлоподобный объект (bytestring) для дальнейшей обработки звука или stdout. Также позволяет предварительно сгенерировать URL-адреса запросов Google Translate TTS для отправки во внешнюю программу.

Библиотека gTTS имеет свои особенности, такие как:

- Настраиваемый токенизатор предложений для конкретной речи, который позволяет читать неограниченное количество текста, сохраняя при этом правильную интонацию, аббревиатуры, десятичные дроби и многое другое.
- Настраиваемые текстовые предпроцессоры, которые могут, например, корректировать произношение.
- Отличается гибкой предварительной обработкой и маркировкой.
- Постоянно нужен быстрый интернет.
- Нельзя воспроизвести аудио средствами самого gTTS.
- Скорость обработки текста ниже, чем у офлайн-синтезаторов.

PyAudio – это привязка Python для PortAudio, кроссплатформенной библиотеки для ввода и вывода аудио [3].

PyAudio записывает полученный аудио поток в объекты типа bytes. В последующем данные могут быть сохранены в виде файлов WAV.

Данная библиотека имеет широкий спектр функций, связанных со звуком и в основном ориентированных на сегментацию, извлечение функций, классификацию и визуализацию:

Используя библиотеку PyAudio, пользователи могут классифицировать неизвестные звуки, выполнять контролируемую и неконтролируемую сегментацию, извлекать звуковые функции и представления, обнаруживать звуковые события и отфильтровывать периоды тишины из длинных записей, применять уменьшение размерности для визуализации аудиоданных и сходства контента и многое другое.

Эта библиотека предоставляет привязки для PortAudio. Пользователи могут использовать эту библиотеку для воспроизведения и записи звука на разных платформах.

```
import speech recognition as sr
import os
import sys
import webbrowser

def talk(words):
  print(words) # Дополнительно выводим на экран
  os.system("say " + words) # Проговариваем слова

talk("Привет, чем я могу помочь вам?")

sr = speech_recognition.Recognizer()
sr.pause_threshold = 1 #пауза между непрерывной речью

commands_dict = {
    'commands': {
        'greeting': ['представься', 'кто ты'],
        'create_task': ['добавить задачу', 'создать задачу', 'заметка'],
        'open_website': ['открыть сайт', 'сайт']
    }
}

def listen_command:
  try:
          with speech_recognition.Microphone() as mic:
                  sr.adjust for ambient noise(source=mic, duration=0.5) #для учета уровня
шума
                  audio = sr.listen(source=mic) #слушать микрофон
                  query = sr.recognize_google(audio_data=audio, language='ru-RU').lower()
#распознавание речи на русском языке в нижнем регистре
          return f'Вы сказали: {query}'
  exept speech recognition.UnknownValueError:
          talk("Ошибка распознавания")

def greeting():
  talk("Я голосовой помощник. Меня зовут НеСири. Очень рада знакомству!")

def create task():

    talk('Что добавим в список дел?')
    query = listen_command()
    with open('todo-list.txt', 'a') as file:
        file.write(f'- {query}\n')
    return f'Задача {query} добавлена в todo-list!'
     talk ("Задача добавлена в ваш список")
def open_website():
  talk ("Какой сайт вы хотели бы открыть?")
  query1 = sr.recognize_google(audio_data=audio, language='ru-RU').lower()
  if 'гугл' in query1
          talk("Уже открываю")
          # Указываем сайт для открытия
          url = 'https://www.google.ru/'
          # Открываем сайт
          webbrowser.open(url)
  elif 'переводчик' in query1
          talk("Уже открываю")
          url = 'https://translate.google.com/?hl=ru'
          webbrowser.open(url)
  elif 'личный кабинет университета' in query1
          talk("Уже открываю")
          url = 'https://lk.sut.ru/cabinet/'
          webbrowser.open(url)

def main():
    query = listen_command()
    for k, v in commands dict['commands'].items():
        if query in v:
            print(globals()[k]())

if __name__ == '__main__':
    main()
```

Рис. 1. Листинг программы голосового помощника

Библиотека PyAudio обеспечивает более низкоуровневое управление, что позволяет пользователям устанавливать параметры для своих устройств ввода и вывода, а также проверять загрузку своего процессора и активность ввода-вывода.

Библиотека PyAudio также позволяет пользователям воспроизводить и записывать звук в режиме обратного вызова, где указанная функция обратного вызова используется, когда новые данные необходимы для воспроизведения и доступны для записи. Библиотека специально используется, если пользователь хочет воспроизвести звук помимо простого воспроизведения.

Для тестирования возможностей библиотек был создан простой голосовой помощник со следующим кодом (рис. 1, см. выше).

В качестве проверки правильности работы программы представляется голосовая команда «добавить задачу», после который в специальный текстовый файл были добавлены три задачи по очереди, а также выведены на экран и озвучены результаты голосовым помощником (рис. 2).

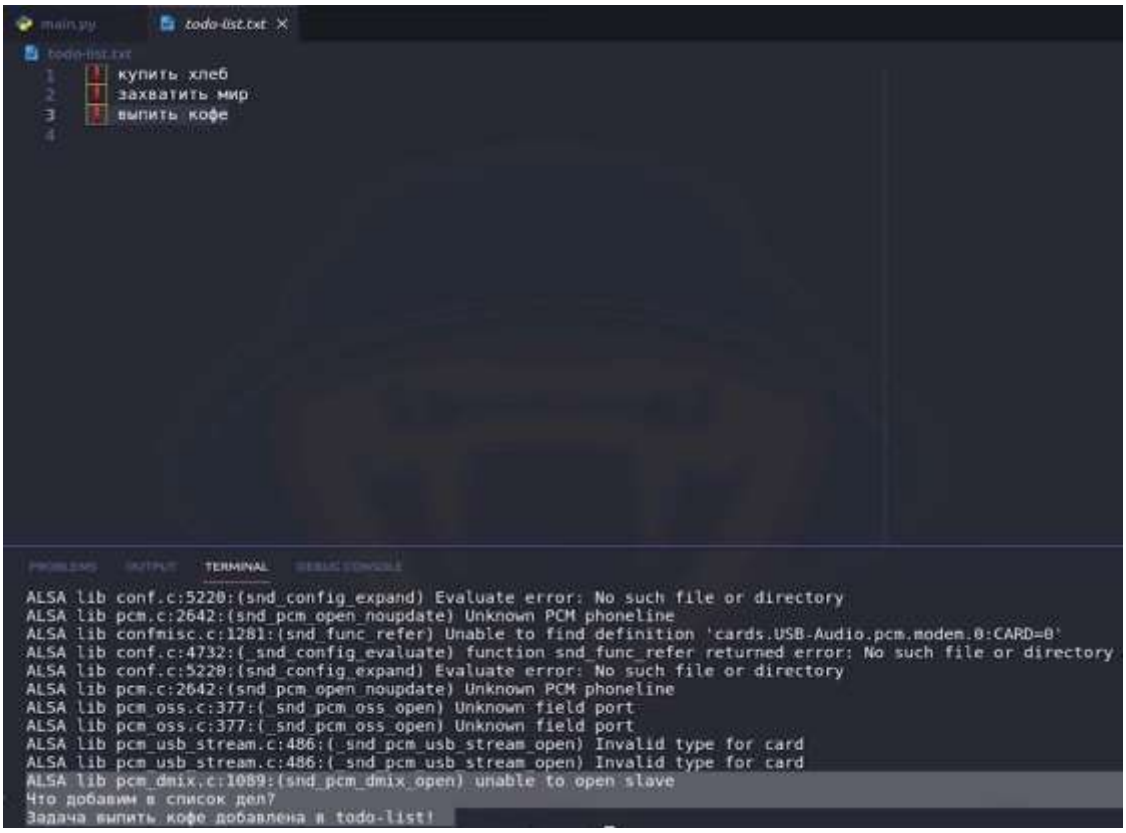


Рис. 2. Результат команды «добавить задачу»

Данный голосовой помощник также способен представиться и открыть веб-сайт, естественно, озвучив эти действия голосом.

Таким образом, анализ основных функций библиотек PyAudio и SpeachRecognition в рамках реализованного голосового помощника показал, что данные библиотеки дали возможность:

– осуществить воспроизведение и запись звука;
– определить форму аудио сигнала;
– определить формат, частоту и длину записи;
– определить язык записи и озвучивания;
– реализовать учет записи шума и периода тишины.

Список используемых источников

1. Распознавание речи и голоса на Python. URL: https://pythonpip.ru/ examples/raspoznavanie-rechi-i-golosa-na-python-podrobno (дата обращения: 14.02.2022).
2. 10 аудиомодулей Python для воспроизведения и записи. URL: https://pythonpip.ru/osnovy/10-audiomoduley-python-dlya-vosproizvedeniya-i-zapisi (дата обращения: 14.02.2022)
3. PyAudio Documentation. URL: https://people.csail.mit.edu/hubert/pyaudio/docs/ (дата обращения: 14.02.2022).
4. SpeechRecognition documentation. URL: https://github.com/Uberi/speech_ recognition (дата обращения: 11.03.2021).
5. gTTS documentation. URL: https://gtts.readthedocs.io/en/latest/index.html (дата обращения: 11.03.2021).

УДК 005:004
ГРНТИ 81.95.33

ИНФОГРАФИКА КАК ФОРМА ГРАФИЧЕСКОГО И КОММУНИКАЦИОННОГО ДИЗАЙНА

Е. П. Бояшова, М. В. Мельников, М. А. Ушанова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена рассмотрению инфографики как формы графического и коммуникационного дизайна. Рассмотрение инфографики с этой позиции позволяет акцентировать внимание на важности формы представления информации. В статье особое внимание уделяется направленности и значимости инфографики в представлении большого объёма статистических данных. В работе приведены варианты классификации инфографики, где информационная графика представлена с различных позиций, а также предложена новая классификация. Помимо этого, в работе рассмотрены и проанализированы примеры инфографики из мировой практики.

инфографика, информационная графика, графический дизайн, коммуникационный дизайн, информация, данные, представление данных.

Введение

В современном мире человека окружает большое количество информации, что связано с развитием информационных технологий, доступа к сети Интернет и цифровизацией сфер деятельности человека.

По способу представления информация может быть текстовой, числовой, звуковой или графической.

Способы представления данных, которые способствуют наиболее и удобному восприятию, повышению эффективности работы с данными, способствуют снижению временных затрат на обработку информации.

Именно графическое представление информации считается наиболее удобным для восприятия [1]. Визуальные образы ускоряют усвоение информации и способствуют активации и усилению мыслительной деятельности.

Для визуального представления информации используется инфографика (информационная графика), которая позволяет упростить восприятие сложной, объёмной информации. Под сложной информацией стоит понимать такую, которая является трудной для восприятия и понимания аудиторией. Объёмная информация, в свою очередь, – это достаточно большие по размеру и количеству данные.

Определение понятия «инфографика»

Термин «инфографика» используется в различных сферах деятельности человека, связанных с обработкой и передачей информации.

Исследователи предлагают совершенно разные определения этого понятия.

В. В. Лаптев, доцент кафедры инженерной графики и дизайна СПбПУ, даёт определяет инфографику как область коммуникативного дизайна. Важно, что в основе инфографики лежит графическое представление информации (связей, числовых данных и знаний) [2].

Г. А. Никулова и А. В. Подобных определяют объекты инфографики следующим образом [3]: «существует особая категория изображений, в которых плотность концентрации коммуникативных возможностей выше, чем у прочих – объекты информационной графики».

Ю. В. Соколова рассматривает инфографику как продукт графического дизайна, содержащий набор элементов [4].

Однозначно можно утверждать, что инфографика структурирует и систематизирует данные, представляя их в графическом виде. При этом её возможно рассматривать как область графического и коммуникационного дизайна. В первом случае акцент делается на эффектном, гармоничном визуальном представлении, а во втором – на точной передаче информации.

Направленность и значимость инфографики

Рассматривая инфографику как форму коммуникационного дизайна, стоит отметить её направленность на быстрое и точное восприятие сложной, объёмной информации аудиторией. Таким образом, можно считать, что инфографика имеет прагматическую направленность. Более того, обеспечение быстрого и точного восприятия информации – это главная цель создания инфографических изображений. Прагматическая направленность инфографики является фактором, обуславливающим её специфику.

Ключевую роль в инфографике играет информация. Однако форма представления данных крайне важна, поскольку одни и те же данные можно представить разным образом. Более того, возможна ситуация, когда аудитория по-разному поймёт представленную информацию и, исходя из этого, сделает разные выводы. От правильности выбора формы представления информации зависит успех применения инфографики. Под успехом в данном случае стоит понимать правильное понимание информации аудиторией и, более обширно, возможность достижения каких-либо результатов.

Если же рассматривать инфографику как форму графического дизайна, стоит акцентировать внимание на визуальных образах, потому что даже простые геометрические формы несут в себе определённую смысловую нагрузку, а также на соблюдении основных принципов графического дизайна и создании гармоничной визуальной среды.

Классификация инфографики

В настоящее время используется огромное количество различных видов инфографики, поэтому актуальной является задача создания классификации, позволяющей представить всё многообразие инфографических изображений в удобном для обозрения и изучения виде.

Конечно, вопросы классификации инфографики затрагиваются исследователями в своих публикациях. При этом стоит заметить, что существующие классификации очень значительно различаются, поскольку исследователи предлагают разделять инфографические изображения на различные группы, а также выделяют в них типы в рамках решения конкретных задач.

Так, например, Г. А. Никулова и А. В. Подобных разделяют инфографику на две большие группы по критерию систематизации типов данных [3] – группы количественной и качественной визуализации.

К. В. Нефедьева разделяет инфографику на типы по способу визуализации данных [5]. Она выделяет матрицы, карты, иллюстрации, графики и диаграммы.

А. В. Авдиенко, отталкиваясь от классификации Лондонской школы PR, выделяет 9 основных типов инфографик [6].

А. А. Жиленко и О. В. Климова предлагают довольно обширную классификацию инфографики по цели, по формату, по типу источника информации, по содержанию, по форме визуализации, по способу распространения, по целевой аудитории [7]. Такая классификация является довольно универсальной.

Специалисты разделяют инфографику на группы в рамках конкретных исследований, касающихся визуализации информации для решения определённых задач.

При этом возможно создание такой классификации, которая рассматривает информационную графику с совершенно разных позиций: по способу визуализации, возможностям взаимодействия с наблюдателем, форме представления, виду используемой графики, типу проекции изображения, палитре используемых цветов и др. Важно отметить, что указанные критерии систематизации типов важны при рассмотрении инфографики именно как формы графического и коммуникационного дизайна.

Учитывая существующие работы в данной области, мы предлагаем следующую классификацию инфографики (рис. 1).

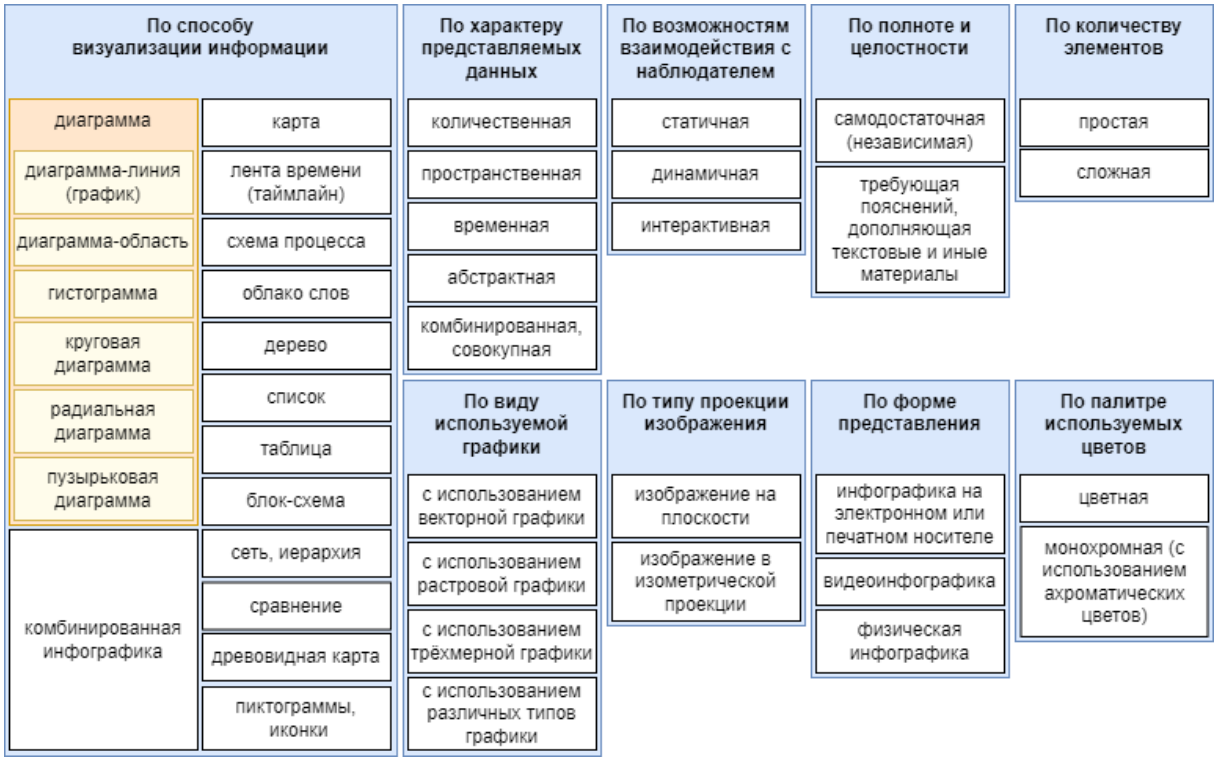


Рис. 1. Классификация инфографики

Более подробного описания требуют две выделенные группы: выделение типов инфографики по характеру представляемых данных и по возможностям взаимодействия с наблюдателем.

Стоит отметить, что комбинированная инфографика представляет собой такое инфографическое изображение, в котором используются различные виды представления данных (т. е. несколько из указанных в группе по способу визуализации информации).

По характеру представляемых данных можно выделить следующие группы:

– количественная – визуализация количественных данных;

– пространственная – представление местоположения объектов, их внешнего вида, структуры, внутреннего устройства;

– временная – отображение данных, изменяющихся во времени, а также событий, явлений на временной шкале в хронологическом порядке;

– абстрактная – представление совокупностей, иерархий, структур, плотности объектов, корреляции данных, а также визуализация качественных параметров;

– комбинированная – представлены данные различных типов.

По возможностям взаимодействия с наблюдателем:

– статичная – все элементы инфографики неподвижны, с ними нельзя взаимодействовать;

– динамичная – инфографика содержит анимированные, изменяющиеся элементы; может отражать динамику развития, прогресс;

– интерактивная – пользователь (наблюдатель) имеет возможность выбора определённых данных для их визуализации, он может изменять различные части инфографики, влиять на её отображение.

Предлагаемая классификация позволяет представить многообразие существующих инфографик в удобном для обозрения и изучения виде как при аналитическом рассмотрении инфографики как формы графического и коммуникационного дизайна, так и при проектировании новых инфографических изображений для решения различных задач.

Анализ примеров инфографики из мировой практики

В современном мире инфографика приобрела огромную популярность. Она используется повсюду, от цифрового маркетинга до школ и детских садов. Некоммерческие организации выбирают инфографику для распространения информации о социально-значимых событиях и актуальных вопросах.

Gapminder – образовательная некоммерческая организация, борющаяся с глобальными заблуждениями. Она задает вопросы людям со всего света, чтобы увидеть, что они думают о мире на основании новостей. После этого организация проверяет данные в ООН и других источниках и выявляет наиболее распространенные заблуждения относительно макро тенденций. Организация стремится развеять ложные представления о мире и делает это при помощи инфографики.

На сайте Gapminder [7] огромное количество данных представлено в разных видах инфографики. Особенное внимание хотелось бы уделить пузырьковым диаграммам. На рис. 2 представлена диаграмма зависимости средней продолжительности жизни от уровня дохода населения.

На диаграмме массив данных организован в единую визуальную систему. Каждый «пузырек» представляет собой отдельную страну, его размер зависит от количества населения, а цвет, от части света, где располагается страна. Горизонтальная ось: доход на душу населения, вертикальная ось: средняя продолжительность жизни. Благодаря качественной инфографике, мы можем убедиться в том, что средняя продолжительность жизни зависит от уровня дохода.

Рис. 2. Пузырьковая диаграмма «Зависимость средней продолжительности жизни от уровня дохода»

На сайте множество динамической инфографики, что позволяет увидеть изменения в мире еще более наглядно. На рис. 3 представлен график изменения доходов населения США, России, Китая и Египта. Благодаря динамической инфографике мы можем наблюдать за последовательными изменениями уровня дохода на душу населения.

Рис. 3. График изменения дохода на душу населения в США, России, Китае и Египте с 1800 по 2021 год

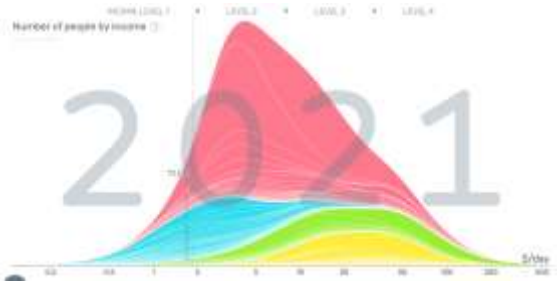


Рис. 4. Распределение населения Земли по уровню дохода

Очень распространенным является заблуждение, что большая часть населения Земли живет в нищете. Благодаря инфографике мы можем убедиться, что это не так (рис. 4), большинство людей имеет средний уровень дохода. Данная инфографика – это диаграмма-линия (график) с областями.

Можно отметить, что Gapminder успешно применяет инфографику в своей деятельности. Информационная графика, представленная на сайте, содержит в себе все элементы, необходимые для решения поставленных задач. Информация на сайте, полностью представленная в графическом виде, хорошо воспринимается.

Заключение

Инфографику возможно рассматривать как форму графического и коммуникационного дизайна.

Инфографика имеет прагматическую направленность, что обуславливает её специфику. Цель создания инфографических изображений — необходимость обеспечить быстрое и точное восприятие сложной, объёмной информации аудиторией. При этом принципиально важна форма представления информации.

Классификация инфографики позволяет представить многообразие существующих инфографик в удобном для обозрения и изучения виде как при аналитическом рассмотрении инфографики как формы графического и коммуникационного дизайна, так и при проектировании новых инфографических изображений для решения различных задач.

Список используемых источников

1. Card S. K., Mackinlay J. D., Shneiderman B. Readings in information visualization: using vision to think. Morgan Kaufmann Publishers, 1999. 686 p.

2. Лаптев В. В. Инфографика: основные понятия и определения // Общество. Коммуникация. Образование. 2013. № 184. URL: https://cyberleninka.ru/article/n/infografika-osnovnye-ponyatiya-i-opredeleniya (дата обращения: 15.01.2022).

3. Никулова Г. А., Подобных А. В. Средства визуальной коммуникации – инфографика и метадизайн // Образовательные технологии и общество. 2010. Т. 13. N 2. С. 369–387.

4. Соколова Ю. В. Инфографика как продукт графического дизайна: проблема определения понятия // Культурологические чтения – 2016: материалы международных научно-практических конференций (Екатеринбург, УрФУ, 16–19 марта). Екатеринбург: УрФУ, 2016. С. 254–261.

5. Нефедьева К. В. Инфографика визуализация данных в аналитической деятельности // Труды СПбГИК. 2013. URL: https://cyberleninka.ru/article/n/infografika-vizualizatsiya-dannyh-v-analiticheskoy-deyatelnosti (дата обращения: 10.01.2022).

6. Авдиенко А. В. Инфографика как альтернативный способ подачи информации // Университетские чтения – 2016: материалы научно-методических чтений ПГУ. Пятигорск: ПГУ, 2016. Ч. 10. С. 58–62. URL: https://pgu.ru/editions/un_reading/ detail.php?SECTION_ID=3676&ELEMENT_ID=147941 (дата обращения: 12.01.2022).

7. Жиленко А. А., Климова О. В. Определение видов инфографики как редакторская проблема // Книжное дело: достижения, проблемы, перспективы : сборник материалов VI Международной научно-практической интернет-конференции. Екатеринбург : УрФУ, 2017. С. 39–45. URL: http://hdl.handle.net/10995/56361 (дата обращения: 12.01.2022).

8. Gapminger Tools. URL: https://www.gapminder.org/tools/ (дата обращения: 24.01.2022).

Статья представлена заведующим кафедрой ИКД СПбГУТ, доктором технических наук, доцентом Д. В. Волошиновым.

УДК 004.855
ГРНТИ 28.23.27

ОБНАРУЖЕНИЕ АНОМАЛИЙ WEB-ТРАФИКА С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Д. А. Бражников, Д. Е. Горохов

Академия Федеральной службы охраны Российской Федерации

Web-трафик – это поток данных, который циркулирует в компьютерной сети в процессе предоставления пользователям множества разнообразных инфокоммуникационных услуг. С развитием компьютерных технологий растет статистика атак на информационные ресурсы. Многие атаки в процессе реализации создают аномалии в структуре web-трафика. Аномалии web-трафика – это определенные изменения в потоке временных рядов. Для надежной и безопасной работы сложных компьютерных сетей необходимо быстро и точно производить их обнаружение. В этой статье предлагается нейронная сеть, связывающая сверточные нейронные сети (CNN), сети с долговременной кратковременной памятью (LSTM) и глубокую нейронную сеть (DNN). Она превосходит другие современные методы обнаружения аномалий, в результате чего общая точность на наборе тестовых данных составляет 96,8 %, а полнота – 88,2 %.

глубокое обучение, временные ряды, обнаружение аномалий.

Обнаружение аномалий трафика обрабатываемого web-серверами представляет собой одномерную задачу классификации временных рядов. Рассматривая поток пакетов проходящих через датчик системы обнаружения атак в некотором временном окне, можно выделить отличительные признаки для распознавания аномальной активности с помощью различных классификаторов. При этом обнаружение аномальных закономерностей в web-трафике представляется нетривиальной задачей ввиду различных статистических характеристик трафика в зависимости от типа предоставляемой услуги и действий пользователей, что приводит к нестационарности временного ряда параметров сетевого трафика [1].

Поток пакетов в некоторой рассматриваемой точке сети может быть описан множеством параметров $X = \{x_1, x_2, \ldots, x_n\}$, каждый из которых представляет собой случайную величину и характеризующуюся своим законом распределения $f(x_i)$.

Гибридная нейронная сеть C-LSTM предназначена для автоматического выявления зависимостей, в том числе нелинейных, в многомерном нестационарном ряду значений параметров потока пакетов. Эти данные записываются в течение некоторого времени и содержат определенные

пространственные и временные зависимости. В свою очередь, администратор может классифицировать нормальные и аномальные шаблоны поведения, встречающиеся в трафике. Также, метод C-LSTM сокращает спектр данных за счет преобразования пространственного контекста с использованием относительно простого уровня CNN. Структура используемой нейронной сети представлена на рисунке.

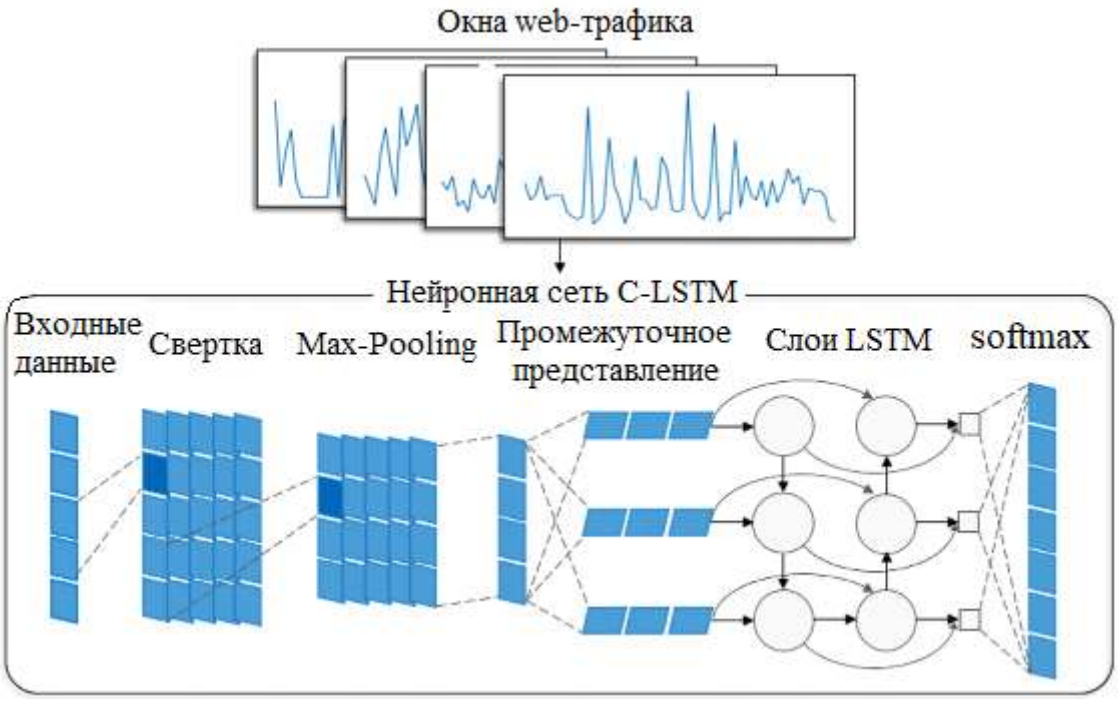


Рисунок. Структура нейронной сети для обнаружения аномалий web-трафика

Нейронная сеть C-LSTM состоит из сверточных слоев (CNN) и LSTM и объединена в линейную структуру. В качестве входных данных используются предварительно обработанные наборы данных. CNN состоит из нескольких слоев свертки и объединения, которые используются для автоматического извлечения высокоуровневых последовательностей пространственных характеристик web-трафика. Эти двумерные операции свертки используют несколько векторов-фильтров, которые скользят по последовательности и обнаруживают особенности по порядку. За сверточным слоем следует функция активации. Это позволяет CNN фиксировать сложные особенности входного сигнала. В качестве функции активации используется tanh, которая масштабируется и сдвигает сигмовидную функцию, это позволяет нейронной сети быстрее обучаться.

В состав исходного набора данных входит большое количество различных характеристик сетевого трафика, анализ которых может дать на выходе системы различные результаты. Предлагается использовать следующие параметры сетевого трафика в качестве исследуемого признакового пространства:

x_1 – интенсивность пакетов, поступивших в адрес рассматриваемого хоста (сети) за время *t* (пак/с);

x_2 – интенсивность пакетов, исходящих от контролируемого хоста (сети) (пак/с);

x_3 – объем трафика в точке контроля на интервале наблюдения (бит);

x_4 – количество наблюдаемых потоков (шт.);

x_5 – количество фрагментированных пакетов (шт.);

x_6 – количество сегментов с флагом SYN на интервале наблюдения (шт.);

x_7 – количество сегментов с флагом FIN на интервале наблюдения (шт.);

x_8 – количество флагов ACK на интервале наблюдения (шт.).

Выходное значение y из *k*-го слоя свертки определяется в соответствии с выражением (1):

$$y_{ij}^{k} = \sigma(b_j^{k-1} + \sum_{m}^{M-1} W_{m,j}^{k-1} x_{i+m-1,j}^{k-1}), \quad (1)$$

где *x* – вектор параметров сетевого трафика; *n* – количество значений в окне; *i* – индекс значения признака; *j* – индекс карты объектов для каждого окна трафика; *M* – размер фильтра.

Слои объединения уменьшают пространственный размер представления, чтобы сократить количество параметров и вычислительную сложность сети. Это также помогает избежать эффекта переобучения [2]. Эффективное уменьшение пространства признаков, достигается применением операции *maxpooling*. Данная операция позволяет повысить обобщающую способность сети и выделять значимые комбинированные признаки для последующего анализа.

В слоях LSTM используются ячейки памяти, что позволяет учитывать временных характеристик данных web-трафика с учетом предположения о существовании шаблонов поведения источников данных, характерных для различных периодов функционирования сети. Выходное значение предыдущего слоя используется в качестве входного, и применяется концепция стробирования. Входные данные, поступающие на слой LSTM, обрабатываются ячейками, которые управляют входными, выходными и забывающими вентилями в памяти ячейки в соответствии с выражениями (2)–(4):

$$i_t = \sigma(W_{pi} p_t + W_{hi} h_{t-1} + W_{ci} \circ c_{t-1} + b_i), \quad (2)$$

$$f_t = \sigma(W_{pf} p_t + W_{hf} h_{t-1} + W_{cf} \circ c_{t-1} + b_f), \quad (3)$$

$$o_t = \sigma(W_{po} p_t + W_{ho} h_{t-1} + W_{co} \circ c_{t-1} + b_o). \quad (4)$$

Выходные данные модуля LSTM сглаживаются в вектор признаков и используются в качестве входных данных для полносвязного слоя (5):

$$d_i^k = \sum_j \sigma(W_{ji}^{k-1}(h_i^{k-1}) + b_i^{k-1}), \quad (5)$$

где W – вес функции; σ – функция активации; b_j^0 – смещение для j-й карты признаков.

Для повышения инвариантности модели к условиям функционирования и структуре сети, множество параметров может быть дополнено статистическими характеристиками, которые описывают распределение случайной величины x_i (табл. 1) [3]:

ТАБЛИЦА 1. Используемые статистические характеристики

Название параметра	**Формула**	**Физический смысл**
Коэффициент асимметрии	$K_a = \frac{\frac{1}{n}\sum_{j=i}^{i+n}(S_j - m_j)^3}{D^3}$	Характеризует асимметричность распределения признака в совокупности
Коэффициент эксцесса	$K_э = \frac{\frac{1}{n}\sum_{j=i}^{i+n}(S_j - m_j)^4}{D^4} - 3$	Представляет собой отклонение вершины эмпирического распределения вверх или вниз от вершины нормального распределения
Коэффициент контрэксцесса	$КоЭ = \frac{1}{\sqrt{\eta}}$, $\eta = Кэ = \frac{\upsilon^4}{\sigma^4}$	Значения коэффициента контрэксцесса лежат в пределах от 0 до 1
Энтропийный коэффициент	$K_{эн} = \frac{\omega N}{2\sigma} 10^{-\frac{1}{N}\sum_{i=1}^{m} n_i \lg(n_i)}$	Определение меры разброса значений
Перекрестная энтропия	$H(p,q) = -\sum_x p(x) \log q(x)$	Служит для количественной оценки разницы между двумя распределениями вероятностей

Использование статистических характеристик вместо исходных параметров, приводит к увеличению размерности пространства параметров в пять раз.

Вероятность классификации трафика на нормальный и аномальный вычисляется в соответствии с выражением (6):

$$P(c \mid d) = \arg\max_{c \in C} \frac{\exp(d^{K-1} w^{K})}{\sum_{l-1}^{N_c} \exp(d^{K-1} w_l)}, \quad (6)$$

где K – индекс последнего слоя; N_c – общее количество классов активности.

После всех проделанных операций обученная модель выполняет обнаружение аномалий в наборе данных с помощью классификатора *softmax*.

Ошибка возникает, если относительно наблюдаемых данных в окне анализа не принимается решение об аномальности при том, что воздействий на сеть или сервис оказывалось или наоборот. Первый тип ошибки – ложноотрицательный (FN), второй – ложноположительный (FP). Точно так же истинно положительный результат (TP) возникает, если правильно идентифицирован нормальный экземпляр, а истинно отрицательный результат (TN) возникает, если правильно классифицирован аномальный экземпляр. В выполненных экспериментах оценка алгоритма выполнялась с использованием подсчета количества исходов TP, TN, FP и FN на основе вычисления метрик *precision, recall* (7)–(8).

$$precision = \frac{TP}{TP + FP}, \quad (7)$$

$$recall = \frac{TP}{TP + FN}. \quad (8)$$

Используя переменные *precision* и *recall*, возможно получить оценку *F1* (9). Это позволит произвести сравнение с уже существующими методами.

$$F1 = 2 * \frac{recall * precision}{recall + precision}, \quad (9)$$

В ходе проведения эксперимента на наборе данных CSE-CIC-IDS2018 были получены результаты, представленные в таблице 2.

ТАБЛИЦА 2. Результаты тестирования виртуальной сети

Метод	**precision, %**	**recall, %**	**F1, %**
LSTM	94,7	87,9	95,3
CNN	95,3	87,6	94,9
C-LSTM	96,8	88,2	96,7

Таким образом, рассмотренная гибридная нейросетевая модель имеет высокую точность и низкую перекрестную энтропию. При этом использование статистических характеристик параметров потока пакетов повышает инвариантность модели к условиям функционирования и структуре сети. В процессе эксперимента, было выявлено, что сложнее всего обнаружить контекстуальные аномалии, за которыми следуют точечные аномалии и коллективные аномалии. Вместе с тем требует дополнительного исследования вопрос оптимизации гиперпараметров модели.

Список используемых источников

1. Обеспечение информационной безопасности на основе анализа сетевого трафика. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-kompyuternyh-setey-na-osnove-analiza-setevogo-trafika (дата обращения: 10.02.22).

2. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб.: Питер, 2018. 480 с.

3. Анализ ключевых характеристик сетевого трафика. URL: https://cyberleninka.ru/article/n/analiz-klyuchevyh-harakteristik-setevogo-trafika (дата обращения: 10.02.22).

ГРНТИ 50.43
УДК 004.428

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

М. Е. Брылев, А. И. Ликарь, М. Д. Поведайко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель исследования – рассмотреть принцип языка жестов и создать приложение, которое будет обучать детей языку глухонемых. Так как приложение разрабатывается специально для детей (до 12 лет), то в работе немало информации уделено о восприятии мира детьми, то есть их мышление на образах и ярких цветах и предметов. Ведь по тому же принципу будет строится внешний вид нашего приложения.

В статье анализируются уже существующие аналоги и учитываются их плюсы и минусы. Даётся сравнение существующих аналогов и своей идеи.

Далее по содержанию следует часть доклада, посвящённая разработке самого приложения – какие технологии и среда разработки использовались при создании приложения и объяснение, почему выбрали именно их. Из-за того, что разрабатываемый программный продукт имеет клиент-серверное назначение, особое внимание также акцентируется на безопасности этого приложения.

мобильное приложение, психология, дети.

Принцип мышления у детей

Развитие мышления начинается с структурирования чувственных восприятий и действий. Мышление зависит от отношений с самого начала. Ребёнок нуждается в эмоциональных, невербальных и вербальных предложениях и реакциях на свои действия со стороны опекунов. Если этот диалог не увенчается успехом, он будет тормозиться в развитии своего мышления. Чувство безопасности и ободряющий взгляд учителя побуждают ребёнка приступить к различным исследованиям окружающего его мира. Особенно важным шагом является включение ребёнком в свои действия воспитателей и создания общего внимания.

С самого начала дети ищут смысл и значение. Уже в шесть месяцев они могут распознавать и запоминать причинно-следственные связи (например, удар ногой – затем движение, потрясение погремушкой – затем звук). Уже в этом возрасте ребёнок способен формировать и запоминать категории и правила (известные и неизвестные звуковые последовательности своего родного языка). Начальное понимание множеств также развивается. Даже маленькие дети понимают, что если сложить 1+1, то не может быть ответ 1.

Также всем известна склонность детей постоянно спрашивать о причинах, то есть находить связь между выдвинутыми гипотезами и реальностью. По сути, вопросами «почему» дети проверяют эти гипотезы. Гипотезы выдвигать ребёнок способен в четырёхлетнем возрасте.

Дети думают картинками и выражают себя через картинки. Им важна ассоциация себя с персонажами и визуализированными образами. Этой форме образного мышления нужно дать пространства, предлагая детям широкий спектр возможностей для выражения своих мыслей и идей. Это форма мышления должна найти своё особое место в эстетико-художественном выражении и музицировании.

Мышление в себя включает все навыки, которые помогают объяснить, структурировать и предсказывать. В частности, речь идёт о создании категорий, поиске и применение правил, понимании причинно-следственных связей, рассуждении и решении проблем, а также о логическом мышлении. Чтобы ребёнок научился применять все эти навыки, ему нужна среда, которая побуждала бы к этому. И речь идёт даже не об изучении фактов, а о способах мышления и стратегии при решении каких-либо задач.

В сфере решений различных задач и упражнений должна выстроится связь между конкретным контекстом и его мышлением в образах и символах. Различные увиденные ребёнком предметы и явления требуют объяснения и вызывают потребность в понимании.

Детское мышление есть мышление целостное, поэтому важно подходить к детским темам и вопросам не изолированно, а рассматривать математические, научные и технические отношения в целом, встраивать их в детские формы выражения, то есть сделать их осязаемыми и визуализированными.

Приложение ASL

ASL Kids – приложение для детей от 1 до 12 лет, предназначенное для изучения американского языка жестов (рис. 1). Само приложение предназначено для детей, которые могут пользоваться им без помощи взрослых. Приложение использует визуализацию и озвучку содержимого контента, что может привести к улучшению обучению детей. Тактильные ощущения помогают легче запоминать то, чему дети уже научились. Все показанные знаки и символы сопровождаются большим изображением и кнопкой образцом, предназначенные для стимуляции речи и слуха [1].

Приложение является бесплатным и не содержит никаких прямых ссылок и рекламы. У родителей есть возможность отслеживать и контролировать все покупки в приложении. Для работоспособности приложения не требуется постоянного подключения к интернету.

Отсутствие сложного текста позволяет детям ориентироваться и легко разобраться в навигации приложения благодаря чётким и доступным изображениям.

Разработчики стремятся постоянно улучшать и развивать своё приложение.

Рис. 1. Заставка приложения ASL на планшете

Технологии для создания приложения

Для создания нашего приложения нам понадобится язык программирования, язык разметки и среда разработки:

● Kotlin – это язык программирования компании JetBrains, чья первая версия вышла в 2016 году. Программы, созданные на этом языке, выполняются с использованием виртуальной машины Java (JVM). Kotlin синтаксически не похож на Java, но может использовать её библиотеки [2];

● XML – язык разметки, используемый для представления иерархической структуры данных в формате текстового файла [2];

● Android Studio – это бесплатная интегрированная среда разработки от Google для создания Android-приложений.

Примеры внешнего вида приложения

На рис. 2 показаны главное меню нашего приложения и пример одного из заданий для выполнения. В задании нужно найти две одинаковые картинки.

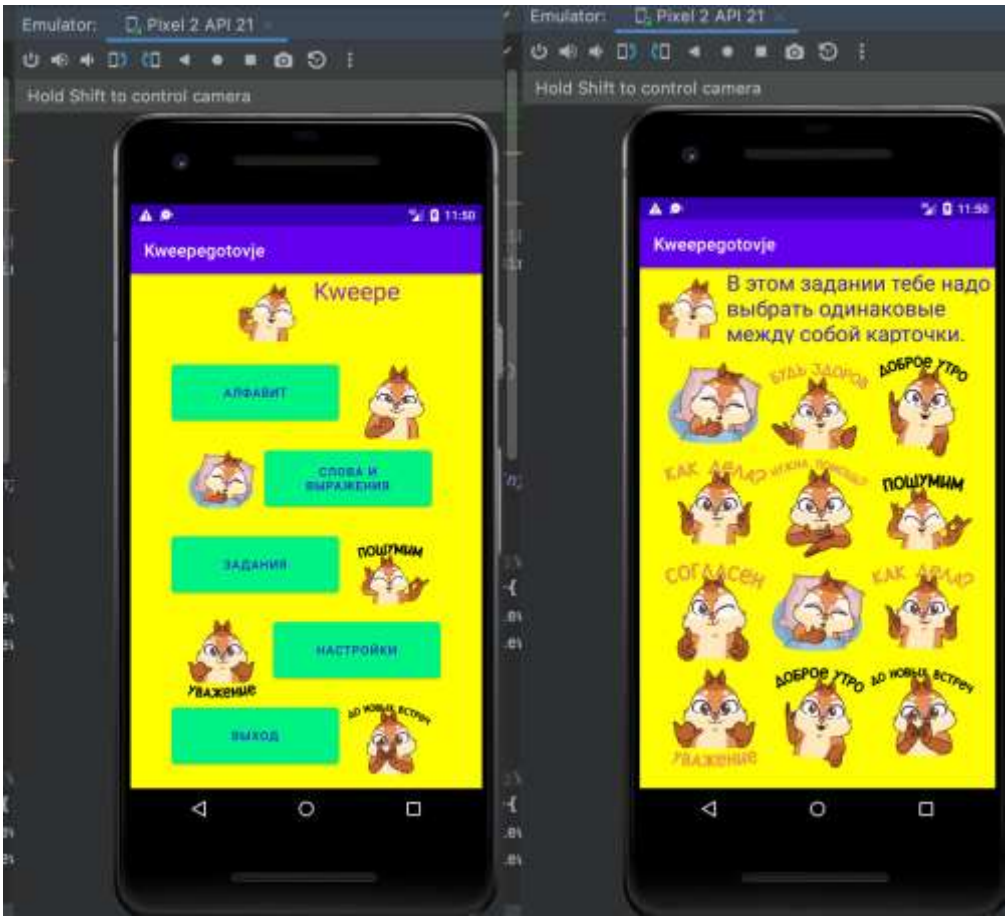


Рис. 2. Меню и задание нашего приложения

Меню и задание на рис. 2 показано на эмуляторе мобильного телефоне на базе Android. Название модели телефона Pixel 2.

Вид приложения был сделан из яркого фона и цветов

Вывод

Таким образом, создано приложение для изучения языка жестов, учитывая специфику мышления ребёнка.

Список используемых источников

1. Application ASL Kids. URL: https://asl-kids.com/sign-language-app/ (дата обращения: 19.01.2022)
2. Guy Vollmer Mobile App Engineering: Eine systematische Einführung – von den Requirements zum Go Live: 2017, 324 pages.

УДК 004.054
ГРНТИ 81.93.29

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ АНАЛИЗА ЗАЩИЩЕННОСТИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Д. О. Булгаков, М. М. Добрышин, Д. Е. Шугуров

Академия Федеральной службы охраны Российской Федерации

Активное и непрекращающееся развитие информационных систем последних десятилетий влечёт за собой и новые угрозы информационной безопасности. При этом информационные системы являются одним из достоверных официальных источников необходимых как для обычных граждан, так и для информационной поддержки деятельности органами государственной власти. При этом государственные информационные ресурсы, находящиеся в открытых сетях достаточно часто подвержены компьютерным атакам. В связи с этим возникает задача о возможности снижения ущерба за счет использования системы мониторинга информационной безопасности и разработки программных средств, которые способны выявлять уязвимости на различных стадиях жизненного цикла информационных систем.

информационная система, уязвимости, средства анализа защищенности, мониторинг информационной безопасности.

В настоящее время трудно представить работу органов государственной власти, государственных учреждений и крупных организаций без использования информационных систем (ИС), которые обеспечивают их деятельность. От внедрения ИС и их профессионального использования зависит оперативность управления, выполнение регламентов, качество и скорость предоставления услуг. Государственные информационные системы (ГИС) предназначены для реализации полномочий госорганов и обеспечения обмена информацией между этими органами, а также для выполнения задач, определяемых федеральными законами. Они создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами, государственными органами,

организациями, органами местного самоуправления. Согласно нормативно правовым документам, государственные органы, ответственные за функционирование ГИС, должны обеспечивать конфиденциальность, целостность и доступность содержащейся в данных системах информации [1].

В связи с развитием информационных технологий происходит совершенствование методов осуществления атак на ГИС [2–4]. По данным одной из ведущих компаний, занимающейся практическими вопросами в области информационной безопасности, *Positive Technologies* количество атак за 2021 год на ИС значительно увеличилось в сравнении с 2020 годом (рис. 1).

Исходя из анализа статистики видно, что количество компьютерных атак за 2021 год на ИС выросло в среднем на 10 % в сравнении с 2020 годом. Учитывая приведенную статистику, можно заметить, что доля компьютерных атак на ИС государственных учреждений возросло и составляет 30 % от общего числа организаций, подверженных компьютерным атакам (рис. 2) [5].

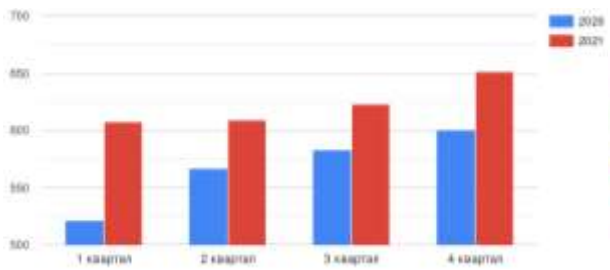


Рис. 1. Статистика компьютерных атак в 2020 и 2021 годах

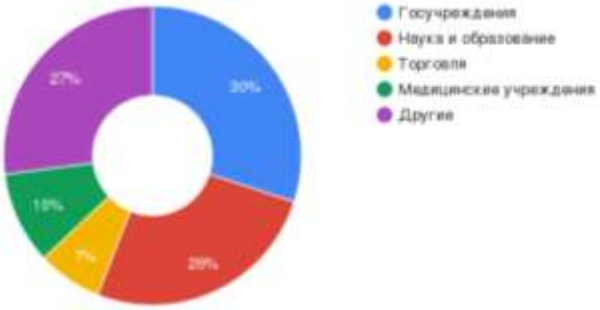


Рис. 2. Категории учреждений подверженных компьютерным атакам

Как правило мотивами реализации атак на ИС государственных учреждений являются компрометация данных, снижение репутации или политическая провокация. При реализации атаки нарушитель использует уязвимости данной ИС, которые приводят к нарушению целостности, конфиденциальности и доступности обрабатываемой информации. Поэтому для снижения возможностей нарушителей, реализующих атаки используя уязвимости ИС, необходимо построить качественную систему мониторинга информационной безопасности (СМИБ) [6–8].

Рассмотрим систему мониторинга информационной безопасности и ее одну из основных решаемых задач по анализу выявления уязвимостей ИС. Мероприятия, которые реализует СМИБ в рамках анализа защищенности ИС имеют следующее содержание:

– выявление и описание уязвимостей объектов ГИС;

– контроль обновлений, настроек и состава технических средств на проверяемых объектах;

– контроль состава средств защиты, их настройка и необходимые обновления;

– информирование ответственных лиц о результатах проведения анализа защищенности.

Поиск уязвимостей является сложным и трудозатратным процессом, в связи с чем применяются средства анализа защищенности (САЗ) (рис. 3) [9, 10].

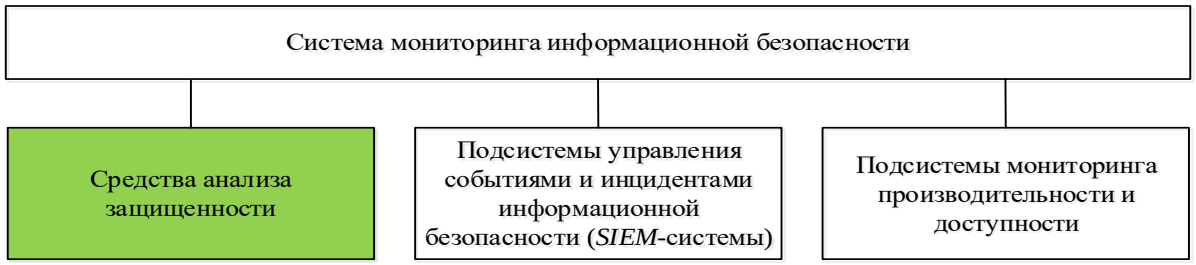


Рис. 3. Состав системы мониторинга информационной безопасности

При проведении анализа защищенности ИС используют два метода: активный и пассивный. Активный метод осуществляется чаще всего на сетевом уровне, производит тестирование и анализ соответствующей реакции исследуемой системы. Пассивный метод используется при анализе ИС на уровнях ОС, СУБД, приложений и осуществляет контроль конфигурационных файлов, версий приложений [8–10].

Объектами оценки безопасности, как правило, являются внешние и внутренние ресурсы ИС, их расположение и определяет место подключения средств анализа защищенности. В рамках исследования были определены особенности применения САЗ для объектов демилитаризованной зоны (ДМЗ), в которой расположены основные информационные системы (рис. 4).

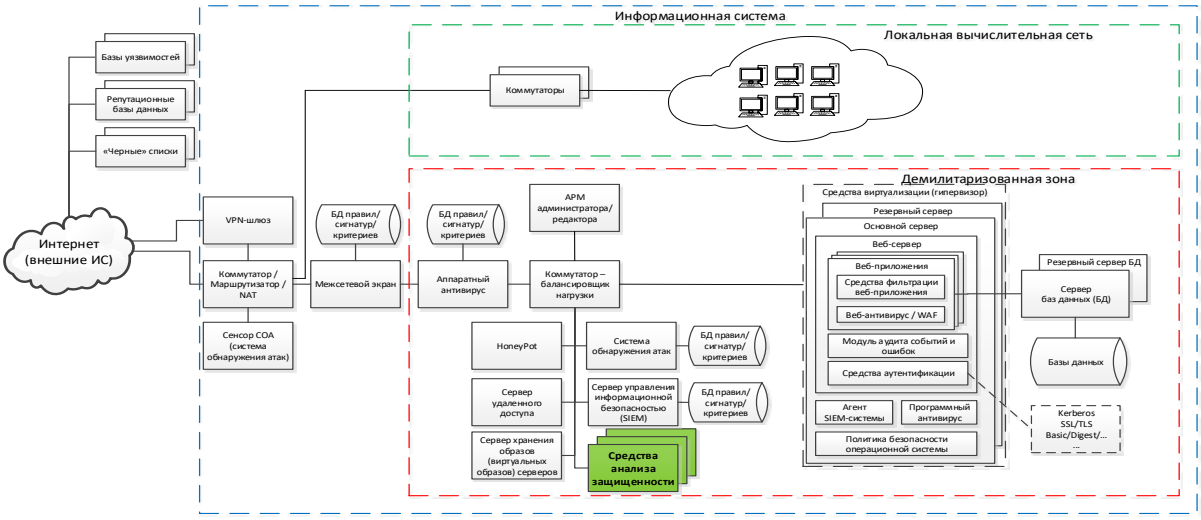


Рис. 4. Размещение средств анализа защищенности в демилитаризованной зоне

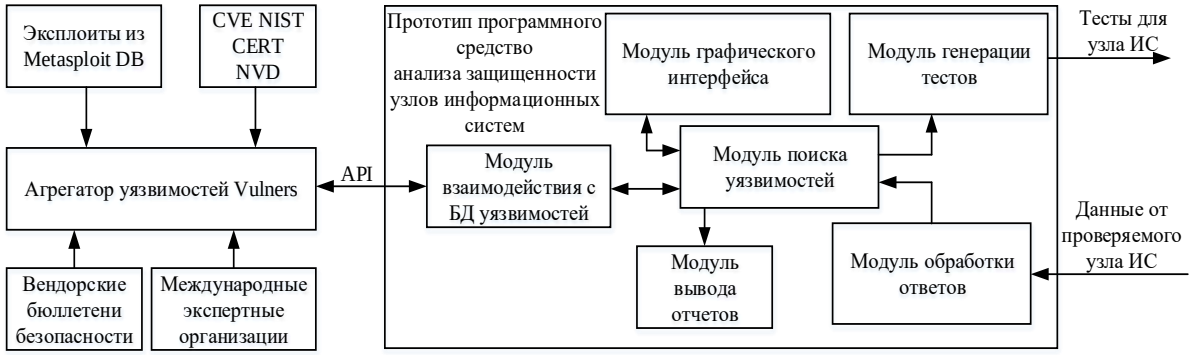


Рис. 5. Структурно-функциональная схема прототипа программного средства анализа защищенности

Для качественной оценки состояния защищенности объектов ДМЗ распределенной сети необходимо выбрать многофункциональный инструментарий, позволяющий осуществлять поиск и обнаружение уязвимостей. Учитывая сложность и особенности функционирования ГИС, предлагается использование модульного программного средства, позволяющего проводить анализ защищенности системы (рис. 5).

Основными функциями, которые выполняет программное средство анализа защищенности, являются:

1. Инициализация базы уязвимости (модуль взаимодействия с БД уязвимостей);

2. Отправка тестовых запросов к проверяемым узлам ИС (модуль генерации тестов);

3. Получение и обработка ответов от узлов ИС, анализ которых позволяет определить используемые протоколы, открытые порты, а также идентифицировать службы и версию ОС (модуль обработки ответов).

4. Поиск уязвимостей, на основе полученных специальных данных об узле ИС, а также управление компонентами программного средства (модуль управления);

5. Формирование отчета о выявленных уязвимостях с рекомендациями по их устранению (модуль вывода отчета).

В качестве базы уязвимостей, по которой осуществляется поиск предлагается использовать агрегатор уязвимостей *Vulners*. В настоящее время база данных *Vulners* агрегировала в себя более 870 тысячи записей об уязвимостях и около 170 тысяч записей об известных эксплойтах [11].

Таким образом, система мониторинга информационной безопасности должна решать основную задачу поиска уязвимости в информационных системах. Для решения данной задачи одним из направлений является необходимость создания специализированного программного средства. В рамках исследования предлагается модульный прототип программного

средства, функции которого позволят достоверно и качественно проводить анализ защищенности узлов, находящихся в демилитаризованной зоне.

Список используемых источников

1. Приказ ФСТЭК России от 11 февраля 2013 г. № 17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Минюст России, 2018.

2. Информационная безопасность в 2021 году // Positive Technologies [сайт]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/informacionnaya-bezopasnost-v-2021-samye-gromkie-vzlomy-i-utechki (дата обращения: 15.03.2022).

3. Добрышин М. М. Особенности применения информационно-технического оружия при ведении современных гибридных войн / I-methods. 2020. Т. 12. № 1. С. 1–11.

4. Добрышин М. М., Шугуров Д. Е. Иерархическая многоуровневая модель таргетированных компьютерных атак в отношении корпоративных компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 35–46.

5. Белов А. С., Добрышин М. М., Шугуров Д. Е. Предложение по оценке распространения компьютерных вирусов в локальной вычислительной сети // Авиакосмическое приборостроение. 2021. № 6. С. 38–48.

6. Гречишников Е. В., Добрышин М. М., Шугуров Д. Е., Берлизев А. В., Макаров В. Н. Способ мониторинга сетей связи в условиях ведения сетевой разведки и информационно технических воздействий / Патент на изобретение RU 2612275 C , 06.03.2017. Заявка № 2015152989 от 09.12.2015.

7. Добрышин М. М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2021. № 9 . С. 113–121.

8. Добрышин М. М. Белов А. С., Горшков А. А., Борзова Н. Ю. Предложение по проектированию систем обеспечения информационной безопасности с применением элементов ТРИЗ // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 38–44.

9. Козачок А. И., Комашинский В. В., Козачок А. В., Юркин А. А., Шугуров Д. Е. Системы анализа защищенности: пособие / под общ. ред. А.И. Козачка. Орел: Академия ФСО России, 2014. 132 с.

10. Добрышин М. М., Шугуров Д. Е., Беляев Д. Л. Модель сетевых атак типа XSS- и SQL-инъекций на веб-ресурсы, учитывающая различные уровни сложности их реализации // Известия Тульского государственного университета. Технические науки. 2021. № 2. С. 196–204.

11. База данных об уязвимостях и эксплоитах // VULNERS, INC. [сайт]. URL: https://vulners.com/ (дата обращения: 15.03.2022).

УДК 681.178.1
ГРНТИ 50.43.17

УСТРОЙСТВО КОНТРОЛЯ ДЛЯ СИСТЕМЫ ДЕЗИНФЕКЦИИ ВОЗДУХА В ЗАКРЫТЫХ ПОМЕЩЕНИЯХ ПРЕДПРИЯТИЙ

А. В. Ваганов, Е. Н. Григорьева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой устройства управления системой дезинфекции, предназначенной для очистки воздуха от биологических загрязнителей в помещениях промышленных предприятий. Обосновывается актуальность разработки системы подобного класса. Представлена структурная схема устройства и вариант построения системы дезинфекции в целом, а также обосновывается выбор современной элементной базы для ее реализации. Разработан специальный алгоритм работы системы дезинфекции воздуха в закрытых помещениях предприятий, учитывающий безопасность персонала. Реализован выбор первичных измерительных преобразователей, предназначенных для контроля процесса очистки. Произведен выбор математического аппарата для расчета устройства. Приведены результаты моделирования и осуществлен их анализ. Даны рекомендации к конструкции аппаратной части.

устройство контроля, датчик, алгоритм управления, математическая модель, структурная схема.

В последние несколько лет проблема дезинфекции воздуха в закрытых производственных помещениях становится все более актуальной. Не все производства возможно перевести на удалённую работу, поэтому необходимо поддерживать чистоту в помещениях, где постоянно работают люди, с целью сохранения здоровья и безопасности сотрудников.

Существуют различные способы проведения профилактической дезинфекции помещений: сухая и влажная уборка, химическая дезинфекция (с применением хлора, спирта и других чистящих средств), ультрафиолетовое обеззараживание. Данные методы либо не подходят для противомикробной обработки поверхностей (сухая уборка), либо требуют повторной уборки от остатков дезинфицирующей химии.

Оптимальным решением проблемы будет озонирование воздуха – процедура очищения воздуха в закрытом помещении с применением озона. Повышенная химическая активность делает его наиболее сильным из известных природных окислителей. Сталкиваясь с вредными соединениями,

молекулы озона стимулируют их распад, после чего снова превращаются в обычный кислород.

Преимущества применения озона:

– озон уничтожает все известные микроорганизмы, не существует и не может возникнуть устойчивых к озону форм микробов;

– полная дезинфекция в труднодоступных местах.

С помощью специального устройства – озонатора – газ выделяется из воздуха без применения химических веществ. Наиболее известные российские компании, осуществляющие продажу озонаторного оборудования: «Эконау» (г. Екатеринбург), «OzonBox» (г. Челябинск), «Ozondex» (г. Чебоксары). Несмотря на широкий ассортимент оборудования, предназначенного для различных отраслей промышленности, мощные озонаторы с выходом озона более 20 г/час имеют высокую стоимость. В качестве альтернативы предлагается разрабатываемая система дезинфекции воздуха.

В общем виде структурная схема системы дезинфекции представлена на рисунке 1:

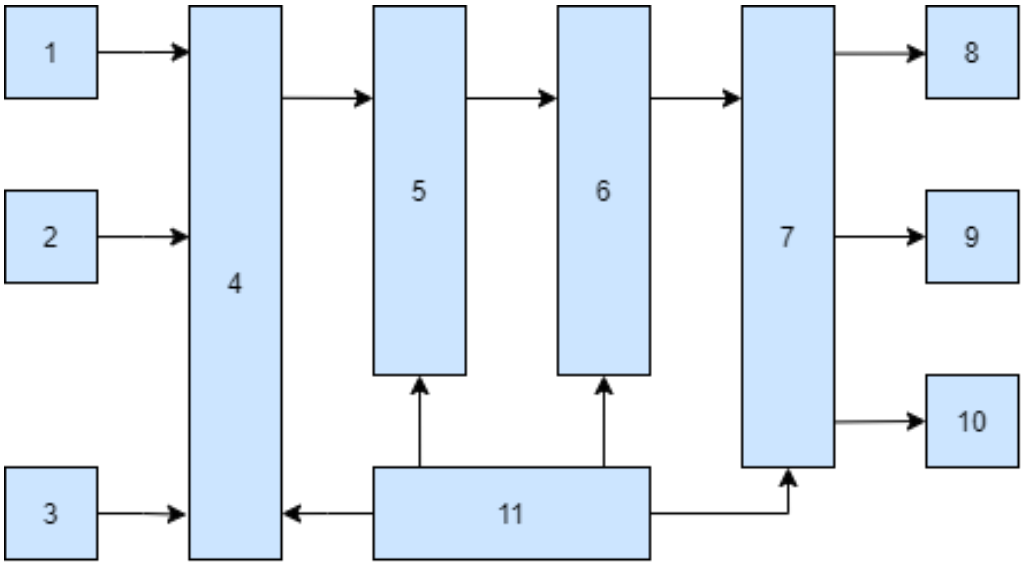


Рис. 1. Структурная схема системы вентилирования воздуха производственных помещений: *1* – датчик движения, *2* – датчик концентрации озона, *3* – датчик температуры, *4* – блок сбора информации о датчиках, *5* – блок обработки информации от датчиков, *6* – блок управления устройствами озонации, *7* – коммутатор устройств озонации, *8-10* – устройства озонации, *11* – блок питания

В качестве первичных измерительных преобразователей подходят современные датчики движения, температуры как с аналоговым, так и с цифровым выходом, высокочувствительные датчики озона. Для реализации тракта обработки сигнала от датчиков используются современные аналоговые операционные усилители, например производства Analog Devices [1], аналого-цифровые преобразователи ADS8862 (“Texas Instruments”).

Устройство генерации озона должно иметь герметичный корпус, для предотвращения попадания пыли и влаги на пластины, между которыми будет формироваться коронный разряд, генерирующий озон, прочный корпус для устойчивости к механическому воздействию, вибрациям. Предусматривается мощная система вентилирования для обеспечения охлаждения устройства и удаления остаточного озона из помещения.

При расчете продолжительности работы озонаторного оборудования используется существующая нормативно-правовая база: ГОСТ 31829-2012 [2], в котором изложены требования к безопасности озонаторного оборудования, и ГОСТ 12.1.007-76 [3], содержащий значения среднесуточной нормы и предельно допустимой концентрации озона.

Алгоритм работы системы описан в блок-схеме на рис. 2.

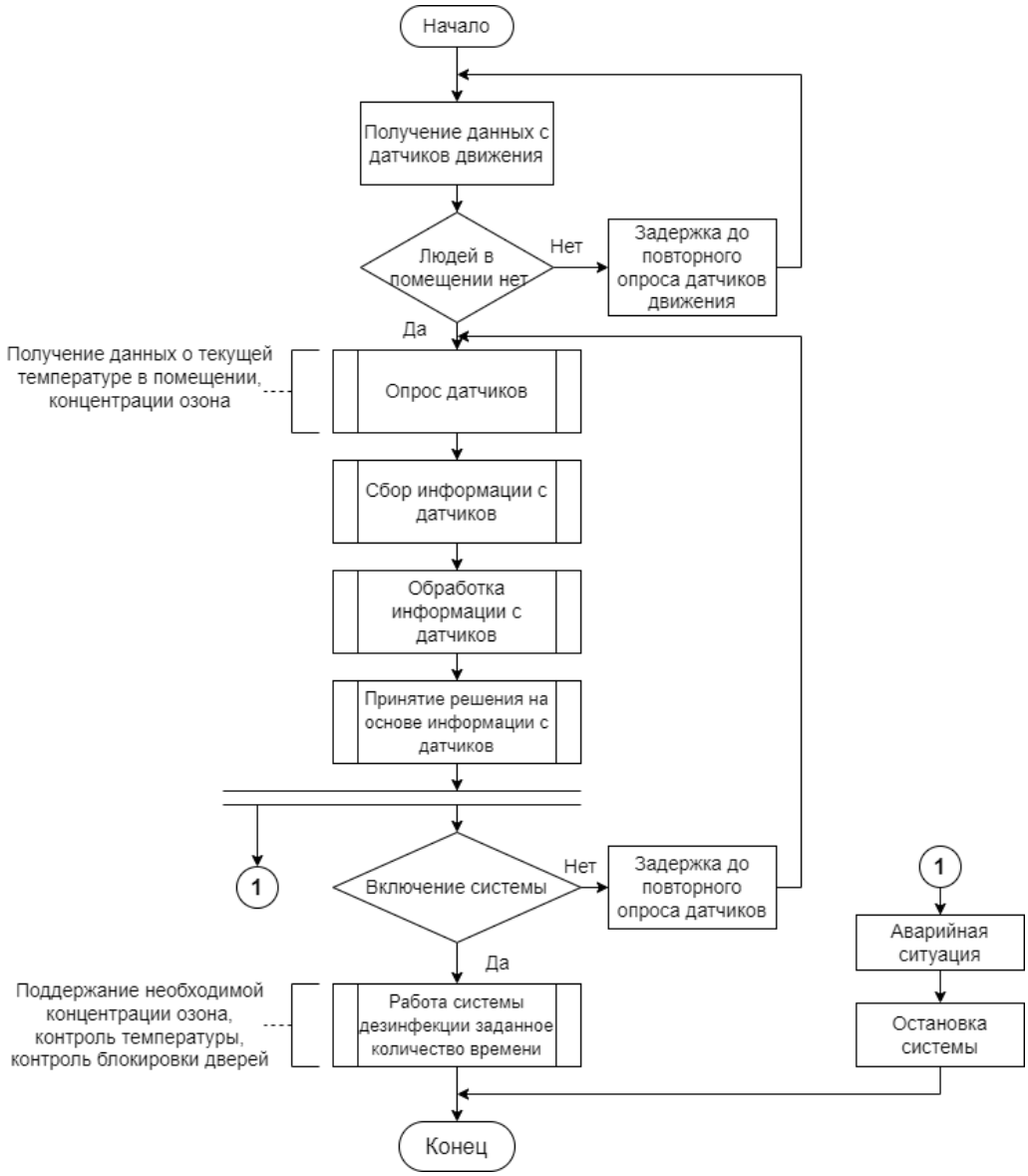


Рис. 2. Алгоритм работы системы вентилирования воздуха производственных помещений

Для описания и анализа работы аналоговых устройств используется математический аппарат передаточных функций, в частности преобразования Лапласа. Передаточная функция системы, на вход которой подается сигнал, вызывающий реакцию на выходе, задается выражением:

$$H(s) = \frac{Y(s)}{X(s)} = \frac{\prod_{k=1}^{m}(s - s_{zk})}{\prod_{k=1}^{n}(s - s_{pk})}, \quad (1)$$

где s_{zk} и s_{pk} – нули и полюсы системы; K – вещественный множитель (1).

В качестве примера в программном пакете Mathcad была рассчитана амплитудо-частотная характеристика фильтра низких частот (рис. 4). Принципиальная схема данного фильтра собрана в программе Multisim и приведена на рис. 3.

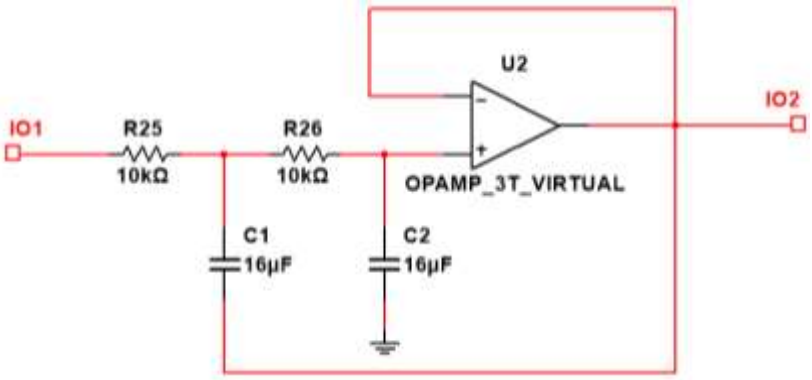


Рис. 3 Принципиальная схема фильтра низких частот

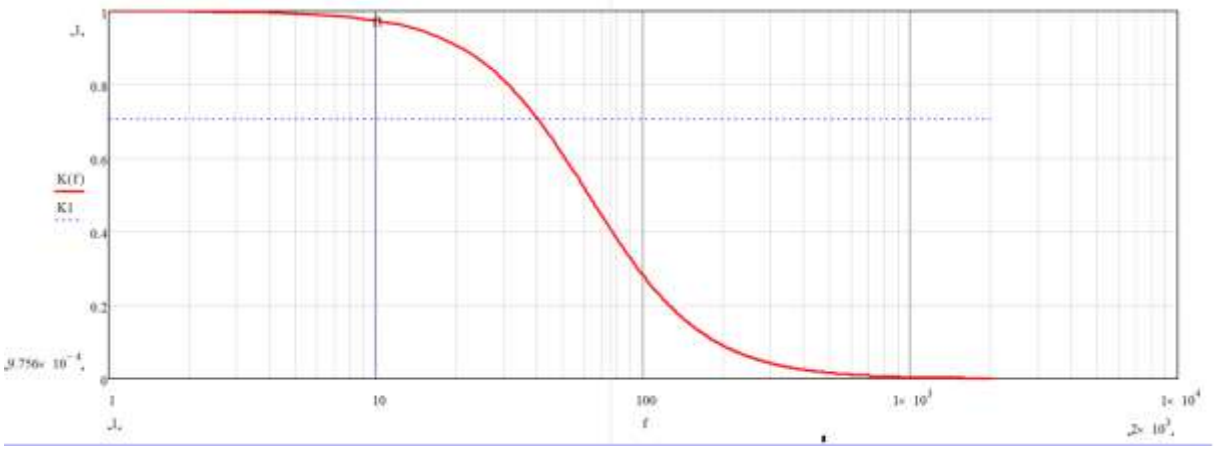


Рис. 4 Амплитудо-частотная характеристика фильтра низких частот

В статье представлена структурная системы дезинфекции, а также обосновывается выбор современной элементной базы для ее реализации. Разработан специальный алгоритм работы системы дезинфекции воздуха в закрытых помещениях предприятий, учитывающий безопасность персонала. Реализован выбор первичных измерительных преобразователей, предназначенных для контроля процесса очистки.

Список используемых источников

1. Сайт дистрибьютора продукции фирмы Analog Devices. URL: https://www.eltech.spb.ru/analog_devices (дата обращения: 29.03.2022);
2. ГОСТ 31829-2012 Оборудование озонаторное. Требования безопасности от 21.11.2012 с изм. и допол. в ред. от 01.04.2019;
3. ГОСТ 12.1.007-76 Система стандартов безопасности труда (ССБТ). Вредные вещества. Классификация и общие требования безопасности от 10.03.1976 с изм. И допол. в ред. от 01.04.2007.

Статья представлена заведующей кафедрой ИСАУ СПбГУТ, доктором технических наук, профессором Г. В. Верховой.

УДК 621.311.6
ГРНТИ 45.01.85

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЭЛЕКТРОПИТАНИЯ ДЛЯ БЛОКОВ УПРАВЛЕНИЯ АСУ

А. В. Ваганов, Д. С. Дмитриенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой системы электропитания, предназначенной для обеспечения стабильной и надежной работы электронных комплексов автоматизированных систем управления современных промышленных предприятий. Обосновывается актуальность разработки подобного класса систем. Представлена структурная схема системы, а также обосновывается выбор современной элементной базы для ее реализации. Разработан специальный алгоритм работы системы электропитания, учитывающий множество параметров: качество напряжения питающей сети, внешние факторы (температура, влажность и т. п.). Произведен выбор первичных измерительных преобразователей, предназначенных для контроля внешних параметров. Осуществлен выбор математического аппарата для расчета отдельных блоков системы. Приведены результаты моделирования и осуществлен их анализ. Даны рекомендации к конструкции аппаратной части.

интеллектуальная система, датчик, алгоритм управления, математическая модель, структурная схема.

Системы автоматизированного управления (АСУ) с каждым днем становится все более распространенными на современных производствах и внедряются практически повсеместно. Главной целью внедрения подобных систем является увеличение эффективности современных производств. Подобные системы позволяют оперативно анализировать изменения в структурах объекта управления (технологический процесс, сборочный

конвейер и др.), а также ускоряют принятие решений специалистами на местах. Различают автоматизированные системы управления объектами (технологическими процессами – АСУТП, предприятием – АСУП, отраслью – ОАСУ) и функциональные автоматизированные системы, например, проектирование плановых расчётов, материально-технического снабжения и т. д.

АСУ являются сложными устройствами с большим количеством электронных систем, для надежного функционирования которых требуется качественное электроснабжение, заключающееся в обеспечении бесперебойной работы всех электронных систем, минимизации влияния помех как внешней электросети, так и внутренних цепях питания (внутри прибора или модуля). Различные внешние факторы могут вызывать перебои во внешнем электроснабжении в виде пропадания напряжения питающей электросети или мощные скачки напряжения в ней, например, из-за грозы.

Классическим решением данной проблемы является применение источников бесперебойного питания (ИБП) [1]. ИБП производятся множеством мировых компаний, например таких как: Siemens, Emerson Electric Company, Cisco и др. А также отечественными фирмами: Штиль, Энергия.

Анализ данных решений позволил выявить следующие их преимущества и недостатки. К преимуществам следует отнести: надежность, отказоустойчивость, наличие встроенного электроисточника, стабильная работа от первичной сети в широком диапазоне напряжений (от 90 до 280 вольт). В качестве основных недостатков следует отметить: сложность установки из-за крупных габаритов, недостаточную гибкость систем при решении нестандартных задач, сложная настройка оборудования, требующая участия специалистов, высокая стоимость (инверторные системы), а главное – это отсутствие интеллектуальной системы, которая позволила бы осуществить прогнозирование и предотвращение аварийных ситуаций.

Устранение указанных недостатков возможно в случае применения новой системы электропитания, которая кроме традиционных функций данного класса систем ещё обладала бы и интеллектуальной системой прогнозирования – ИСЭП.

Структурная схема подобной системы приведена на рис. 1.

В качестве первичных измерительных преобразователей вполне подходят как отечественные, так и зарубежные решения, имеющие необходимый рабочий диапазон и требуемую погрешность измерения [2].

Функционирование ИСЭП осуществляется на основе специально разработанного алгоритма ее работы, учитывающего множество параметров как внешней сети питания, так и окружающей среды. Именно благодаря отслеживанию и анализу внешних параметров таких как: температура, влажность, вибрация и др. ИСЭП может оперативно на них реагировать на их опасное изменение и предотвращать негативные ситуации для электронных систем АСУ. Функционирование алгоритма заключается в следующем.

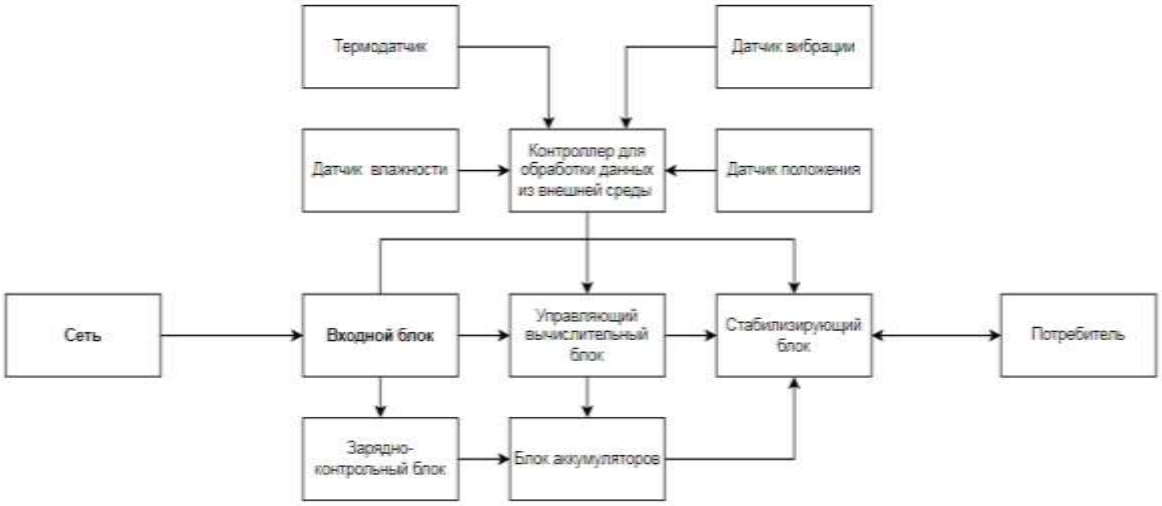


Рис. 5. Структурная схема интеллектуальной системы электропитания

Сначала инициализируются порты, производится опрос подключенных к ним датчиков, выясняется состояние окружающей среды, проверяется влажность, температура, уровень вибрации в помещении и положение системы.

Если все в порядке, то отключается питание от сети переменного тока и производится контроль встроенного аккумулятора, если напряжение на нем ниже нормы, то система выдает предупреждение. Если батарея исправна, то производится контроль напряжения на измерительной обмотке трансформатора – если сеть не исправна, то выполняется отключение от сети.

Алгоритм работы изображен в виде блок-схемы на рис. 2.

Как следует из рис. 1 ИСЭП содержит множество

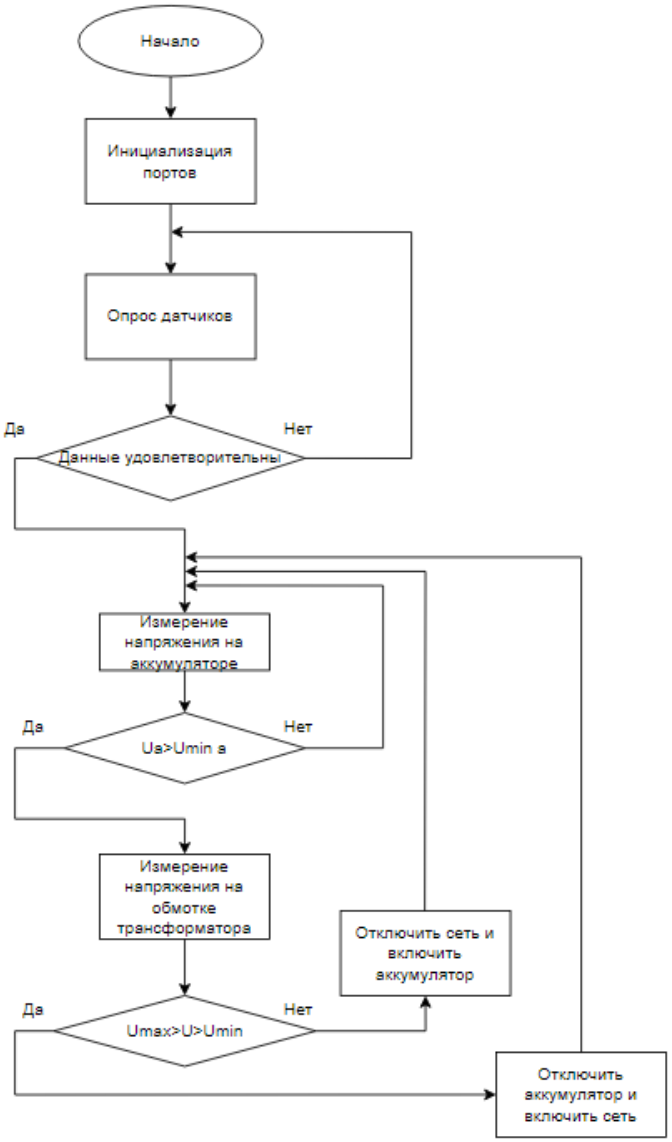


Рис. 2. Алгоритм работы системы

блоков и элементов. В качестве математического аппарата для расчета и моделирования ее элементов использованы математические модели на функционально-логическом уровне (аппарат передаточных функций). В качестве наглядного примера рассмотрен фрагмент входного блока, а именно противопомеховый фильтр (рис. 3) [3].

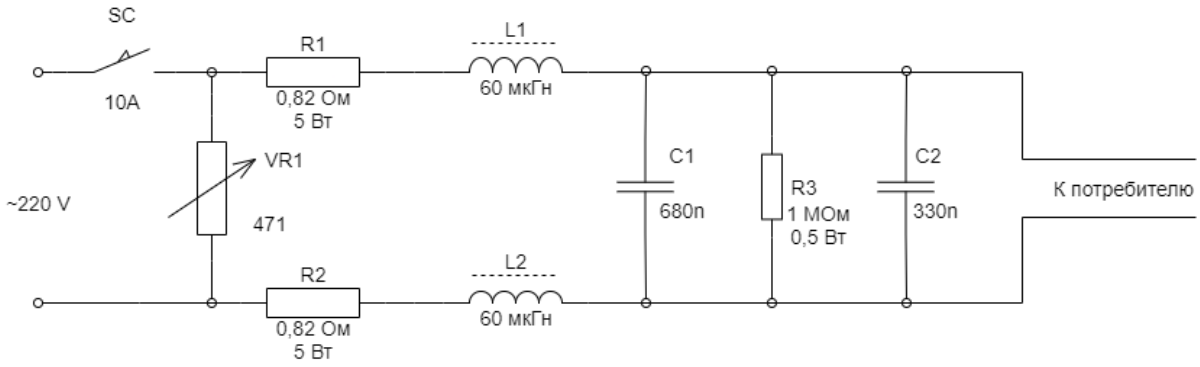


Рис. 3. Схема фильтра входного блока

Токовый ключ SC обеспечивает защиту подключенных потребителей от перегрузок и токов коротких замыканий.

Высокоомный резистор R3 на (1-10 Мом) выполняет функцию разряда конденсатора C1 при выключении питания, обеспечивая возможность безопасного обслуживания.

Для анализа аналоговых цепей фильтра входного блока используется математический аппарат, полученный с помощью преобразования Лапласа. Аппроксимация его передаточной функции представлена ниже:

$$H(f) = \frac{R_{C\text{общ}(f)}}{(R_1 + R_{L1(f)} + R_{C\text{общ}(f)} + R_{L2(f)} + R_2)}, \quad (1)$$

где

$$R_{L1} = 2\pi f L_1, R_{L2} = 2\pi f L_2,$$

$$R_{C\text{общ}} = \frac{1}{2\pi f C_{\text{общ}}},$$

$$C_{\text{общ}} = C_1 + C_2.$$

Результат моделирование данного фильтра показан на рисунке 4. Исследование производилось с применением математического пакета MathCAD.

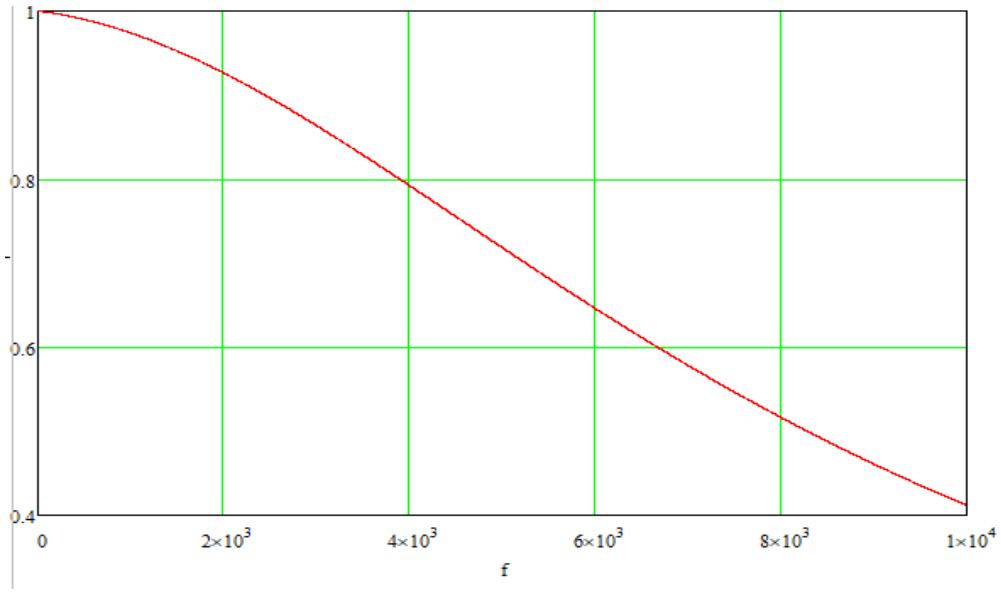


Рис. 4. График передаточной функции противопомехового фильтра входного блока

По результатам моделирования сделан вывод, что на частоте в 10 кГц подавление помех происходит с эффективностью более 50 %, что свидетельствует о достаточной его эффективности против более высокочастотных помех (f > 100 кГц). При этом на частоте 50 Гц коэффициент передачи близок к 1.

В статье были рассмотрены задачи проектирования интеллектуальной системы электропитания, обеспечивающей более эффективное и надежное функционирование электронных систем АСУ современных предприятий по сравнению с традиционными СЭП за счет применения блока анализа качества питающей сети и внешних параметров среды.

Осуществлен синтез структуры и приведено описание блоков, входящих в ИСЭП. Рассмотрен пример структурной реализации фрагмента системы электропитания с проведением его исследования в специализированном математическом пакете.

Список используемых источников

1. Белоусов О. А., Муромцев Д. Ю. Электропитание систем радиосвязи: учебное пособие. Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2016. 84 с. ISBN 978-5-8265-1533-4.

2. Anadigm, the dpASP company. URL: https://anadigm.com/ (дата обращения: 15.01.2021).

3. Сетевые фильтры – как они работают. URL: https://radiostorage.net/4817-setevye-filtry-kak-oni-rabotayut-primery-skhem.html (дата обращения: 19.02.2021).

УДК 004.021
ГРНТИ 50.51.15

ГЕНЕРАЦИЯ И/ИЛИ-ДЕРЕВА ДЛЯ МОРФОЛОГИЧЕСКОГО МНОЖЕСТВА, ЗАДАННОГО НА ЯЗЫКЕ STRUCTURALIST

М. А. Васильев, Г. В. Верхова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящёна преобразованию описания морфологического множества, представленного на языке Structuralist, в И/ИЛИ-дерево. В работе приведено описание структур дерева, соответствующих основным конструкциям на языке Structuralist: агрегации, определению классификационных признаков и ограничению на классификационные признаки. Представлен способ преобразования, состоящий из двух этапов: создание модели морфологического множества по тексту на языке Structuralist и создание И/ИЛИ-дерева по данной модели. Указан порядок действий для выполнения обоих этапов и представлена блок-схема для второго этапа. Описана объектная модель, используемая при выполнении преобразования. Приведён пример преобразования.

структурно-параметрический синтез, морфологическое множество, И/ИЛИ-дерево.

При проектировании системных объектов автоматизация решения задачи структурно-параметрического синтеза, как правило, ограничена верификацией или моделированием варианта объекта, созданного человеком. Системы же автоматизированного проектирования, которые способны выполнять синтез автоматически, используют для этого специфические для своей предметной области методы.

Система структурно-параметрического синтеза, основанная на четырёхуровневой интегративной модели [1], для синтеза использует морфологическое множество создаваемого объекта. Каждое решение в таком множестве имеет специальный идентификатор, а множество всех идентификаторов представлено в виде И/ИЛИ-дерева (идентификатор выбирается путём вырождения [2] ИЛИ-вершин дерева). Такое дерево генерируется по описанию морфологического множества, заданному на языке *Structuralist* [3].

Таким образом, объектом исследования является автоматизация структурно-параметрического синтеза, а предметом – генерация множества идентификаторов решений системного объекта в виде И/ИЛИ-дерева по описанию морфологического множества, данного на языке *Structuralist*.

Основными конструкциями языка *Structuralist* являются определения модуля, его классификационных признаков (КП), ограничений классификационных признаков (ОКП) и правил генерации подмодулей (ПГП).

Определение модуля представляет собой списки КП, ОКП и ПГП. По определению модуля строится дерево, содержащее идентификаторы всех структурных решений объекта.

КП представляет собой свойство объекта, имеющее название и конечное число возможных принимаемых значений.

ОКП – это зависимость возможных значений одного признака от значений других.

ПГП определяет, при каких значениях некоторых КП необходимо сгенерировать дочерний модуль (или несколько модулей).

В результате работы синтаксического и семантического анализаторов текст на языке *Structuralist* преобразуется в промежуточную модель морфологического множества, типы объектов которой и отношения между ними показаны на рис. 1.

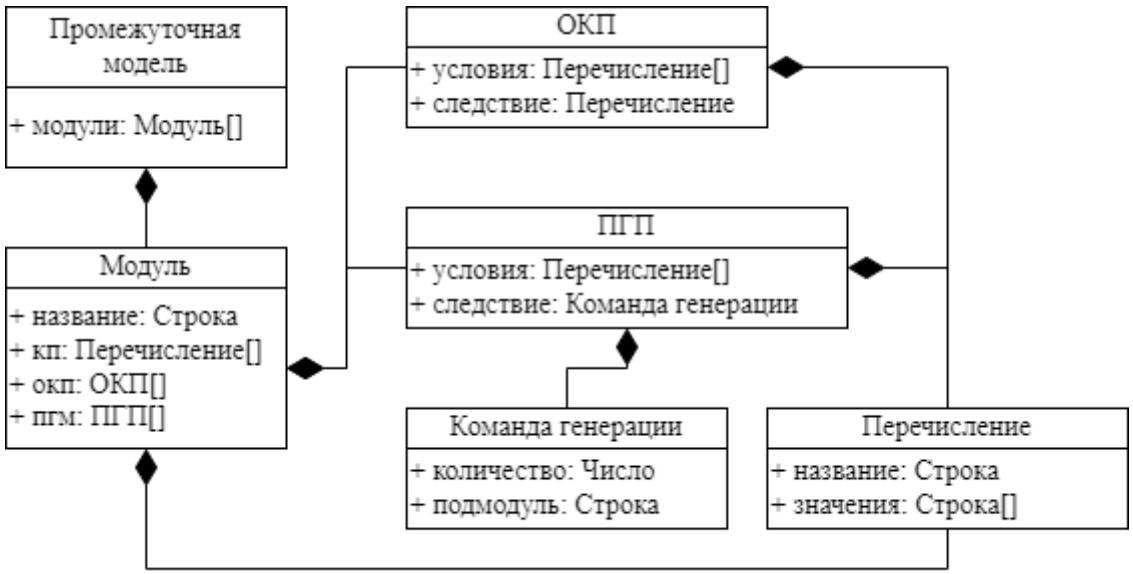


Рис. 1. Типы объектов промежуточной модели и отношения между ними

В упрощённом виде алгоритм построения такой модели выглядит следующим образом:

1. Прочитать очередную конструкцию *Structuralist*.

2. Проверить, что конструкция находится на верном уровне (признаки, ограничения и правила не объявляется вне модуля).

3. Проверить порядок признаков в ограничении – признаки, определённые позднее, не могут ограничивать признаки, определённые ранее.

4. Если конструкция прошла проверки, добавить её в промежуточную модель, иначе выдать ошибку.

5. Если входные данные закончились, завершить создание промежуточной модели, иначе вернуться к пункту 1.

На основе построенной модели для любого модуля в ней можно построить И/ИЛИ-дерево. Для этого необходимо:

1. Сгенерировать базовое дерево на основе КП модуля.
2. Преобразовать дерево, применив ОКП.
3. Преобразовать дерево, применив ПГП.

Чтобы показать, как выполняются эти шаги, введём несколько типов:

$$V\text{: строка} - \text{значение КП},$$

$$FID\text{: строка} - \text{название КП},$$

$$VS: \{V_1, \dots, V_n\},$$

$$FIDS: \{FID_1, \dots, FID_m\},$$

где $FIDS$ – упорядоченное множество. Также определим функцию

$$F_f: FID \to VS,$$

которая для текущего модуля будет возвращать все возможные значения КП по его названию. Дерево определим через взаимную рекурсию:

$$T: \langle type, FID|nil, VS, F\rangle,$$

$$F: \{T_1, \dots, T_k\},$$

$$type \in \{and, or\},$$

где $FID|nil$ означает, что значение может быть либо пустым, либо иметь тип FID. Тогда функция BT_f создания базового дерева может быть определена следующим образом:

$$S_f: FID, VS \to T,$$

$$S_f(fid, \{v_1, \dots, v_n\}) = \langle or, nil, \emptyset, \{\langle or, fid, \{v_1\}, \emptyset\rangle, \dots, \langle or, fid, \{v_n\}, \emptyset\rangle\}\rangle$$

$$BT_f: FIDS \to T,$$

$$BT_f: (fs) =$$

$$|fs| = 1 \to \langle and, \min fs, F_f(\min fs), \{S_f(\min fs, F_f(\min fs))\}\rangle;$$

$$|fs| > 1 \to$$

$$\langle and, \min fs, F_f(\min fs), \{S_f(\min fs, F_f(\min fs)), BT_f(fs \setminus \min fs)\}\rangle.$$

После генерации базового дерева к нему необходимо применить по очереди каждое ОКП. Введём несколько вспомогательных типов:

$$ENUM: \langle FID, VS \rangle,$$
$$ENUMS: \{ENUM_1, \dots, ENUM_q\},$$
$$CON: \langle ENUMS, ENUM \rangle.$$

Тип CON – это формализация ОКП. Первый элемент типа $ENUMS$ представляет условия ОКП, а второй элемент типа $ENUM$ – ограничиваемый КП. Тогда функция C_f применения к дереву ОКП определяется так:

$$C_f: T, CON \to T,$$
$$C_f(\langle and, fid, vs, \{l, r\}\rangle, \langle cond, cons\rangle) =$$
$$\exists c = \langle fid_c, vs_c\rangle \in cond: fid = fid_c, vs \cap vs_c \neq \emptyset, vs \setminus vs_c \neq \emptyset \to$$
$$\langle or, nil, \emptyset, \{\langle and, fid, vs \cap vs_c, \{S_f(fid, vs \cap vs_c), C_f(r, \langle cond, cons\rangle)\}\rangle,$$
$$\langle and, fid, vs \setminus vs_c, \{S_f(fid, vs \setminus vs_c), r\}\rangle\}\rangle;$$
$$\exists c = \langle fid_c, vs_c\rangle \in cond: fid = fid_c, vs \cap vs_c = vs \to$$
$$\langle and, fid, vs, \{l, C_f(r, \langle cond, cons\rangle\}\rangle;$$
$$\nexists c = \langle fid_c, vs_c\rangle \in cond: fid = fid_c \to \langle and, fid, vs, \{l, C_f(r, \langle cond, cons\rangle\}\rangle;$$
$$cons = \langle fid_c, vs_c\rangle, fid = fid_c, vs \cap vs_c \neq \emptyset \to$$
$$\langle and, fid, vs \cap vs_c, \{S_f(fid, vs \cap vs_c), r\}\rangle;$$
$$C_f(\langle and, fid, vs, \{l\}\rangle, \langle cond, \langle fid, vs_c\rangle\rangle) =$$
$$vs \cap vs_c \neq \emptyset \to \langle and, fid, vs \cap vs_c, \{S_f(fid, vs \cap vs_c)\}\rangle;$$
$$C_f(\langle or, nil, \emptyset, \{t_1, \dots, t_k\}\rangle, con) =$$
$$\langle or, nil, \emptyset, \{C_f(t_1, con), \dots, C_f(t_k, con)\}\rangle.$$

Стоит отметить, что функция в таком виде не учитывает возможные «мёртвые» ветки, когда у КП не остаётся ни одного возможного значения. В случае возникновения такой ситуации, можно либо удалить такую ветку, либо выдать ошибку.

Пример дерева после применения к нему ОКП показан на рис. 2.

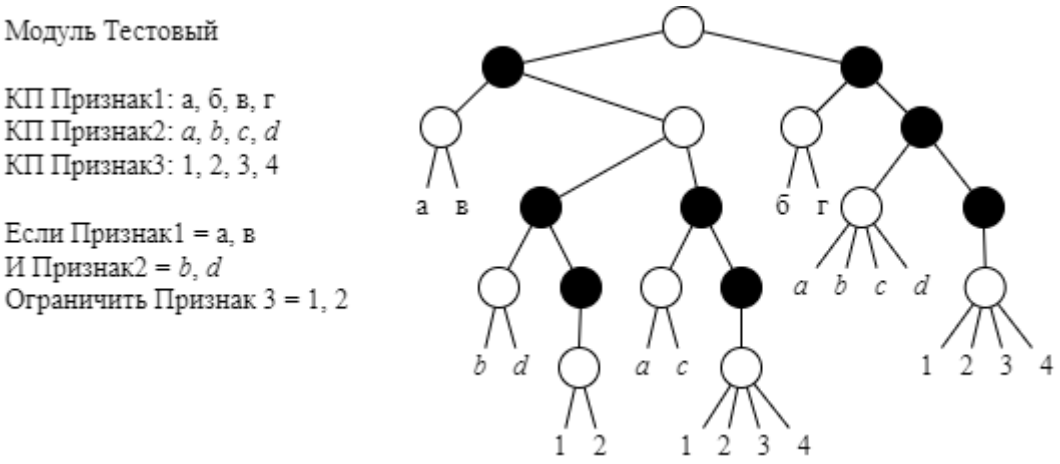
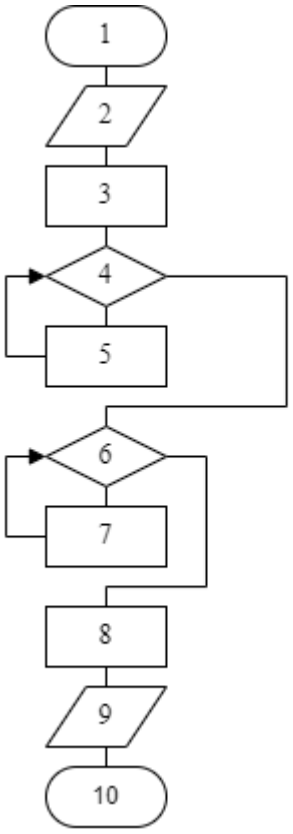


Рис. 2. Пример преобразования дерева по ОКП

После применения всех ОКП аналогично применяются ПГП. ПГП трансформирует дерево подобно ОКП, но вместо удаления лишних значений КП на последнем этапе оно отслеживает, были ли применены все условия. После применения всех условий ПГП добавляет к текущей вершине необходимое количество дочерних вершин, которые затем становятся корневыми для подмодулей.

В общем виде алгоритм генерации И/ИЛИ-дерева по промежуточной модели представлен на рис. 3.



1. Начало.
2. Входные данные - промежуточная модель и выбранный модуль.
3. Генерация базового дерева.
4. Цикл для всех ОКП.
5. Применить ОКП.
6. Цикл для всех ПГП.
7. Применить ПГП.
8. Сгенерировать подмодули.
9. Выходные данные - И/ИЛИ-дерево.
10. Останов.

Рис. 3. Алгоритм преобразования промежуточной модели в И/ИЛИ-дерево

Список используемых источников

1. Васильев М. А. Разработка интеллектуальной системы структурно-параметрического синтеза // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей; сб. лучших докладов конф. / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2022. С. 332–335.
2. Морфологическое И/ИЛИ-дерево // Structuralist проблемы автоматизации структурно-параметрического синтеза. URL: http://www.structuralist.narod.ru/ dictionary/morphtree.htm (дата обращения: 21.11.2021).
3. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS : монография. СПб. : СПбГУТ. 2018. 187 с.

УДК 004.428
ГРНТИ 20.15.13

СРАВНЕНИЕ МИКРОСЕРВИСНОГО И МОНОЛИТНОГО ПОДХОДОВ К РЕАЛИЗАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ ПОСТОЯННОЙ СМЕНЫ ЕГО РАЗРАБОТЧИКОВ

Н. А. Васильев, А. О. Кудрявцев, М. А. Румянцев

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В статье проведено сравнение микросервисного и монолитного подходов к реализации программного обеспечения, выявлены их достоинства и недостатки. Проанализирована возможность долгосрочной разработки и сопровождения монолитного и микросервисного программного обеспечения в условиях постоянной смены разработчиков.

архитектура программного обеспечения, монолитная архитектура, модульная архитектура, микросервисная архитектура, командная разработка, авторская разработка.

Введение

В последние годы программисты все чаще меняют своё место работы, особенно это касается небольших IT-компаний. Задачи таких компаний могут включать в себя необходимость долгосрочной разработки сложного программного обеспечения. Для его создания необходимо не только выбрать правильный архитектурный подход, но и учитывать то, что из-за объема задачи и необходимого времени на её выполнение вести разработку могут раз-

ные программисты, со своими соответствующими знаниями языков программирования, навыками использования инструментов разработки, общим видением проекта [1].

Существует множество архитектурных подходов к разработке программного обеспечения. К ним можно отнести архитектуру каналов и фильтров, многоуровневую архитектуру, архитектуру, управляемую событиями, микроядерную архитектуру, модульную архитектуру и микросервисную архитектуру. С ростом сложности разрабатываемых программных систем, увеличением времени их разработки и необходимостью дальнейшего сопровождения одни архитектурные подходы устаревают, им на смену появляются новые. На сегодняшний день популярными архитектурными подходами для разработки сложных программных систем являются монолитный и микросервисный [2–4]. Оба подхода повсеместно применяются при разработке программного обеспечения любой сложности, однако имеют свои достоинства и недостатки.

Статья посвящена сравнению монолитного и микросервисного подходов к разработке сложного программного обеспечения и выбору оптимального из них с учетом как достоинств и недостатков самих архитектурных подходов, так и проблемы долгосрочной реализации и сопровождения такого программного обеспечения в условиях постоянной смены разработчиков.

Монолитная архитектура

Архитектура – это базовая организация системы, которая описывает связи между компонентами этой системы (и внешней средой), а также определяет принципы её проектирования и развития. Однако многие другие определения архитектуры признают не только структурные элементы, но и их композиции, а также интерфейсы и другие соединительные звенья.

Монолитная (модульная) архитектура (рис. 1) позволяет разрабатывать приложения, которые можно разделить на ряд функциональных блоков (модулей), которые в совокупности между собой являются единым целым. Доработка такого

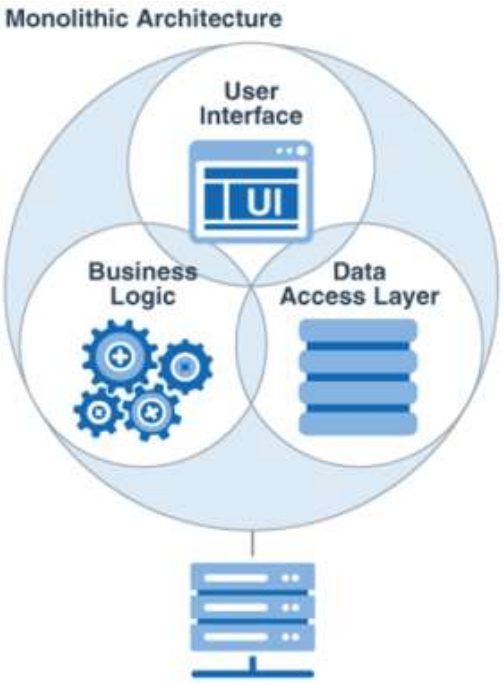


Рис. 1. Архитектурная схема монолитного (модульного) приложения

приложения состоит в создании модулей с недостающим функционалом. Новые модули получаются путём переиспользования частей монолита (ядра или других модулей). Бизнес-логика прописывается внутри монолита: для программы (приложения, сайта, портала) есть одна точка входа и одна точка выхода.

Достоинства монолитной архитектуры

Большим преимуществом монолитного программного обеспечения является то, что его относительно легко реализовать. В приложении с монолитной архитектурой можно быстро начать разрабатывать свою бизнес-логику, вместо того чтобы тратить время на размышления о взаимодействии его отдельных частей.

Из-за отсутствия большого числа независимых частей монолитное программное обеспечение легче тестировать, так как нет необходимости подключать множество необходимых сервисов и их зависимостей.

Монолитные приложения легко развертывать, масштабировать и эксплуатировать. Для развертывания можно использовать скрипт, загружающий модули и запускающий приложение. Масштабирование достигается путем размещения Loadbalancer перед несколькими экземплярами приложения.

Недостатки монолитной архитектуры

Основным недостатком монолитного приложения является сложность добавления в него нового функционала. Проблема заключается в том, что все монолитные системы не предназначены для серьёзного переопределения функционала. Код таких приложений, как правило, перерождаются из своего исходного, чистого состояния в так называемый нечитаемый и неподдерживаемый. Это состояние возникает, потому что архитектурные правила, со временем, все сильнее нарушаются, что приводит к срастанию частей приложения.

Это перерождение замедляет процесс разработки: каждую будущую функцию будет сложнее развивать. Из-за того, что компоненты растут вместе, их также необходимо переопределять вместе. Создание новой или переопределение существующей функции может означать прикосновение к нескольким различным местам. Когда происходит много переопределений, монолитное приложение существенно изменяется. Важно помнить, что зависимость между объёмом нового функционала и количеством модулей монолитного приложения нелинейная: для добавления одной функции нужно либо внести изменения в несколько модулей, каждый из которых меняет работу другого, либо в новом модуле переопределить большое количе-

ство методов других модулей, что в целом, не меняет сути. После всех изменений система так усложняется, что для добавления следующих доработок будет требоваться огромное количество часов.

Следующая проблема монолитных приложений – сильная связность кода. При добавлении новой или переопределении существующей функции, из-за сильной связности компонентов в монолитном приложении необходимо изменить кодовую базу во многих местах, что может породить большое количество багов, появление ошибок в работающем до этого функционале.

Еще одна проблема монолитных приложений заключается в сложности их документирования. Документацию для таких систем сложно поддерживать в актуальном состоянии. Её много, и она устаревает с каждым изменением. Доработка одного модуля влечёт изменения в нескольких документах (в пользовательской, технической документации), и все их нужно переписывать.

Микросервисная архитектура

Микросервисная архитектура (рис. 2) позволяет разрабатывать приложения, разбитые на множество небольших сервисов, называемых микросервисами. Каждый микросервис включает в себя бизнес-логику и представляет собой совершенно независимый компонент. Сервисы одной системы могут быть написаны на различных языках программирования и общаться друг с другом, используя различные протоколы.

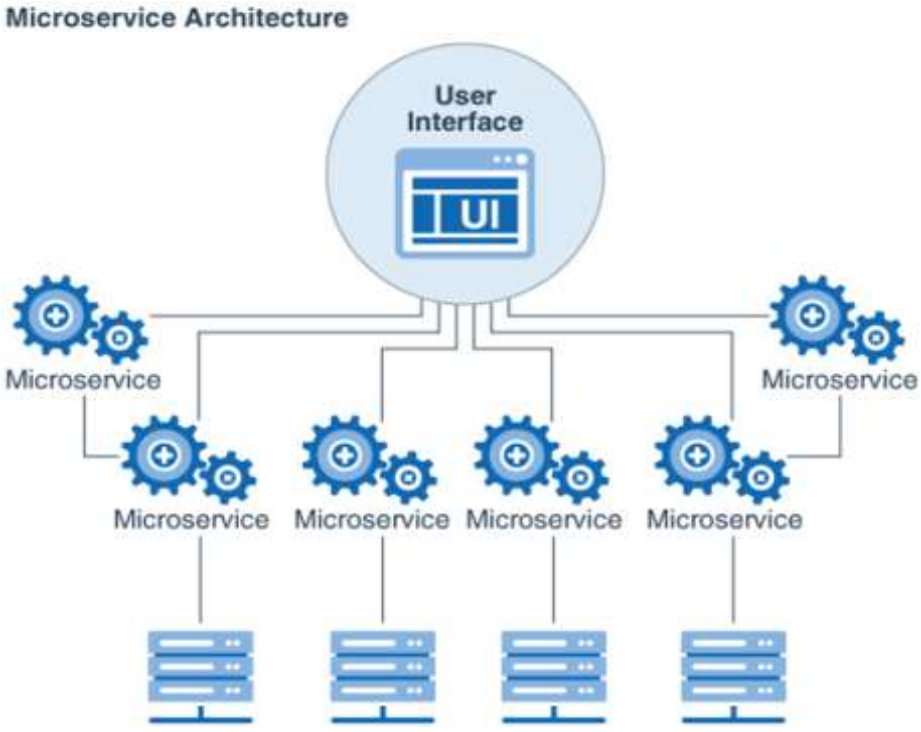


Рис. 2. Архитектурная схема микросервисного приложения

Поскольку каждый микросервис является отдельным проектом, то существует возможность распределения работы над ними между командами разработчиков, таким образом над системой могут одновременно трудиться несколько десятков программистов. Микросервисная архитектура позволяет с легкостью масштабировать приложение – если есть необходимость внедрить новую функцию (развертывать каждый микросервис можно по отдельности), то можно просто написать новый сервис, а если какой-то функцией никто не пользуется – отключить соответствующий сервис.

Достоинства микросервисной архитектуры

Основным преимуществом микросервисного программного обеспечения является его отказоустойчивость. Части (сервисы) микросервисного программного обеспечения изолированы друг от друга, за счет чего приложение может продолжать эффективно работать даже тогда, когда какой-то из его сервисов неисправен.

Микросервисные приложения сильно масштабируемы за счет того, что каждую его часть можно развертывать независимо от других на разных серверах.

Микросервисные приложения отлично документируются, а новым разработчикам легче погружаться в кодовою базу проекта из-за небольшого количества кода каждого сервиса, а также отсутствия их связности. Их легко расширять и поддерживать, при этом отсутствует приверженность приложения к одному стеку технологий – сервисы одной системы могут быть написаны на различных языках программирования и общаться друг с другом, используя различные протоколы.

Недостатки микросервисной архитектуры

К основным недостаткам микросервисной архитектуры можно отнести следующие: сложность разработки приложения на начальном этапе, сложность тестирования и сложность развертывания.

Сложность разработки микросервисного приложения, в сравнении с монолитным, заключается в том, что перед началом реализации своей бизнес-логики необходимо продумать сценарии взаимодействия сервисов между собой. Однако на дистанции микросервисные приложения легче разрабатывать и поддерживать, чем монолитные (модульные) за счет отсутствия сильной связности кода и возможности выносить новые функции в отдельные сервисы. Объем разработанного функционала микросервисного приложения, со временем, постепенно выравнивается и, в последствии, обгоняет объем функционала того же самого приложения, если бы оно разрабатывалось с использованием монолитного подхода к разработке (рис. 3).

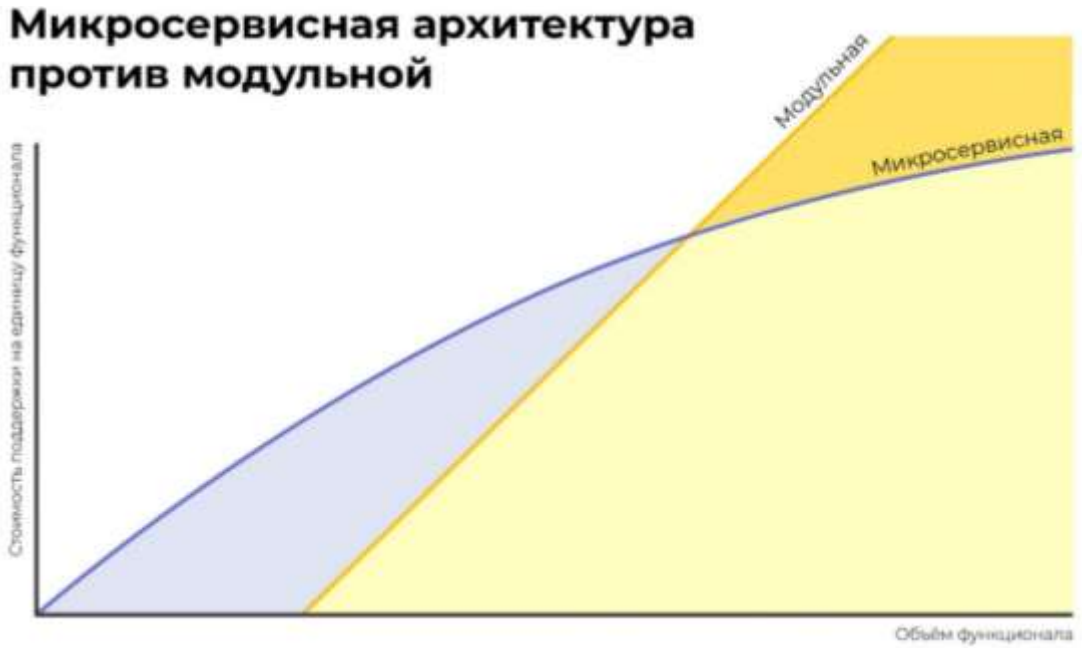


Рис. 3. Зависимость сложности внедрения нового функционала в приложение в зависимости от его архитектуры

Сложность тестирования заключается в том, что для его проведения необходим запуск всех необходимых сервисов, которые могут находится на разных машинах, в отличие от монолитного (модульного) приложения, для которого необходимо запустить скрипт для его запуска только на одной машине.

Сложность развертывания также заключается в необходимости запуска и настройки множества сервисов, находящихся на разных машинах, а также настройке их взаимодействия друг с другом.

Заключение

Сравнив достоинства и недостатки двух архитектурных подходов к программной разработке, можно прийти к выводу, что при долгосрочной реализации программного обеспечения в условиях постоянной смены его разработчиков необходимо использовать микросервисную архитектуру. Несмотря на необходимость проработки на начальном этапе создания приложения сценариев взаимодействия сервисов друг с другом и алгоритма его развертывания, микросервисное приложение, по сравнению с монолитным, имеет ряд критически важных положительных сторон.

Во-первых, микросервисные приложения хорошо документируемы, а сама документация постоянно поддерживается в актуальном состоянии из-за отсутствия каких-либо изменений в коде сервисов при добавления нового функционала, что обеспечивает возможность обеспечения преемственности работы.

Во-вторых, погрузиться в разработку таких приложений легче, так как новым программистам нет необходимости изучать всю существующую кодовую базу для добавления в проект нового функционала – они могут самостоятельно, с нуля, написать свой сервис, выполняющий необходимую функцию.

В-третьих, нет необходимости подбирать для продолжения работы программистов, знающих какой-то конкретный стек технологий – сервисы одного приложения могут быть разработаны на разных языках программирования с использованием различных фреймворков.

Список используемых источников

1. Tregubov A., Boehm B., Rodchenko N., Lane J. A.. Impact of Task Switching and Work Interruptions on Software Development Processes // ICSSP 2017: Proceedings of the 2017 International Conference on Software and System Process, 2017. pp. 134–138.

2. Chavan P. U., Murugan M. and Chavan P. P. A Review on Software Architecture Styles with Layered Robotic Software Architecture // 2015 International Conference on Computing Communication Control and Automation, 2015. pp. 827–831.

3. AI-Debagy O., Martinek P. A Comparative Review of Microservices and Monolithic Architectures, 2019.

4. Gos K., Zabierowski W. The Comparison of Microservice and Monolithic Architecture // 2020 IEEE XVIth International Conference on the Perspective Technologies and Methods in MEMS Design, 2020. pp. 150–153.

Статью представил начальник отдела организации научной работы и переподготовки научных и педагогических кадров ВАС, кандидат технических наук, доцент, полковник Д. О. Федосеев.

УДК 004.42
ГРНТИ 50.41.25

МОДЕЛЬ АВТОМАТИЗИРОВАННОГО УЧЕТА ЛИЧНЫХ ДОСТИЖЕНИЙ ФИЗИЧЕСКИХ ЛИЦ В РАМКАХ ОБЪЕДИНЕННЫХ ИНТЕРОПЕРАБЕЛЬНЫХ КИБЕРФИЗИЧЕСКИХ СРЕД

Г. В. Верхова, Э. Р. Крылова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из основных целей формирования единой киберсреды является сокращение рутинных операций при заполнении всевозможных бланков и форм, которые в настоящее время отнимают у сотрудников и учащихся значительную часть рабочего времени.

В статье предложена модель автоматизированного учета личных достижений физических лиц, осуществляемого в рамках объединенных интероперабельных киберсред виртуальных предприятий. Особенностью интероперабельных киберфизических сред является возможность бесшовной интеграции в глобальную киберфизическую среду. Личные достижения физического лица аккумулируются в электронном портфолио, представляющий собой открытую информационную систему, которая может взаимодействовать и интегрироваться с другими информационными системами для обмена информацией методом «нажатия одной кнопки».

киберфизическая среда, киберсреда, электронное портфолио, виртуальные предприятия, Индустрия 4.0, цифровой двойник.

В настоящее время все сферы современного общества находятся в процессе цифровой трансформации с использованием различных информационных технологий. В частности, различные предприятия находятся в процессе цифровизации, создавая цифровых двойников для эффективного контроля процессов и сокращения рутинных операций. Именно поэтому тема автоматизированного учета личных достижений физических лиц в рамках объединенных интероперабельных киберфизических сред актуальна в настоящее время, поскольку она напрямую связана с цифровизацией любой организации, включая образовательные, государственные, медицинские организации, различные предприятия и компании.

Киберфизические системы – это сложные спроектированные системы, объединяющие физические, программные и сетевые аспекты. Концепция киберфизических систем состоит из технологий, которые обеспечивают связь и взаимодействие между машинами, людьми и другими компонентами [1].

Электронное портфолио физического лица выступает в качестве системы мониторинга над успеваемостью, освоения компетенций, а также курирование результатов научно-исследовательской, учебной и профессиональной деятельностей участника киберсреды. Данная система обеспечивает эффективное планирование и оценивание процесса распределения кадровых ресурсов. По причине необходимости работы с большим объемом информации для управления персоналом, возникает проблема обмена данных между различными информационными системами. Для решения проблемы были сформированы международные стандарты, разрабатываемые с целью обозначения требований к взаимодействию информационных систем, а также упрощению обмена и управления данными между предприятиями. Такими разработками занимались международные консорциумы EuroPortfolio Consortium на базе EIfEL, HR-XML Consortium, Inter/National Coalition for Electronic Portfolio Research и IMS Global Learning Consortium Inc.

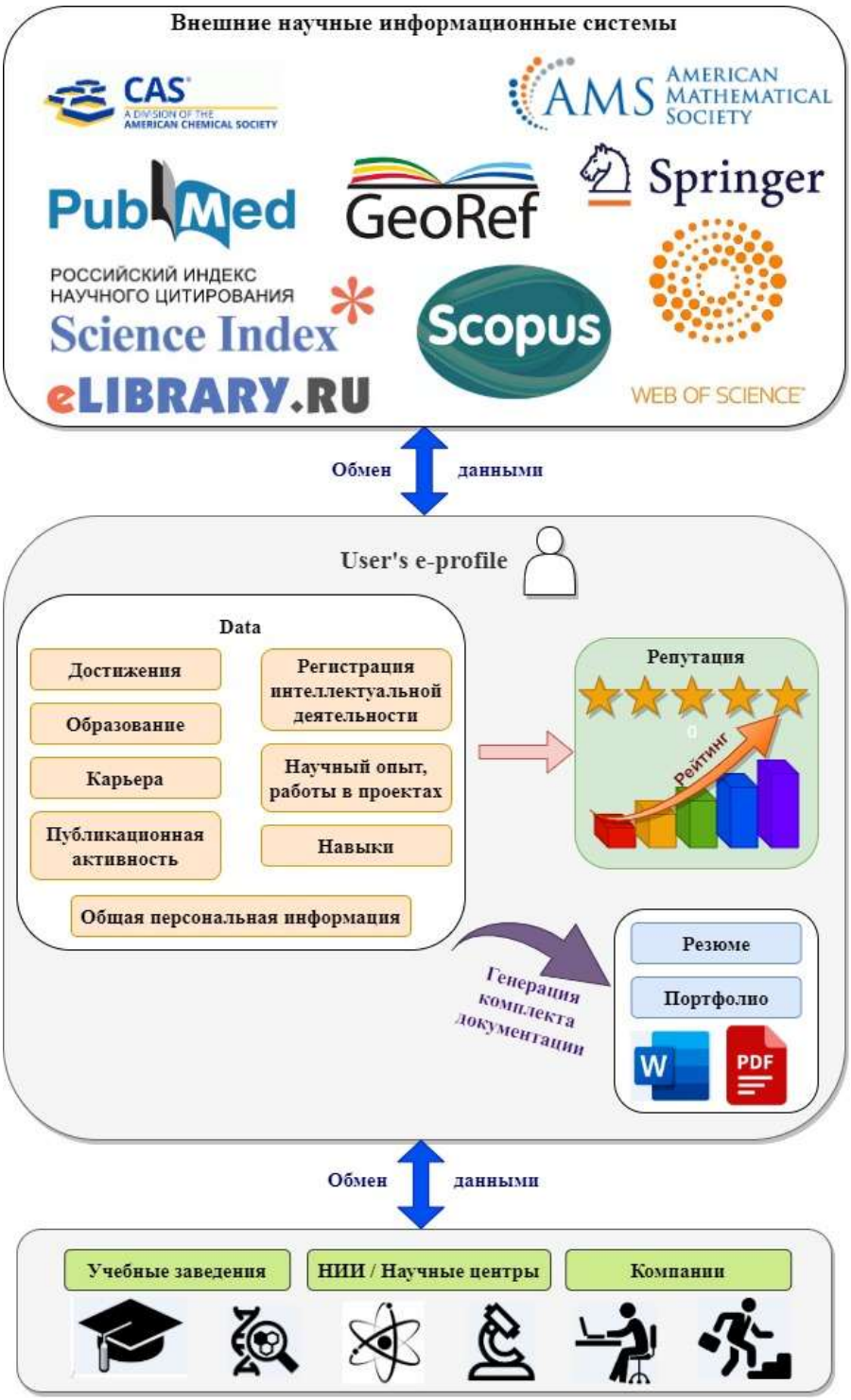


Рис. 1. Схема функционирования и взаимодействия электронного портфолио субъекта с внешними ресурсами

В 2020 году был опубликован международный стандарт ИСО/МЭК 20013:2020 «Информационные технологии для обучения, образования и подготовки – Справочная база информации электронного портфолио», который определяет понятие «электронное портфолио» как совокупность электронных объектов, объединенных в единую информационную систему

и используемых для обеспечения образовательного процесса и повышения квалификации с помощью использования автоматических и неавтоматических средств с целью хранения персональных электронных артефактов (результатов интеллектуальной деятельности); личных журналов для глубокого изучения; сравнения результатов обучения, опыта и достижений; презентации выбранных видов контента для потенциальных и существующих работодателей [2].

Электронное портфолио физического лица представляет собой цифровой двойник участника киберфизической среды, хранящий всю информацию о достижениях и интеллектуальных трудах участника за время его обучения и профессиональной деятельности, автоматически подсчитывает рейтинг участника и формирует комплекты важных документов, такие как портфолио, резюме, Форма 16, методом «одного клика» [3]. Система также имеет функцию интеграции с другими информационными системами для обмена информацией (рис. 1, см. выше). Сгенерированные документы впоследствии можно автоматически отправить в электронном виде в информационную систему сторонних организаций учебных заведений, организаторов мероприятий и конкурсов, отраслевых компаний, научных центров, с которыми интегрируется система электронного портфолио.

Информационная структура электронного портфолио физического лица строится на основе формализмов теории множеств и комплексных моделей. Подобная структура в общем виде отражает различные аспекты системы электронного портфолио, а также связи между этими аспектами и обеспечивающими их формализмами. По канторовской теории множеств структуру комплексной информационной модели электронного портфолио физического лица можно представить в следующем виде:

$$EP_f = \{A, I, PD, C, Ed\}, \quad (1)$$

где A – множество достижений (Achievements);

I – множество результатов интеллектуальной деятельности (Intelligent Works);

PD – множество персональных данных о субъекте (Personal Data);

C – множество данных о профессиональной деятельности (Career);

Ed – множество данных об образовании и повышении квалификации (Education).

Используя электронное портфолио, пользователь в роли физического лица имеет возможность производить следующие действия:

– заполнять данные о себе, своих достижениях и результатах интеллектуальной деятельности (РИД);

– воспроизводить поиск необходимой информации;

– контролировать процесс за своей успеваемостью и рейтингом;

– делать выборку своих достижений и результатов научно-профессиональной деятельности по определенным компетенциям;

– автоматически формировать необходимую документацию для предоставления информации о себе в сторонние организации;

– формировать список достижений за определенный период времени;

– составлять отзывы и рецензии для других физических лиц;

– выполнять поиск подходящих вакантных мест для проектной деятельности или устройства на работу;

– выполнять авторизацию в других информационных системах посредством профиля электронного портфолио.

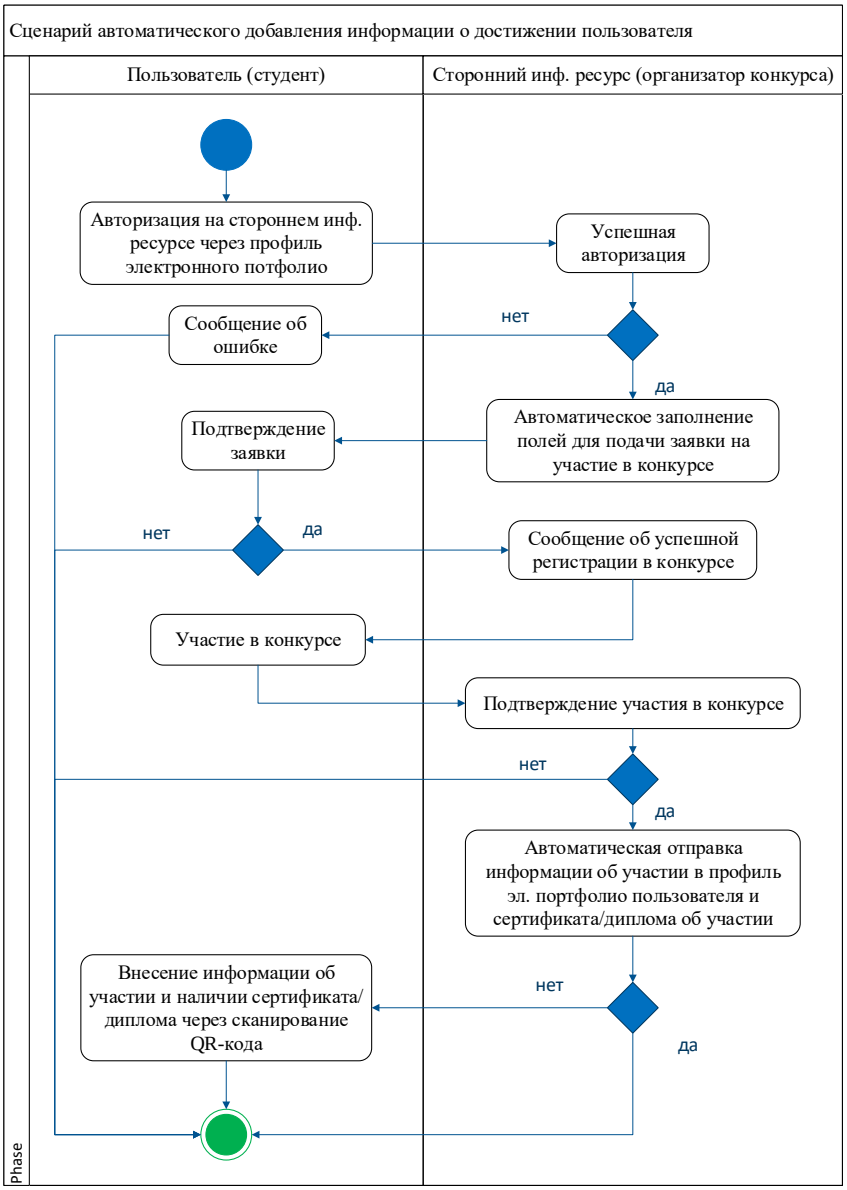


Рис. 2. Диаграмма деятельности автоматического добавления информации в профиль электронного портфолио субъекта посредством интеграции со сторонним информационным ресурсом

Пример алгоритма автоматического добавления информации в профиль электронного портфолио субъекта посредством интеграции со сторонним информационным ресурсом приведен на рис. 2 (см. выше). Диаграмма деятельности отражает процесс автоматического добавления информации в профиль электронного портфолио субъекта (в данном случае студента) посредством интеграции со сторонним информационным ресурсом (в данном случае информационный ресурс организатора конкурса, в котором участвует студент).

Взаимодействие двух киберсред происходит в двухстороннем режиме. Если студент получает автоматически загруженные сертификаты и информацию об участии, то сам ресурс по регистрации студентов на участие в конкурсе получает необходимую информацию об участнике непосредственно из электронного портфолио на момент нажатия пользователем кнопки «Хочу участвовать в конкурсе» – ресурс организации конкурса обращается к профилю электронного портфолио заявителя и автоматически заполняет поля необходимой информацией.

Список используемых источников

1. Paulo Carreira, Vasco Amaral, Hans Vangheluwe. Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems // The Editor(s) (if applicable) and The Author(s) 2020, Springer, Cham. eBook ISBN 978-3-030-43946-0. DOI https://doi.org/10.1007/978-3-030-43946-0.

2. Акимов С. В., Давлетшина Э. Р. Модели управления кадровыми ресурсами в киберсреде виртуальных предприятий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2021. Т. 2.; с. 23–27. URL: https://elibrary.ru/item.asp?id=46545618.

3. ISO/IEC 20013:2020 Information technology for learning, education and training – Reference framework of e-Portfolio information.

УДК 004.5
ГРНТИ 50.41.29

ФОРМИРОВАНИЕ ГРАФИЧЕСКОГО ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА СЕРВИСОВ КИБЕРФИЗИЧЕСКОЙ СРЕДЫ С ПОМОЩЬЮ МИКРОФРОНТЕНДОВ

Г. В. Верхова, Д. В. Овсянников

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится описание формирования графического пользовательского интерфейса сервисов киберфизической среды с помощью микрофронтендов. Описаны конкретные примеры реализации кастомных html элементов, а также приведен один из возможных примеров взаимодействия между изолированными частями пользовательского интерфейса киберфизических сред.

микрофронтенды, пользовательские интерфейсы, киберфизические среды, распределенные системы.

Микрофронтенды – это архитектурный подход, при котором независимые приложения собираются в одно большое приложение. Это позволяет комбинировать разные виджеты или страницы, написанные разными командами с использованием разных фреймворков, в одном приложении [1]. Для наглядности данного подхода представлен рис. 1.

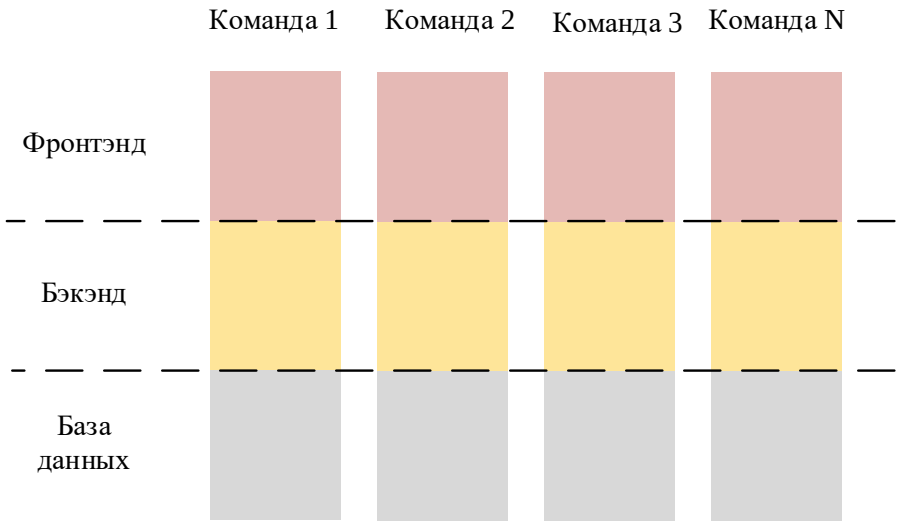


Рис. 1. Схематичное представление подхода «Микрофронтэнды»

Ниже приведен условный пример сформированного графического пользовательского интерфейса сервисов киберфизической среды с помощью микрофронтендов. Разными цветами отмечены зоны ответственности разных сервисов. При этом, каждая команда разработчиков может выбирать свой стек технологий, и разрабатывать свой сервис независимо [2–3].

Рис. 2. Условный пример графического пользовательского интерфейса различных сервисов с помощью микрофронтендов

Для разграничения зоны ответственности различных команд разработчиков внутри DOM’а предлагается использовать кастомные html элементы. Ниже приведена упрощенная часть кода (рис. 3), демонстрирующая создание такого элемента.

```
class BlueBuy extends HTMLElement {
  connectedCallback() {
    this.innerHTML = `<button type="button">Купить</button>`;
  }
  disconnectedCallback() { ... }
}
window.customElements.define('blue-buy', BlueBuy);
```

Рис. 3. Упрощенная часть кода, демонстрирующая создание кастомного html элемента

Приведенный код выше, в верстке браузера будет отображаться следующим образом (рис. 4).

Если появится необходимость передачи информации между различными элемен-

```
<html>
▶ <head>…</head>
▼ <body>
  ▼ <blue-buy>
      <button type="button">Купить</button> == $0
    </blue-buy>
  </body>
</html>
```

Рис. 4. Отображение кастомного html элемента в браузере

тами, то можно воспользоваться общим стейтом, добавить стандартные или кастомные события, а также добавить слушателей этих событий, на принимаемом информацию элементе. Пример такого кода приведен на рис. 5.

```
const state = {
    count: 0,
 };
class BlueBuy extends HTMLElement {
…
addToCart() {
  state.count += 1;
    this.dispatchEvent(new CustomEvent('blue:basket:changed', {
        bubbles: true,
    }));
  }
…
}
class BlueBasket extends HTMLElement {
    connectedCallback() {
        this.refresh = this.refresh.bind(this);
        this.render();
        window.addEventListener('blue:basket:changed', this.refresh);
    }
…
    refresh() {
      this.render();
    }
…
}
```

Рис. 5. Пример взаимодействия кастомных html элементов

В киберсреде микрофронтенды позволят разделить ответственность за кодовую базу, создавая небольшие команды для работы над приложением. Таким образом, до объединения всех частей приложения можно выполнять независимые развертывания и тесты.

Более того, в киберсреде микрофронтенды позволят смешивать и сочетать разные технологии – например, созданные в новейших Vue или React, а другие – в Angular. Такое решение, скорее всего, будет очень полезно в крупных проектах, так как не будет необходимости переписывать весь код проект под один стек технологий, либо будет возможность обновлять кодовую базу постепенно.

Список используемых источников

1. Микросервисный подход в веб-разработке: micro frontends. URL: https://bookflow.ru/ (дата обращения: 15.03.2022).

2. Arif Balaev. Микрофронтенды. URL: https://dev.to/ (дата обращения: 16.03.2022).

3. Jenny V. Микрофронтенды – а почему бы и нет? URL: https://medium.com/ (дата обращения: 17.03.2022).

УДК 004.896
ГРНТИ 28.23.27

ПРИМЕНЕНИЕ SLAM В МНОГОАСПЕКТНЫХ ГЕОИНФОРМАЦИОННЫХ МОДЕЛЯХ

Г. В. Верхова, П. А. Прокофьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены результаты исследований методов одновременной локализации и построения карт для автономных транспортных средств. Рассмотрены способы применения методов синхронной локализации и построения карт для сбора геоинформации. Рассмотрены пути интеграции гетерогенной информации в геоинформационных сервисах с помощью многоаспектных моделей. Предложен концепт интеграции методов одновременной локализации и построения карт в геоинформационные сервисы с помощью многоаспектных моделей. Рассмотрены пути построения библиотек программно-алгоритмического обеспечения методов локализации, построения и обновления геоинформационных многоаспектных моделей.

SLAM, ГИС, многоаспектные модели, построение карт, автономные транспортные средства.

Многоаспектные геоинформационные модели позволяют обеспечить целостное представление гетерогенной информации об объекте, распределенном в пространстве. За счёт этого акценты смещаются с отдельных слоев геоинформационных систем на аспекты, отражающие различные стороны объекта [1]. Данные модели применимы к географическим регионам [2].

Современные методы сбора информации об окружающей среде позволяют реализовать обновление геоинформационных данных в реальном времени. Кроме того, они могут быть совместимы с многоаспектными моделями. Рассмотрим концепт интеграции методов одновременной локализации и построения карт (SLAM) в геоинформационные сервисы с помощью многоаспектных моделей.

Методы SLAM (англ. Simultaneous Localization and Mapping) обеспечивают сбор данных и построение на их основе карты окружающей среды. Алгоритмы SLAM реализуются на базе подвижных роботов, имеющих на борту лазерные дальномеры (лидары), камеры, одометры и другие устрой-

ства, позволяющие сканировать окружающую среду и отслеживать путь робота. Процесс интеграции данных в геоинформационную систему (ГИС) представлен на рис. 1.

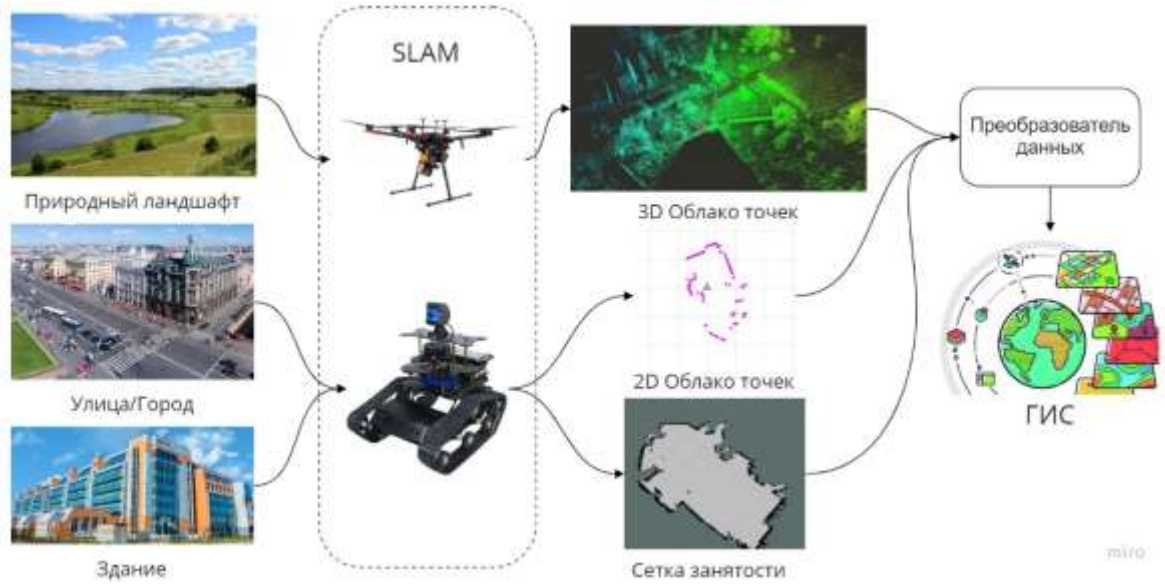


Рис. 1. Процесс интеграции SLAM в ГИС

Робот получает информацию об окружающей среде и в результате работы алгоритмов SLAM появляется карта в виде облака точек или сетки занятости (2D-матрицы, в которой каждой ячейке присваивается вероятность её занятости) [3]. Далее необходимо использовать преобразователь данных, который бы позволял трансформировать сырые данные SLAM в формат, совместимый с ГИС. Преобразованные данные отправляются в ГИС, происходит обновление информации.

Следует отметить, что преимуществами использования SLAM для обновления геоинформационных систем являются: автоматизированный сбор геоинформации, обновление данных в реальном времени, возможность изучить труднодоступную местность, автономность инструментов.

Среди недостатков можно выделить соотношение временных затрат и зоны покрытия. SLAM следует использовать для сканирования небольших объектов, таких как здания или улицы.

Поскольку при работе с ГИС мы используем многоаспектные модели, предлагается модифицировать структуру, указанную в [2]. Обновленная структура многоаспектной геоинформационной модели представлена на рис. 2.

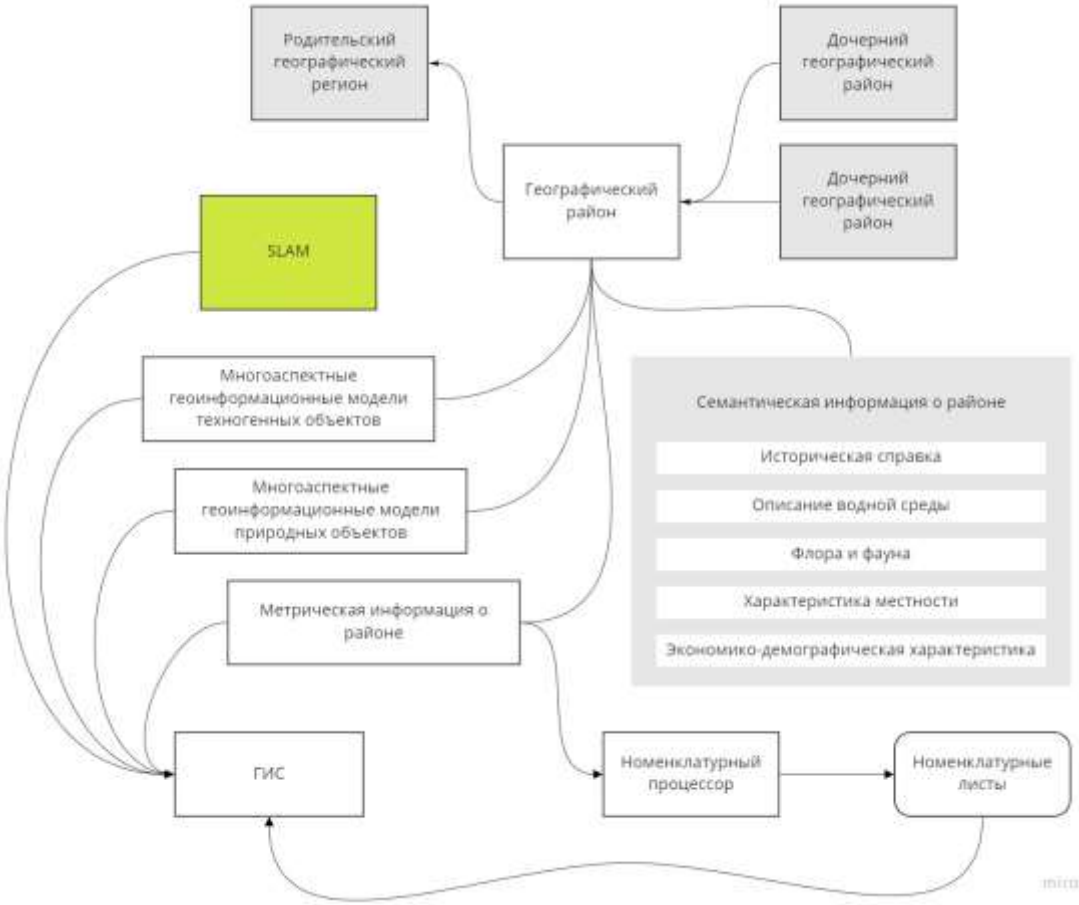


Рис. 2. Структура многоаспектной геоинформационной модели географического района

Метрическая информация, главным образом, задает границы моделируемого района. Номенклатурные листы для данного района динамически загружаются из геоинформационной системы либо добавляются как ссылки на графические файлы. Многоаспектные геоинформационные модели природных и антропогенных объектов находятся в отдельной среде моделирования и аналогично интегрируются в модель географического района с помощью ссылок. Семантическая информация задается с помощью гипермедийных документов и включает в себя: общую характеристику района, историческую справку, характеристику местности, информацию о флоре и фауне, экономико-демографическую характеристику. При необходимости данный список может быть дополнен. SLAM в данном случае выступает как инструмент для обновления геоинформационной системы и работает в интеграции с многоаспектной моделью.

Список используемых источников

1. Акимов С. В., Добросельский М. А., Курносов В. И. Многоаспектное моделирование системных объектов на этапах жизеннного цикла // I-methods. 2018. Т. 10. № 3. С. 5–13

2. Верхова Г. В., Акимов С. В., Присяжнюк С. П. Метод многоаспектного геоинформационного моделирования географического района // Информация и Космос. 2021. N 4 (1). С. 123–129.

3. Верхова Г. В., Прокофьев П. А. Методы синхронной локализации и построения карт для автономных транспортных средств // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 127–129.

УДК 621.39
ГРНТИ 49.01.75

АНАЛИЗ НОРМАТИВНОЙ БАЗЫ КРИТИЧНОСТИ ОБЪЕКТОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В. А. Волостных[1, 2], О. А. Остроумов[1], А. Д. Синюк[1]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский государственный университет им. проф. М. А. Бонч-Бруевича

Вопросам обеспечения безопасности и устойчивости функционирования объектов критической информационной инфраструктуры уделяется много внимания. Постоянно происходит совершенствование нормативной базы, регулирующей вопросы в этой области. В работе проведен анализ современного состояния нормативной базы России в области обеспечения безопасности критичности объектов различных сфер жизнедеятельности общества.

критическая информационная инфраструктура, критически важный объект, функциональная устойчивость, безопасность, сложные системы.

Развитие современных систем и средств привело к увеличению их возможностей, функций, которые они могут выполнять. Все это способствовало использованию их для функционирования других систем и объектов, при этом порой, без их устойчивого функционирования отдельные предприятия и отрасли промышленности не могут эффективно функционировать.

Зависимость одних систем, объектов, отраслей от других способствовало необходимости государством проработки вопросов значимости одних для других, а также вопросов критической значимости. Все это способствовало появлению в различных странах мира нормативной базы, регулирующей вопросы обеспечения устойчивого и безопасного функционирования критически значимых объектов.

События осуществления компьютерной атаки на систему управления атомной станции в Иране в 2010 года показали всему миру, что воздействие

программы на объект может привести к его физическому разрушению и тяжелым последствиям. Они, а также постоянно возрастающее использование сетей связи, информационных сетей и автоматизация многих сфер жизни, способствовали выделению в отдельный класс объектов – объекты критической информационной инфраструктуры. На уровне государства в различных странах мира [1] началась проработка нормативного обеспечения вопросов безопасности и устойчивости критически важных объектов.

С этого времени в России также начинается работа по разработке новых нормативных документов [2]. В ноября 2011 году представлены Поручения Президента РФ № ПР-3400, определившие основы государственной политики в области обеспечения безопасности населения РФ и защищенности КВО и ПОО от угроз природного и техногенного характера и террористических актов на период до 2020 года. Данный документ носил концептуальный. Дальнейшая работа в данном направлении привела к разработке Советом Безопасности утвержденного Президентом Российской Федерации 3 февраля 2012 г. № 803 документа, определившего основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ. Документ разрабатывался в рамках реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 года и учитывал три этапа развития: первый с 2012 по 2013, второй с 2014 по 2016 и третий с 2017 по 2020, включающий целый комплекс мероприятий по поддержанию организационной, экономической, научно-технической и технологической готовности РФ к предотвращению угроз безопасности ее критической информационной инфраструктуры.

Здесь приводится понятие критически важного объекта (КВО) и критическая информационная инфраструктура (КИИ) [3, 4].

В процессе выполнения первых двух периодов и дальнейшей работы в направлении обеспечения безопасности и устойчивого функционирования критически важных объектов были доработаны и разработаны ряд документов.

Федеральный законе от 21.12.1994 N 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», в котором уточнялось понятие КВО, а также определялась необходимость обеспечения устойчивого функционирования таких объектов.

Основным документом, регулирующим отношения в области обеспечения безопасности КИИ стал Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон вводит понятийный аппарат КИИ, определяет полномочия и обязанности органов власти, субъектов КИИ, требования по категорированию объектов КИИ, необходимость создания и совершенствования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

С момента вступления последнего закона возникло много вопросов, касаемо порядка выполнения мероприятий, предусмотренных законом.

В соответствии с законом подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА являются подразделения ФСБ, а Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры РФ – ФСТЭК.

Перечень нормативных документов оценка соблюдения, которых является предметом государственного контроля (ГК) в области обеспечения безопасности КИИ представлен в приказе ФСТЭК РФ от 2019 года №135.

Основными документами определяющими требования к КИИ являются ФЗ № 187 от 2017 года, Постановление Правительства РФ от 8 февраля 2018 г. N 127 «Правила категорирования объектов критической информационной инфраструктуры Российской Федерации», Приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказом ФСТЭК России от 11.12.2017 № 229 введена форма акта проверки, составляемого по итогам проведения ГК в области обеспечения безопасности значимых объектов КИИ РФ. Правила осуществления ГК в области обеспечения безопасности значимых объектов КИИ РФ введены постановлением Правительства РФ от 17.02.2018 №162. Постановлением Правительством РФ от 8.07.2019 № 743 установлены правила подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ.

Приказом ФСТЭК России от 06.12.2017 № 227 определяется порядок ведения реестра значимых объектов КИИ РФ. Сведения о результатах присвоения объекту КИИ одной из категорий значимости и форма их предоставления представлены в приказе ФТЭСК России от 22.12.2017 года № 236.

Кроме этого, разработаны и разрабатываются методические документы по определению значимости объектов КИИ в политической, экологической, экономической, социальной областях, а также области обеспечения обороны страны, безопасности государства и правопорядка.

Вопросы создания и функционирования ГосСОПКА регулируются указом Президента №31с о создании ГосСОПКА на информационные ресурсы РФ и ФЗ №187. Указом Президента РФ от 22.12.2017 года № 620 определяются полномочия органов ФСБ по обеспечению функционирования ГосСОПКА.

Кроме этого, директором ФСБ разработаны документов, включающие приказы директора ФСБ от 24.07.2018 года № 366 «О Национальном координационном центре по компьютерным инцидентам» (НКЦКИ), от 24.07.2018 года № 367 «Об утверждении перечня информации, представляемой в ГосСОПКА на информационные ресурсы РФ и порядка предоставления информации в ГосСОПКА на информационные ресурсы РФ», от 24.07.2018 года

№ 368 «Об утверждении порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и порядка получения субъектами КИИ РФ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения», от 19.07.2019 года № 282 «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ РФ», от 6.05.2019 года № 196. «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ».

Совершенствование нормативной базы является неотъемлемой частью системы обеспечения безопасного и устойчивого функционирования критически важных объектов. В России, как и в других странах, вопросу значимости объектов инфраструктуры уделяется много внимания. Основные нормативные документы разработаны, однако остается не до конца проработанным вопрос методологического и методического обеспечения. Необходима разработка методических документов по определению значимости объектов министерств и ведомств государства, учитывающие их особенности, а также методик определения социальной, экологической, политической значимости объектов.

Список используемых источников

1. Лепешкин О. М., Синюк А. Д., Митрофанов М. В., Остроумов О. А. Подходы к определению критичности объектов инфраструктуры в различных странах мира // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей III Всероссийской научной-технической конференции. Анапа, 2021. С. 391–400.

2. Лепешкин О. М., Остроумов О. А., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. № 8. С. 109–114.

3. Остроумов О. А., Лепешкин О. М., Ковалев Д. С., Остроумова Е. В. К вопросу о понятии критической информационной инфраструктуры системы управления // I-metods, 2021. № 3. С. 10–15.

4. Лепешкин О. М., Черных И. С., Остроумов М. А., Остроумов О. А. К вопросу о понятии критически важного объекта // Проблемы технического обеспечения войск в современных условиях. Труды VI межвузовской научно-практической конференции. Санкт-Петербург, 2021. С. 17–20.

УДК 004.056.55
ГРНТИ 81.93.29

ПРОГРАММНОЕ СРЕДСТВО АУТЕНТИФИЦИРОВАННОГО ШИФРОВАНИЯ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

И. В. Гаврилов, Д. А. Мартынов

Академия Федеральной службы охраны Российской Федерации

В статье представлены результаты разработки программного средства аутентифицированного шифрования для систем электронного документооборота. Рассмотрены основные шаги алгоритма данного программного средства для реализации процесса аутентифицированного шифрования при передаче графических файлов с указанием структурных элементов формата jpg.

шифрование, аутентификация, ассоциативные данные, система электронного документооборота.

Системы электронного документооборота [1], в настоящее время работающие по открытым каналам связи, должны иметь возможность безопасной передачи информации с возможностью аутентификации сторон и проверки целостности. В качестве решения данной задачи в [2] предложено использовать режим MGM Multilinear Galois Mode (MGM) [3–5], который реализует аутентифицированное шифрование на основе ассоциированных данных (AEAD – Authenticated Encryption with Associated Data).

Авторами статьи на основе описанного в [2] алгоритма применения аутентифицированного шифрования для графических файлов в системах электронного документооборота разработано программное средство аутентифицированного шифрования графических файлов

Программное средство аутентифицированного шифрования графических файлов предназначено для обеспечения конфиденциальности и целостности графических файлов при помощи применения режима работы блочных шифров MGM, реализующего аутентифицированное шифрование. Данное программное средство выполняет обработку графических файлов в формате jpg, при этом загружаемое изображение должно иметь базовую кодировку (т.е. при кодировании использовалось дискретно-косинусное преобразование и код Хаффмана). Данное ограничение обусловлено особенностями процесса формирования графического файла указанного формата. В ходе работы программного средства обеспечение конфиденциальности графического файла реализовано путем зашифрования его тела (т.е. байтовой

последовательности, содержащей информацию непосредственно о картинке), а целостность обеспечивается путем выработки значения имитовставки для заголовка изображения (т. е. описательной структуры изображения, в которой указан его размер, разрешение, цветовая модель, число бит на компонент, их соотношение и т. д.). Структура файла формата jpg представлена на рис. 1.

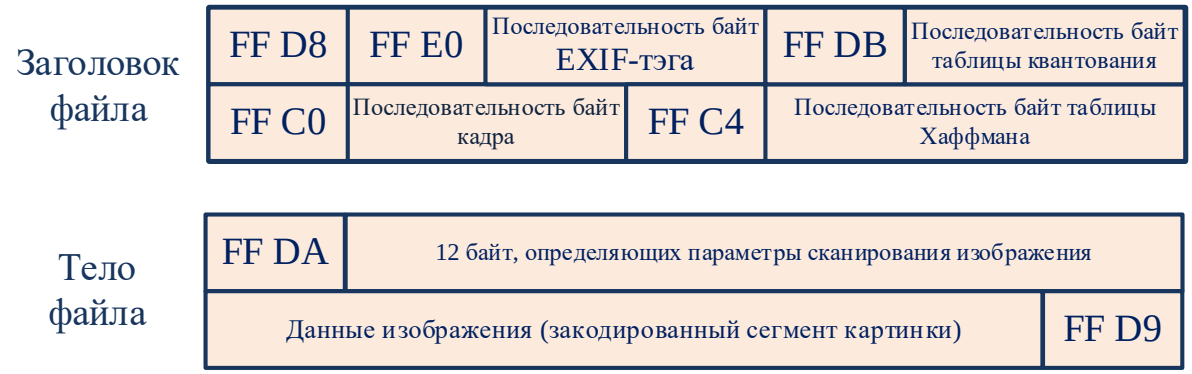


Рис. 1. Общая структура графического файла в формате jpg

Программное средство аутентифицированного шифрования графических файлов работает по *следующему алгоритму*:

1. *Загрузка изображения, определение его размера.*

2. *Определение позиции маркера начала сканирования* (0xFF 0xDA).

Поиск данного маркера в загруженной байтовой последовательности осуществляется с конца последовательности, т. к. байты данного маркера могут быть обнаружены в заголовке изображения в составе метаданных (т. е. байтов EXIF-тега.

3. *Определение заголовка и тела файла из ранее загруженного изображения.*

Определение границы между заголовком и телом файла в загруженной байтовой последовательности выполняется на основе ранее выделенной позиции маркера начала сканирования. Таким образом, первая часть байтовой последовательности файла, расположенная перед данным маркером, относится к заголовку файла, а вторая часть относится к его телу. Обозначенные ранее части загруженной байтовой последовательности файла будут впоследствии представлять собой такие параметры режима MGM, как открытый текст (тело файла), и ассоциированные данные (заголовок файла).

4. *Генерирование ключевых данных и вектора инициализации, определение длины имитовставки.*

В соответствии с рекомендацией по стандартизации, определяющей режим MGM, длина ключевых данных должна составлять 256 бит, а длина вектора инициализации должна быть равна n-1, где n – длина блока открытого текста. Также, согласно вышеуказанной рекомендации, для работы

данного режима может использоваться произвольный блочный шифр с длиной блока n. В программном средстве «JPG_encryptor» используется симметричный алгоритм блочного шифрования с размером блока 128 бит, определяемый в соответствии с ГОСТ 34.12–2018. Используемые для работы с графическом файлом ключевые данные и вектор инициализации генерируются в ходе обработки байтовой последовательности, после чего ключ помещается в отдельный файл, а вектор инициализации встраивается в файл в виде метаданных.

5. *Зашифрование тела файла и выработка имитовставки для его заголовка.*

Вычисленная на основе байтовой последовательности заголовка файла имитовставка помещается в конец файла.

6. *Помещение значения размера заголовка и вектора инициализации в конец файла.*

Для обеспечения возможности корректного определения открытой и зашифрованной частей сформированного графического файла, полученного в результате использования программного средства, необходимо предусмотреть встраивание информации о границах данных частей в формируемый файл. Необходимость в определении данной границы обусловлена тем, что при зашифровании тела графического файла в нем могут образоваться байты, совпадающие со значением байт маркера начала сканирования (0xFF 0xDA), что вызовет неверное определение байтовых последовательностей, используемых для расшифрования и расчета значения имитовставки. Следовательно, информацию о длине байтовой последовательности, содержащей в себе заголовок файла и хранящейся в открытом виде, необходимо встроить в формируемый файл (для данной части файла обеспечивается только целостность за счет выработки имитовставки). В разработанном программном средстве информация о длине указанной байтовой последовательности, а также сгенерированный ранее вектор инициализации помещается в конец файла (после значения имитовставки) в составе EXIF-тэга.

7. *Формирование графического файла в формате jpg и его помещение в заданный каталог.*

Алгоритм работы программного средства при зашифровании графического файла представлен на рис. 2.

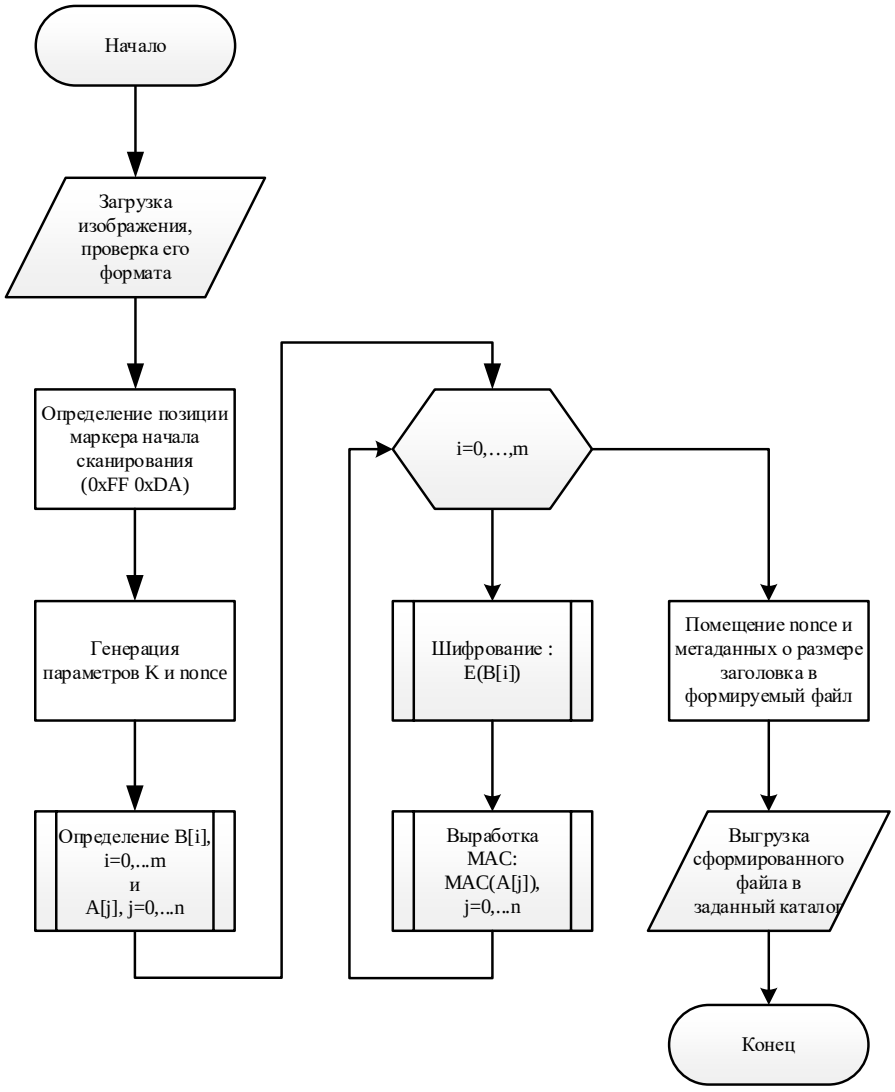


Рис. 2. Алгоритм работы программного средства при зашифровании

При расшифровании графического файла указанная последовательность действий выполняется в обратном порядке, т. е. *алгоритм работы программного средства в ходе расшифрования* имеет следующий вид:

1. Загрузка зашифрованного изображения.

2. Определение параметра nonce и метаданных о размере заголовка, загрузка параметра K из отдельного файла.

3. Определение границ заголовка и тела файла на основе метаданных, полученных на предыдущем шаге алгоритма.

4. Выполнение процедур расшифрования и вычисления имитовставки.

5. Проверка значения вычисленной имитовставки.

6. Формирование расшифрованного файла в случае корректности вычисленного значения.

7. Выгрузка сформированного файла в заданный каталог.

Подводя итог, необходимо отметить, что в системах электронного документооборота для обеспечения безопасной передачи информации авторами статьи предложено использовать режим MGM аутентифицированного шифрования с ассоциативными данными. Для реализации данного режима разработано программное средство, с помощью которого на примере графического файла jpg проводится процедура шифрования и расшифрования.

Список используемых источников

1. Мокрый В. Ю. Системы электронного документооборота: учебное пособие. СПб.: Инфо-да, 2018. 48 с.

2. Мартынов Д. А., Гаврилов И. В. Алгоритм применения аутентифицированного шифрования для графических файлов в системах электронного документооборота // Инновационные научные исследования. 2021. № 8-1(10). С. 41–47.

3. Ноздрунов В. Режим работы параллельного и двойного блочного шифра (PD-mode) для аутентифицированного шифрования. CTCrypt, 2017.

4. Ноздрунов В., Шишкин В. Multilinear Galois Mode (MGM). Проект CFRG, 2018.

5. Фомин Д., Курочкин А. MGM вне рамок дня рождения. CTCrypt, 2019.

УДК 004.415.53
ГРНТИ 50.41.25

ОСОБЕННОСТИ ПРОЦЕССА ИНТЕЛЛЕКТУАЛИЗАЦИИ В ТЕСТИРОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Е. Ю. Галимова, А. И. Ходанович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье обсуждаются основные тенденции процесса интеллектуализации тестирования программного обеспечения. Обозначены важные для специалиста по тестированию различия между программными системами, разработанными на базе объектно-ориентированного подхода, и системами искусственного интеллекта.

тестирование программного обеспечения, искусственный интеллект, интеллектуализация, регрессионное тестирование, машинное обучение.

Актуальность вопросов интеллектуализации в тестировании программного обеспечения связана с тем, что потребности в объемах хранения и скоростях использования данных постоянно растут. Большие данные что называют «новым топливом» или «цифровой нефтью». На сегодняшний день данные характеризуются большими объемами, разнообразием форматов и высокой скоростью прироста [1]. Классические алгоритмы машинного

обучения используются сегодня при работе с относительно небольшим количеством данных. Для наиболее значительных объемов данных применяются алгоритмы глубокого обучения: сверточные сети, рекурентные сети, трансформеры, графовые сети. Концептуальная схема работы искусственного интеллекта приведена на рисунке.

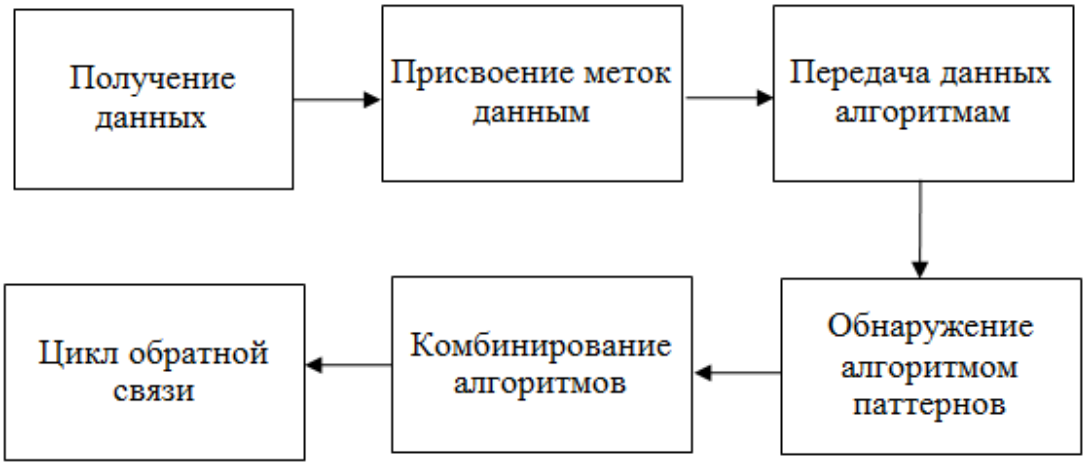


Рисунок. Основные шаги работы искусственного интеллекта

Можно выделить четыре основные функции искусственного интеллекта: восприятие, обучение, абстрагирование, логический вывод. Наиболее хорошо реализованы в наши дни первые две. Активные исследовательские работы ведутся в направлении создания систем, обладающих функциями абстрагирования и логического вывода.

Искусственный интеллект имеет часть признаков программного обеспечения – это двоичный код, исполняемый микропроцессором (табл. 1). Важным отличием является отсутствие GUI, то есть пользовательский интерфейс нельзя протестировать классическими методами. Ещё отличие – искусственный интеллект не программируется строчками кода, а проходит обучение, он должен уметь работать с данными и с метками на данных. В программировании основным выходным продуктом является программный код, в случае искусственного интеллекта – это данные. Для тестирования программного обеспечения используются кодоцентричные методы. Для тестирования искусственного интеллекта требуются датацентричные методы.

ТАБЛИЦА 1. Сравнение объектно-ориентированного программного обеспечения и искусственного интеллекта

Сравнительные характеристики	**Объектно-ориентированное программное обеспечение**	**Искусственный интеллект**
Способ представления данных	двоичный код	двоичный код

Сравнительные характеристики	Объектно-ориентированное программное обеспечение	Искусственный интеллект
Графический интерфейс пользователя (GUI)	есть	нет
Выходной продукт	программный код	данные
Изменяется в процессе выполнения	нет	да
Ключевой специалист	программист	эксперт по аналитическим данным (data scientist)
Методы тестирования	кодоцентричные	датацентричные

С добавлением нового функционала в проект, сложность последнего растет нелинейно. Требуется больше ресурсов на проведение регрессионного тестирования. Кроме существенной (essential) сложности, в проекте часто присутствует случайная (accidental) сложность. Существенная сложность является свойством решаемой задачи. Случайная сложность привносится в проект во время его разработки. Она также увеличивает затраты на тестирование. Выбор эффективных инструментов разработки способствует низкой случайной сложности [2]. Для получения аналогичного эффекта в поддерживаемом программном коде, применяется рефакторинг.

Задача минимизации затрат на регрессионное тестирование является оптимизационной. Один из вариантов решения – оптимизация по количеству выполняемых тестов. Производится декомпозиция программного обеспечения по функциональным областям. Для каждой области формируется необходимый набор тестов. Для решения данной задачи можно применять машинное обучение, в частности, один из подходов – кластеризацию.

Еще одна задача в тестировании, которую способен выполнять искусственный интеллект – разработка оптимального набора тестовых сценариев. Например, перебрать все возможные комбинации сценариев, а затем выбрать набор сценариев, необходимых для выполнения, по критерию частоты встречаемости. Компания Infosys уже выпустила программный продукт NIA, который на основе анализа выполнения предыдущих тесов предлагает дальнейшие направления тестирования.

Тестирование пользовательского интерфейса с применением искусственного интеллекта приобрело большую популярность [3]. Создан ряд готовых библиотек, которыми могут пользоваться тестировщики и разработчики. На их основе создаются приложения для тестирования пользовательского интерфейса, в частности, Applitools. Искусственный интеллект может обнаружить визуальные ошибки в интерфейсе, охватывая при этом значительно большие тестовые области. Например, можно научить

систему записывать в тестовый сценарий фактический элемент пользовательского интерфейса, такой как поле формы, а затем обучить искусственный интеллект распознавать изменения в интерфейсе данного поля.

Искусственный интеллект способен спрогнозировать результаты предстоящего цикла тестирования, выявляя закономерности и будущие тенденции. Одним из дальнейших направлений интеллектуализации процесса тестирования может стать применение искусственного интеллекта для выявления неоднозначностей в тестовых сценариях [4]. Исходя из вышеизложенных тенденций, можно прогнозировать, что в недалеком будущем искусственный интеллект возьмет на себя все рутинные задачи в тестировании и позволит тестировщикам заниматься в основном исследовательским тестированием, искать «творческие» подходы к работе.

Список используемых источников

1. Вьюгин В. В. Математические основы теории машинного обучения и прогнозирования. Москва: МЦНМО, 2013. 387 с.

2. Галимова Е. Ю. Тестирование нейронной сети системы автоматизированного вождения для зерноуборочных комбайнов // Развитие научного наследия великого ученого на современном этапе: Сборник международной научно-практической конференции, посвященной 95-летию члена-корреспондента РАСХН, Заслуженного деятеля науки РСФСР и РД, профессора М. М. Джамбулатова (III Том), Махачкала, 17 марта 2021 г. Махачкала: Изд-во Дагестанского ГАУ, 2021. С. 181–184.

3. Myers B. A. User Interface Software Tools // ACM. Transactions on Computer-Human Interaction, Vol. 2, No.1, March 1995. pp. 64–103.

4. Галимова Е. Ю. Метод исследования неоднозначности в тестовых сценариях // XXI Международная конференция по науке и технологиям Россия-Корея-СНГ. Москва, 26–28 августа 2021: труды конференции. Коллектив авторов. Новосибирск: Изд-во НГТУ, 2021. С. 17–21.

Статья представлена научным руководителем,
доктором педагогических наук, профессором А. И. Ходановичем.

УДК 004.77
ГРНТИ 49.33.29

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ NAT ДЛЯ РЕГИСТРАЦИИ УСТРОЙСТВ В WAN СЕТЯХ

И. В. Гвоздков, И. В. Кильдяев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современное время, ежесекундно появляется огромное количество пользователей в глобальной сети, которым требуются IP-адреса, но на протоколе IPv4 имеется огромная нехватка адресов и что бы решить данную проблему и облегчить переход к IPv6 был создан NAT. В статье дается информация о технологии NAT, возможных концепциях, проблемах, которые возникают при использовании, а также самые популярные решения проблем связанных с регистрацией устройств в глобальных сетях.

NAT, Hole punching, глобальные сети, пиринговые сети, сквозная адресация, регистрация устройств.

В век цифровых технологий сложно представить наш мир без глобальной сети Интернет, поэтому огромное количество людей постоянное ей пользуются. Но со времён создания протокола IPv4 прошло достаточно большое количество времени и его ресурс, который раньше считался просто огромным, в количестве немного меньше 4.3 миллиардов адресов стал заканчиваться. Сейчас уже существует протокол IPv6, которого хватит нам на долгое время благодаря своему размеру – 340 ундециллионов адресов. Но переход с протокола IPv4 на IPv6 затруднён из-за трудозатрат, стоимости и отсутствия обратной совместимости и что бы отсрочить этот переход была разработана технология NAT [1].

NAT (Network Address Translation) – механизм преобразования сетевых адресов использующийся в сетях TCP/IP, который изменяет заголовок сетевого пакета, проходящего через устройство маршрутизации трафика, изменяя там IP адрес. Получив пакет от компьютера, находящегося в локальной сети, маршрутизатор смотрит на IP-адрес назначение. Если адрес назначения находится в пределах локальной сети, то пакет спокойно пересылается другому компьютеру без изменений, а если нет, то происходит замена IP-адресов для доступа выхода в глобальную сеть. Пример использования NAT изображен на рис. 1.

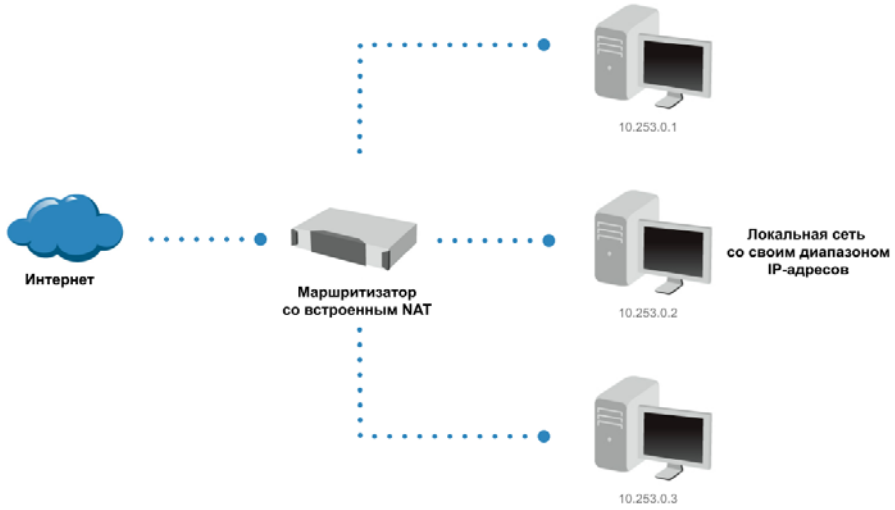


Рис. 1. Пример использования NAT.

NAT бывает трёх концепций:

1. Статический NAT – адресная трансляция, имеющая сопоставление между глобальными и локальными IP-адресами на основании один к одному. Пример представлен в таблице 1.

ТАБЛИЦА 1. Сопоставление статических адресов NAT

Таблица статического NAT	
Внутренний локальный адрес	Внутренний глобальный адрес
192.168.1.2	208.165.18.5
192.168.1.3	208.165.18.6
192.168.1.4	208.165.18.7

2. Динамический NAT – адресная трансляция, где локальные IP-адреса меняются на глобальный IP-адрес из пула доступных IP-адресов. Пример показан на таблице 2.

ТАБЛИЦА 2. Сопоставление динамических адресов NAT

Таблица статического NAT	
Внутренний локальный адрес	Пул доступных глобальных IP-адресов
192.168.1.2	208.165.18.5
Доступен	208.165.18.6
Доступен	208.165.18.7

3. Перезагружаемый NAT (PAT) – адресная трансляция, форма динамического NAT, который меняет несколько локальных адресов в единственный глобальный IP-адрес, воспользовавшись различными портами. Пример использование перезагружаемого NAT можно увидеть на рис. 2.

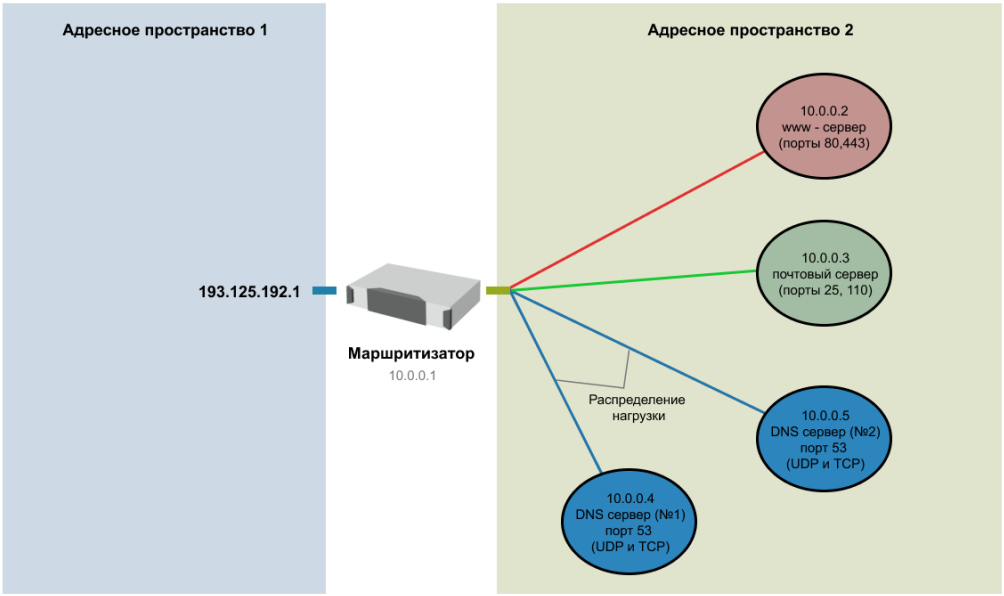


Рис. 2. Пример использования перезагружаемого NAT

Основными преимуществами технологии трансляции сетевого адреса являются:

– Используя концепцию PAT, имеется возможность зарегистрировать большую локальную сеть всего лишь под одним общедоступным IP-адресом для выхода в глобальную сеть, что позволяет значительно сэкономить;

– Благодаря большому количеству пулам адресов, пулам балансировки и резервному копированию обеспечиваются надёжные сетевые подключения, что повышает гибкость коммуникации в глобальной сети;

– При размещении NAT в локальной сети сохраняется возможность облегчённого внесения изменений в общедоступную схему адресации, то есть изменение провайдера с сохранением локальной сети;

– Частная сеть с технологией NAT скрывает внутренние IP-адреса и топологию, что повышает уровень безопасности.

Недостатками, которые значительно влияют на технологию NAT в настоящее время являются:

•Из-за большого количества изменений IP-адресов сетевых пакетов осложняется трассировка, а также определения и устранения неполадок;

•Из-за того, что технология NAT трансформирует пакеты каждого IPv4-адреса производительность интернет-сети снижается;

•Технология трансляции сетевого адреса осложняет работу протоколов туннелирования и IPsec из-за изменения значений заголовков, что усложняет проверки целостности.

•Потеря сквозной адресации. Если приложение пользуется физическими адресами, то пакеты не попадают к получателю через роутер с технологии NAT.

Потеря сквозной адресации означает, что устройства не смогут передавать пакеты напрямую в глобальной сети что является главной проблемой в механизме трансляции сетевого адреса, так как на ней завязаны все протоколы реального времени и значительная часть приложений [2].

Решение данной проблемы является не тривиальной задачей, так как универсального способа решения нет из-за разных архитектур сетей и отдельно взятые методы не всегда дают нужный эффект, но использовав несколько методов вместе можно решить возникшую проблему.

Популярные методы обхода NAT:

1. Обход NAT из-за ретрансляции сетевого потока через сторонний публичный сервер. Для реализации ретрансляции используется протокол Traversal Using Relay NAT (TURN). Благодаря данному методу можно добиться обхода любого NAT, но возникают проблему с задержкой и надёжностью, так как весь поток зависит от обработки потока на сервере.

2. Session Traversal Utilities for NAT (STUN) – сетевой протокол и стандартизированный набор методов для определения глобального IP-адреса, способ трансляции и порта во внешней сети узлу, находящемуся за NAT [3].

3. Interactive Connectivity Establishment (ICE) – метод, используемый для нахождения наиболее прямого соединения для двух компьютеров друг с другом, использующий STUN и TURN (при необходимости) [4].

4. Universal Plug and Play (UPnP) – набор сетевых протоколов, созданных на основе открытых интернет-стандартах предназначенных для автоматической настройки сетевых устройств для дома и корпоративной сети, которые позволяют открыть и перенаправить внешние порты устройства и передать настройки NAT автоматически без физического доступа к NAT или его панели администрирования

5. Пробивка отверстий (Hole punching) – метод в компьютерной сети, созданный для установления прямого соединения между двумя устройствами, где как минимум один находится за маршрутизатором или межсетевым экраном с технологией трансляции сетевого адреса. Для создания дыры, каждое устройство подключается к публичному неограниченному стороннему серверу, который сохраняет информацию о локальном и глобальном IP-адресе и порте для каждого устройства на время. После чего сервер отправляет информацию о полученном устройстве другому, и воспользовавшись полученной информацией устройства соединяются друг с другом. Пробивка отверстий имеет 3 варианта с разными используемыми протоколами, например:

– пробивка отверстий UDP использует дейтаграмму пользователя;

– пробивка отверстий TCP использует протоколы управления передачей;

– пробивка отверстий ICMP требует управляющее сообщение Интернета [5].

Благодаря перечисленным методам выше, решается одна из основных проблем механизма преобразования сетевых адресов – отсутствие сквозной адресации. Создав сквозную адресацию между двумя устройствами, мы регистрируем их для NAT другого устройства и пакеты не отбрасываются, что позволяет повысить эффективность и надёжность сети, особенно для VoIP, и приложениях, завязанных на пакетах реального времени.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2016. 847 с.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 487-488 с.: ил. ISBN 978-5-459-00342-0

3. Rosenberg J., Weinberger J., Huitema C., Mahy R. STUN - Simple Traversal of User Datagram Protocol (UDP). Network Address Translators (NATs). RFC 3489, 2003. 3 с.

4. Keranen A., Holmberg C., Rosenberg J. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal. RFC 8445, 2018. 5-12 с.

5. Srisuresh P., Ford B., Kegel D. State of Peer-to-Peer (P2P). Communication across Network Address Translators (NATs). RFC 5128, 2008. 7-21 с.

Статья представлена научным руководителем, кандидатом технических наук, доцентом М. Д. Поведайко.

УДК 007.658.5
ГРНТИ 20.15.13

ПРИМЕНЕНИЕ МОДЕЛИ УГРОЗ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

И. В. Гвоздков, М. А. Мироненкова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Все отношения и действия, которые связаны с персональными данными и их обработкой в информационных системах персональных данных, регламентирует Федеральный закон РФ №152 от 22.07.2006 года.

Важнейшей задачей, при обработке персональных данных, является обеспечение их защищенности.

Федеральный закон РФ №152, персональные данные, информационная система персональных данных, обработка, утечка, Модель угроз.

В статье 19 Федерального закона РФ №152 констатируется следующее: обеспечение безопасности персональных данных достигается определением

угроз безопасности персональных данных при их обработке в информационных системах персональных данных, при помощи разработки Модели угроз безопасности информации, которая является обязательной для федеральных органов исполнительной власти, органов государственной власти субъектов РФ, Банка России, органов государственных внебюджетных фондов и т.д. Кроме того, ассоциации, союза и иные объединения операторов вправе определять дополнительные угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных [1].

К персональным данным можно отнести ФИО с адресом проживания, номером телефона, паспортными данными; медицинскую карту или финансовую ведомость; ИНН, СНИЛС, лицевые счета, счета за различные жилые и коммунальные услуги.

Данный список можно дополнить разнообразными примерами, которые зависят от условий, при которых осуществляется обработка персональных данных.

В жизни любого человека его персональные данные задействованы во всех сферах деятельности. Это может обуславливаться личными и семейными нуждами, либо деловыми или рабочими потребностями, начиная от проезда в общественном транспорте до начисления заработной платы в бухгалтерии.

– Проезд на общественном транспорте по проездному или льготному билету.

– Регистрация дисконтных карт в магазинах.

– Использование пропусков для легитимного прохождения через систему контроля и управления доступом на территорию организации.

– Оплата счетов за ЖКХ.

– Заявления при устройстве на работу или заявления для получения образовательных услуг.

– Регистрация сим-карт.

– Карты пациентов в поликлиниках и больницах.

– Личные страницы в социальных сетях, где зачастую указывается настоящее ФИО, фотография человека, номер телефона, электронная почта, политические и религиозные взгляды и т.п. (в том числе регистрация личной страниц в социальной сети, так как это происходит по номеру телефона и (или) электронной почты).

– Предоставление банковских услуг (выпуск карты, кредиты, рассрочки, ипотека и прочие различного рода банковские операции)

Среднестатистический день любого студента состоит из десятка различных операций, которые включат в себя обработку персональных данных.

– Утром на учёбу студент добирается на общественном транспорте, используя студенческий проездной билет, который применяется в метрополитене и на наземном транспорте. В некоторых случаях студент добирается до города на пригородной электричке – для покупки билета на электричку могут использоваться данные либо студенческого, либо проездного билета.

– Чтобы попасть на территорию учебного заведения, студенту необходимо предоставить свой личный именной пропуск или студенческий билет на входе.

– В течение дня студент пользуется социальными сетями и различными хостингами, необходимые в учебной деятельности, где запрашивают разрешение на использование файлов cookie.

– На обеденном перерыве студент оплачивает обед в столовой учебного заведения или ином месте общественного питания, расплачиваясь банковской картой.

– Для того, покинуть место учёбы необходимо предоставить личный именной пропуск или студенческий билет на выходе.

– По дороге домой студент может зайти в почтовое отделение для получения своего заказа, где необходимо предоставить свои данные, чтобы подтвердить личность и забрать онлайн-покупку.

– В течение всего дня студент пользуется социальными сетями для личных нужд.

При обработке персональных данных любой категории, в любой сфере и с любой целью обработки, сохранение их конфиденциальности, целостности и доступности имеет наивысший приоритет. Таким образом, возникает необходимость построения системы защиты, которая полностью обеспечит сохранность персональных данных, исключая возможность их утечки.

Статистика утечек персональных данных в России за 2020–2021 г.

Центр ресурсов кражи личных данных (ITRC) провел исследование, включающее в себя анализ утечек персональных данных в России за 2020–2021 г. Приведя подробную статистику общего количества утечек персональных данных.

Согласно данной статистики было зафиксировано, что в 2020 году, количество утечек данных в мире превысило общее количество событий более, чем на 17 %.

Экспертно-аналитический центр InfoWatch провел анализ российского рынка на предмет утечек данных. Специалисты выявили более четырехсот случаев утечек в коммерческих и государственных компания. Согласно отчету:

– В 2020 году в РФ зарегистрировали на 2,2 % больше утечек данных, чем в 2019 году.

– За 2020–2021 год «утекло» более 100 млн записей персональных данных и платежной информации.

– Более 40 % зарегистрированных утечек произошли в сфере высоких технологий и финансовом секторе.

– Почти 80 % утечек данных произошло в результате умышленных действий сотрудников (в 2019 году доля утечек по вине внутренних нарушителей составляла 38,7 %).

– Почти 20 % утечек происходит через мессенджеры, а 14,8 % пришлось на неопределенные случаи утечек.

Графическое изображение анализа российского рынка на предмет утечки персональных данных приведено на рис. 1.

Рис. 1. Количество утечек данных и пострадавших лиц

Самые громкие утечки, на территории России, связаны с крупнейшими банками. В это число попали «Совкомбанк», «Альфа-Банк» и «Сбербанк».

Свои итоги по защите прав и интересов граждан в сфере персональных данных, за 2021 год, подвел и Роскомнадзор

Сотрудниками Роскомнадзора было зафиксировано, что за 2021 год поступило белее тридцати восьми тысяч жалоб граждан на неправомерную обработку их личной информации. В число организаций, на владельцев которых поступали жалобы, входят кредитные учреждения, организации ЖКХ, коллекторские агентства.

Всероссийский центр изучения общественного мнения провел независимый опрос граждан России, касающийся их мнения, в отношении сбора, использования и безопасности их личных данных.

Исходя из данного опроса следует, что 74% россиян полагают, что не застрахованы от утечки своих личных данных.

Кроме того, в ходе исследования, было изучено, в какие организации россияне предоставляют свои персональные данные и почему.

Как выяснилось, почти половина опрошенных (49 %) за 2021 год получали банковские услуги, при которых это необходимо, – оформление кредитов и заявления на получение зарплатных карт. На втором месте менее очевидный вариант – 46 % давали разрешение на определение своей геолокации при использовании навигаторов и других приложений, программ или сайтов. 45 % регистрировались на сайтах госучреждений, 38 % – оформляли доставку на дом и столько же – сами делились информацией в социальных сетях, например, выставляли свои фотографии.

Графическое изображение проведенного исследования приведено на рис. 2.

Рис. 2. Результаты проведенного исследования

Исходя из результатов исследований очевидно, что россияне предоставляют свои личные данные как в государственные, так и в коммерческие организации, удовлетворяя личные, финансовые, деловые, развлекательные и прочие потребности, но с присутствующим высоким риском их утечки, который может повлечь за собой значительные моральные и материальные потери.

Исключение возможных рисков возможно только при построении комплексной системы защиты информации, которая включает в себя организационные и технические меры по противодействию возможным внешним и внутренним нарушителям для информационных систем, в которых осуществляется обработка персональных данных граждан.

Ответственность за обеспечение защищенности персональных данных лежит на организациях, которым граждане предоставили свою личную информацию, в соответствии с нормативно-правовыми актами Российской Федерации.

Федеральная служба по техническому и экспортному контролю утвердила Методический документ «Методика оценки угроз безопасности информации» 5 февраля 2021 года. Благодаря данному Методическому документу возможно разработать Модель угроз безопасности информации для информационных систем, в которых обрабатываются не только персональные данные, но иная конфиденциальная информация. Моделирование угроз безопасности информации позволит определить технологический процесс обработки информации, возможные источники угроз безопасности, возможные негативные последствия от реализации угроз безопасности, возможные объекты воздействия и прочие факторы, благодаря которым можно полноценно оценить, какие угрозы могут быть реализованы в информационной системе.

Благодаря Модели угроз безопасности информации для информационной системы, представляется реальной возможность построения системы защиты таким образом, чтобы исключить вероятность утечки любой информации.

Список используемых источников

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.
2. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом М. Д. Поведайко.

УДК 004.056.53
ГРНТИ 81.93.29

ПРОТОТИП МНОГОУРОВНЕВОЙ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

И. В. Гвоздков, А. А. Орехов, А. А. Саранцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Безопасность информации является стратегически важной целью общества. Безопасными должны быть все процессы производства, хранения и обмена информацией, все технические и программные компоненты, участвующие в этих процессах. Многофакторная аутентификация лучше однофакторной. Но если посмотреть на способы аутентификации в системах контроля доступом практически любой организации, окажется, что в большинстве систем используется однофакторная аутентификация. В статье приводится предложение по реализации прототипа многоуровневой системы

контроля доступа способствующий повышению безопасности объекта при минимальных вложениях.

СКУД, система контроли и управления доступом, многофакторная аутентификация, TOTP, FaceID, MFA.

При защите любого важного объекта используют системы контроля и управления доступом (СКУД). С их помощью разграничивают права для прохождения на объекты определенных лиц с целью обеспечения безопасности и регулирования посещения определённого объекта.

Система контроля доступа состоит из четырех основных блоков: идентификатор, считыватель, контроллер и преграждающее устройство.

В качестве идентификаторов может выступать карта, брелок, ключ, биометрия (черты лица, сетчатка радужной оболочки глаза, отпечатки пальцев либо ладони, голос, форма кисти руки, ДНК). От вида оборудования зависит и уровень надежности, различные виды риска подмены, быстродействие процедуры распознавания. Одни из более эффективных признаны биометрические технологии, они характеризуются защитой от эмуляции, очень высокой точностью, быстротой, и что немаловажно комфортом для пользователя.

Выделяется три фактора аутентификации – это фактор знания (например, пароль), фактор владения (например, смарт-карта) и фактор признака (например, биометрия).

В биометрии различают два аутентификационных метода – статический и динамический. Статические методы, в основе которых лежат физиологические признаки человека, присутствующих с ним на протяжении всей его жизни: идентификация по отпечатку пальца, лицу, радужной оболочке глаза, геометрии руки, термограмме лица, ДНК, на основе акустических характеристик уха, идентификация по рисунку вен.

Динамические методы, в основе которых лежат поведенческие характеристики людей, а конкретнее – подсознательные телодвижения в процессе повторения различных повседневных действий, например, походка, почерк, голос [1].

Для повышения безопасности СКУД используют многофакторную аутентификацию, в которой пользователю системы, чтобы получить доступ к информации нужно предъявить больше одного идентификатора.

Одним из самым распространённых, простых и бюджетных решений являются двухфакторные системы контроля доступа, использующие сочетание факторов знания и владения, например, RIFD метка и пароль пользователя.

Также существуют различные вариаций комбинирований факторов. И чем больше используются независиме факторы в системе, тем выше становится уровень защиты. Но при этом и стоимость кратно возрастает.

Систему двухфакторной авторизации, одним из методов в которой является биометрическая проверка, можно считать эталоном безопасности.

Главный минус биометрического СКУД – это их сложная настройка.

Однофакторная система аутентификации (SFA) – это базовый и элементарный метод проверки подлинности, при котором используется единственная категория аутентификации. Самым распространенным примером однофакторной аутентификации в СКУД является использование смарт-карты или введением простого PIN-кода.

Двухфакторная аутентификация (2FA) – двухэтапный процесс проверки, при котором учитывается два разных типа пользовательских данных. Например, комбинирование двух базовых методом – смарт-карта и PIN-код.

Многофакторная аутентификация (MFA) – является самым актуальным и современным методом проверки подлинности, который использует два, три или даже более уровней безопасности при аутентификации. Различные категории всех уровней должны быть независимыми друг от друга, чтобы устранить любую уязвимость в системе. Примером является использование одновременно нескольких факторов – смарт-карты, отпечатка пальца или ладони, сетчатки радужной оболочки глаза и голосу или любые другие сочетания факторов [2].

Но главная проблемой MFA это сложная настройка взаимодействия между факторами в одной системе. Также при внедрении дополнительного фактора, резко увеличивается стоимость внедрения и обслуживания.

Многоуровневая система позволяет внедрить дополнительный биометрический фактор в уже существующую СКУД. Это на порядок повышает безопасность системы контроля и управления доступом при этом позволяет внедрить этот фактор без сильных затрат.

В качестве предлагаемого решения представлена схема на рис. 1.

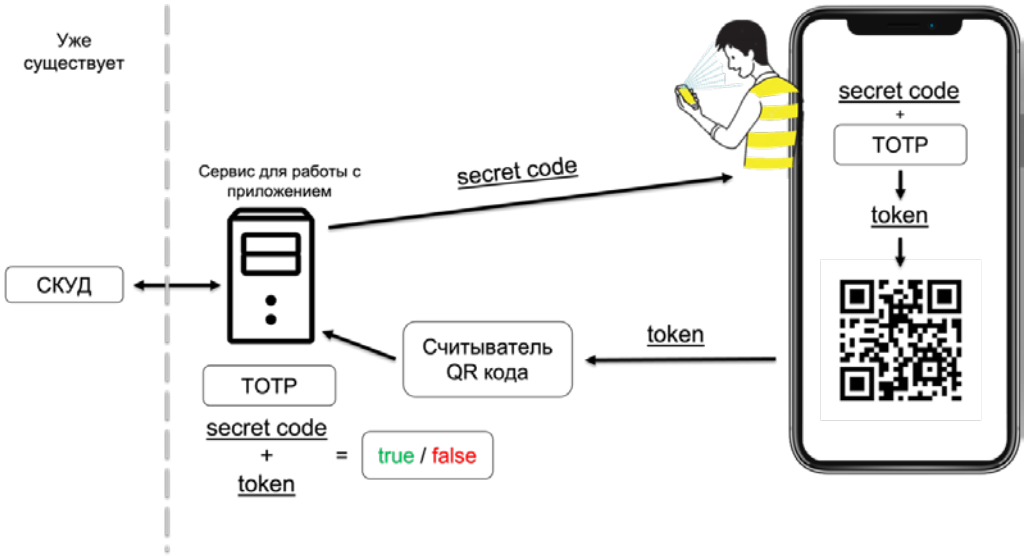


Рис. 1. Схема предлагаемого решения

Для внедрения дополнительного фактора аутентификации в уже существующую СКУД используется биометрия лица. Сканер объёмно-пространственной формы лица человека создается с помощью камеры FaceID которая уже встроена с завода в клиентское устройство и позволяет легко взаимодействовать с ней.

Система работает на основе TOTP алгоритма. Сервер взаимодействует с уже существующей СКУД, куда просто отправляется информация о том, пройден ли дополнительный фактор аутентификации или нет.

Сервер выполняет следующие задачи: регистрация, аутентификация и проверка TOTP токена (рис. 2).

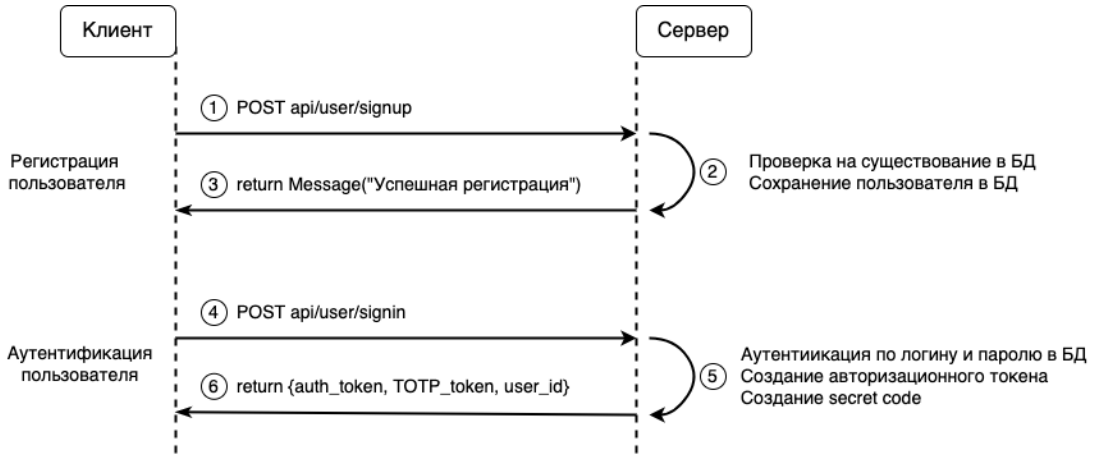


Рис. 2. Схема взаимодействия клиента с сервером

Клиент регистрируется в системе с логином и паролем, шаг 1. Шаг 2 сервер проверят на существование данного пользователя в базе данных. Если пользователя нет, то сервер регистрирует его и возвращает сообщение с успешной регистрацией на шаге 3. Далее, когда пользователь уже зарегистрирован, он может пройти аутентификацию – шаг 4. При аутентификации (шаг 5), сервер проверяет введенные пользователем логин и пароль, если данные верны, то сервер создает авторотационный токен с помощью которого возможно дальнейшее взаимодействие с сервером без ввода логина и пароля. А также на этапе 5 генерируется секретный код (secret code на рис. 1), который сохраняется в базу данных и передается в клиентское приложение на устройство пользователя, который нужен для последующей генерации одноразового TOTP токена (token на рис. 1). Для того чтобы считыватель смог идентифицировать клиента, на шаге 6 передается *id* пользователя.

Для проверки TOTP токена, используется TOTP алгоритм. Если токен валидный, то существующей СКУД сообщается то, что дополнительный фактор аутентификации был пройден успешно.

Схема взаимодействия клиента со считывателем представлена на рис. 3.

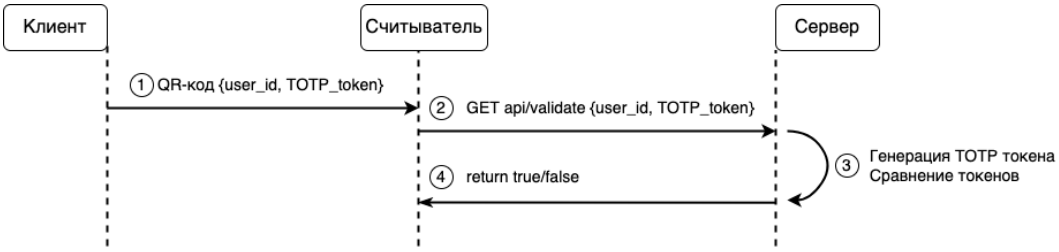


Рис. 3. Схема взаимодействия клиента со считывателем

В мобильном приложении у клиента генерируется TOTP токен на основании secret code. Используя *id* пользователя и secret code, создается QR-код, который отображается на экране. Далее на шаге 1 QR-код считывается с помощью считывателя. После того как приложение сгенерировало токен, токен представляется в формате QR-кода, который в дальнейшем удобно представить для считывателя QR-кодов, который имеет связь с сервером. Считыватель преобразует данные, которые есть в QR-коде и делает запрос на сервер передавая полученные данные – шаг 2. На шаге 3, сервер получая *id* пользователя находит в базе данных srcret code, который соответствует клиенту, и не основании TOTP алгоритма генерирует TOTP токен используя данный код. Если токен сгенерированный сервером и полученный от считывателя, равны и идентичны, то сервер возвращает на считыватель положительный результат, если токены не совпадают, то возвращается отрицательный результат – шаг 4. Также информация о сравнении токенов на шаге 3 отправляется в уже существующую СКУД, тем самым сообщая о прохождении фактора аутентификации. На основании полученного результата, считыватель может отобразить информацию о том, прошел ли данный фактор аутентификации или нет [3].

Каждый раз, когда пользователь открывает мобильное приложение и хочет пройти аутентификацию, смартфон использует FaceID и Time-of-flight-камеру, с помощью которой делает дальностное изображение (дальностный портрет). Используется для создания изображений, которые в качестве пикселов содержат оценки расстояний от экрана до конкретных точек наблюдения. Если черты лица окажутся достаточно похожи на 3D-карту лица из памяти телефона, клиент будет признан легитимным пользователем, то есть ему будет позволено войти в систему для генерации TOTP токена [4].

Работа прототипа представлена на рис. 4.

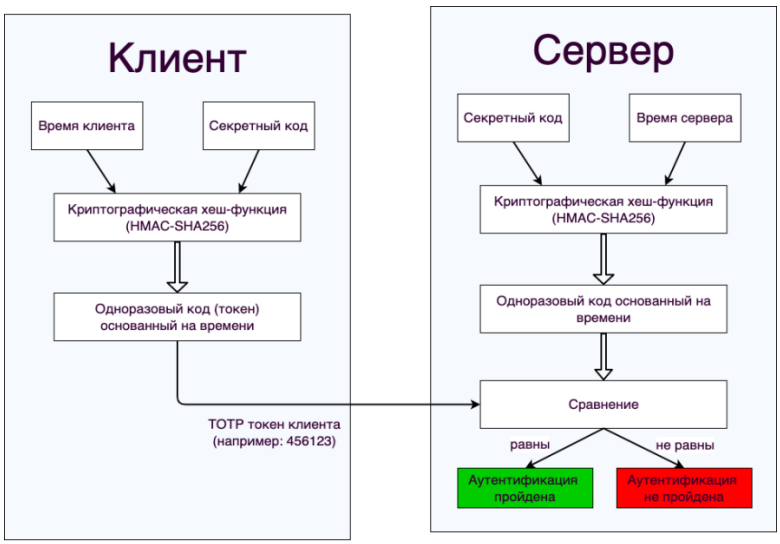


Рис. 4. Схема работы прототипа

Клиентское приложение и сервер генерирует одноразовый код с помощью криптографической хэш-функции, основанной на алгоритме HMAC-SHA256, используя для алгоритма текущее время и секретный код. Клиент отправляет сформированный токен на сервер, где происходит сравнение двух токенов. Если эти токены одинаковы, то аутентификация пройдена, иначе – не пройдена.

Список используемых источников

1. Вайнштейн Ю. В., Демин С. Л. Основы информационной безопасности: Учебное пособие. Красноярск, 2014. 270 с.

2. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Advances in cryptology, EUROCRYPT'99, 1999. С. 223–238.

3. Feldman, P. A Practical Scheme for Non-interactive Verifiable Secret Sharing // IEEE Symposium on Foundations of Computer Science, 1987. Pp. 427–437.

4. Pedersen T. P. «Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing» // EUROCRYPT’91, 1991. Pp. 129–140.

Статья представлена заведующим кафедрой БИС СПбГУТ, кандидатом технических наук, доцентом Ю.М. Бородянским.

УДК 004.855
ГРНТИ 28.23.37

ОБНАРУЖЕНИЕ АНОМАЛИЙ НА ХОСТЕ С ИСПОЛЬЗОВАНИЕМ МОДЕЛЕЙ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Г. Л. Голубенков, Д. Е. Горохов

Академия Федеральной службы охраны Российской Федерации

Системный вызов – обращение прикладной программы к ядру операционной системы для выполнения какой-либо операции. Хостовая система обнаружения вторжений на основе поведенческого метода определяет атаки на основе отклонения системы от нормального поведения. Однако данные системы имеют низкую скорость обнаружения. В данной статье предлагается использование нейронных сетей в качестве механизма принятия решения, использующих в качестве входных данных трассировки системных вызовов. Для обучения предлагаемых моделей обнаружения вторжений и проверки их эффективности используется набор данных ADFA-LD.

глубокое обучение, системные вызовы, обнаружение аномалий.

Задача обнаружения аномального поведения программных средств на уровне хоста в настоящее время остается актуальной несмотря на значительное внимание к ней исследователей и разработчиков систем информационной безопасности. По данным экспертов из «Positive Technologies» атаки с использованием ВПО занимают первое место среди инструментов, используемых киберпреступниками. Отмечается, что 20 % жертв злоумышленников являются госучреждениями, что свидетельствует о большом внимании преступников к данному сектору, а также неспособность вышеуказанного сектора обеспечить требуемый уровень защиты в области информационной безопасности [1].

При проведении атак, злоумышленники в 87 % случаях выбирают объектом атак компьютеры, серверы и сетевое оборудование, используя вредоносное программное обеспечение. Доля эксплуатации данного метода увеличилась с 63 % до 73 % по сравнению с предыдущим кварталом. Также в качестве атаки достаточно часто выбирают сотрудников, в том числе и для использования их как средства доставки вредоносного программного обеспечения. Для этого используются методы социальной инженерии. 30% всех атак происходит при эксплуатации уязвимостей цели. Этому подвержено как аппаратное (компьютеры, серверы, сетевое оборудование), так и программное (веб-ресурсы) обеспечение.

Статистика показывает, что задача выявления признаков деятельности злоумышленника по реализации угроз критической информационной инфраструктуры на сегодняшний день решена не в полном объеме. Исходя из этого считается необходимым совершенствовать защиту устройств в области информационной безопасности для нивелирования угроз, существующих в данный момент, а также потенциально возможных в будущем.

Указанные угрозы могут выявляться в режиме реального времени с использованием системы обнаружения вторжений (СОВ), которая также имеет аббревиатуру IDS (Intrusion Detection System – система обнаружения вторжений). IDS можно разделить на два типа: хостовые IDS (HIDS – Host-based IDS) и сетевые IDS (NIDS – Network IDS). Данное деление опирается на различия в размещении и зонах ответственности на основе источников данных [2]. Для обнаружения компьютерных атак HIDS анализирует информацию, собранную из конкретных систем хоста, в то время как NIDS отслеживает сетевой трафик [3], на основе которого обнаруживает векторы атак, то есть в отличие от сетевой, хостовая система обнаружения вторжений фокусируется на мониторинге и анализе внутренней системы, а не внешней сети.

Существует две модели обнаружения вторжений, а именно метод обнаружения злоупотребления (сигнатурный метод обнаружения) и метод обнаружения аномалий (поведенческий метод обнаружения). Оба подхода используют информацию, извлеченную из объекта анализа, чтобы определить, произошло ли вторжение [4, 5, 6]. Метод обнаружения злоупотреблений, который используется в сигнатурных HIDS, эффективен при обнаружении известных векторов атаки; тем не менее, он уязвим для атак, вектор которых отсутствует в базах данных сигнатур. В связи с этим необходимы методы обнаружения аномалий [6, 7]. В частности, такой подход определяет и обнаруживает любые аномалии, то есть отклонения от нормального поведения на основе существующих сценариев использования сети, внутренних системных вызовов и т. д. Как следствие, данный тип систем способен определить атаки нулевого дня. Однако данный подход имеет высокую вероятность ложной идентификации. Начиная с подхода, предложенного в [8], работы по снижению частоты ложных тревог в HIDS привели к большому количеству исследований [6]. Однако следует отметить, что точность методов все еще недостаточно высока.

Фундаментальным компонентом HIDS является источник данных, предоставляющий неотъемлемую информацию, на основе которой механизм принятия решений может классифицировать действия. Со времени первой работы Форреста [8] системные вызовы широко признаны предпочтительным источником данных для HIDS. Системные вызовы – это метод, с помощью которого программы могут получить доступ к основным функциям ядра и обеспечить широкий спектр разрешенных взаимодействий

с низкоуровневым пространством ОС. Сбор обычно осуществляется путем группировки системных вызовов, полученных ядром, с использованием исходного процесса и времени сбора. Результатом этого процесса является набор трассировок, где каждая трассировка содержит системные вызовы одного процесса в том порядке, в котором их получило ядро.

Среди различных экспериментальных наборов данных, используемых для исследования HIDS, общедоступный набор данных для обнаружения и интеллектуального анализа данных ADFA-LD обеспечивает комплексный подход к формированию данных для системы обнаружения вторжений. Эксплойты, используемые для ADFA-LD, представляют собой полную компрометацию системы, от первоначального проникновения до повышения привилегий.

Таким образом, для решения задачи построения (оптимизации гиперпараметров) алгоритма выявления аномалий параметров потока системных вызовов предлагается использовать общедоступный набор данных ADFA-LD. При этом в рамках разрабатываемого алгоритма следует учесть различные способы предварительной обработки потока системных вызовов.

Многолетние исследования методов принятия решений для IDS показали, что наиболее точно работают методы, основанные на использовании скрытых марковских моделей и нейронных сетей [9, 10]. Недостатком скрытых марковских моделей является сложность вычислительных процедур при расчете матриц переходных вероятностей в условиях высокой размерности задачи. Глубокие нейронные сети приспособлены к обработке обширного массива данных, что позволяет сделать выбор в их пользу при решении инженерных задач.

Согласно семантической теории наборы правил могут использоваться для описания последовательностей единичных блоков. С точки зрения естественного языка эти правила формируют грамматику рассматриваемого языка и позволяют строить правильные предложения в рамках этого набора правил. Эти грамматики также можно использовать для выявления недопустимых или не соответствующих структуре языка предложений, и именно данная возможность предполагает их применимость в системах обнаружения вторжений. Гипотеза предполагает, что системные вызовы должны по своей сути следовать определенной грамматике, поскольку они принадлежат системе, основанной на правилах, и имеют четко определенный синтаксис. Таким образом, атаки, связанные с использованием внедренного кода или использованием необычных режимов работы программного обеспечения должны выглядеть как недопустимые или нестандартные предложения (подпоследовательности системных вызовов), следовательно, должны быть отличимы от предложений, получаемых в результате нормального функционирования системы.

Расширение семантической теории на анализ системных вызовов приравнивает реальные системные вызовы к буквам, последовательность системных вызовов к слову и наборы последовательностей системных вызовов к фразам. В рамках CFG системные вызовы становятся завершающими единицами, а последовательности – незавершающими единицами.

На основе проведённого анализа входных данных были выбраны две модели нейронных сетей, хорошо показывающие себя в задачах обработки естественного языка: BERT и LSTM.

BERT представляет собой нейронную сеть, основу которой составляет композиция кодировщиков трансформера. Необходимо отметить, что BERT является автокодировщиком. В каждом слое кодировщика применяется двустороннее внимание, что позволяет модели учитывать контекст с обеих сторон от рассматриваемого токена, а значит, точнее определять значения токенов. LSTM является модификацией рекуррентной нейронной сети, которую во многих задачах превосходит. LSTM решила проблему долговременных зависимостей, присутствующую в RNN.

ТАБЛИЦА 1. Результирующие параметры моделей в зависимости от количества входных данных

Количество данных, тыс.	**Тип нейросети**	**Точность**	**Время обучения, мин**	**Время предсказания, сек**
14	BERT	0,92512	4	20
	LSTM	0,88334	23	8
40	BERT	0,94702	8,5	44
	LSTM	0,89654	70	38
100	BERT	0,95454	14	112
	LSTM	0,90573	105	50
120	BERT	0,96410	23	138
	LSTM	0,91284	119	65

ТАБЛИЦА 2. Результирующие параметры моделей в зависимости от размера скользящего окна

Размер окна	**Тип нейросети**	**Точность**	**Время обучения, мин**	**Время предсказания, сек**
7	BERT	0,90807	2,5	15
	LSTM	0,86834	13	6
10	BERT	0,91466	3,3	17
	LSTM	0,87719	17	7
14	BERT	0,92512	4	20
	LSTM	0,88334	23	8
17	BERT	0,91208	5,2	25

Размер окна	Тип нейросети	Точность	Время обучения, мин	Время предсказания, сек
	LSTM	0,87953	28	10

После разработки моделей были проведены эксперименты для повышения точности определения аномалий в входящих данных. Результаты экспериментов приведены в таблицах 1, 2.

В ходе экспериментальных исследований на общедоступном наборе данных ADFA-LD определен наилучший в смысле минимума ошибки моделирования размер окна. Кроме того, модель BERT продемонстрировала выигрыш по отношению к LSTM по показателям точности и затраченного на обучение времени, однако данная модель имеет сравнительно низкую оперативность предсказания, что может ограничивать ее применимость в реальных приложениях. Таким образом, если время обучения не является критичной величиной для исследователей, есть возможность достичь такой же точности на LSTM, при этом сократив время предсказания.

Дальнейшим направлением исследования считается необходимым повышение точности моделей, а также их тестирование на других наборах данных и применение на реальных практических системах. Нерешенным остается вопрос формального обоснования оптимальности гиперпараметров моделей.

Список используемых источников

1. Отчет Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/news/ (дата обращения: 15.11.2021).

2. Wagner D., Soto P. Mimicry Attacks on Host-Based Intrusion Detection Systems // Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02). Washington DC, Nov. 2002.

3. Modi C., Patel D. [et al.]A Survey of Intrusion Detection Techniques in Cloud // Journal of Network and Computer Applications. Jan. 2013. Vol. 36, No. 1.

4. Depren O., Topallar M. [et al.]. An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks // Expert Systems with Applications. Nov. 2005. Vol. 29, No. 4.

5. Garcia-Teodoro P., Diaz-Verdejo J. [et al.] Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges // Computers & Security. 2009. Vol. 28, No. 1-2.

6. Creech G., Hu J. A Semantic Approach to Host-based Intrusion Detection Systems using Contiguous and Discontiguous System Call Patterns // IEEE Transactions on Computers. Apr. 2014. Vol. 63, No. 4.

7. Torkaman A., Javadzadeh G., Bahrololum M. A Hybrid Intelligent HIDS Model using Two-layer Genetic Algorithm and Neural Network // 5th Conference on Information and Knowledge Technology (IKT). 28–30 May 2013.

8. Forrest S., Hofmeyr S. A. [et al.]. A Sense of Self for Unix Processes // Proceedings of IEEE Symposium on Security and Privacy. May 1996.

9. Creech G. and Hu J. Developing a high-accuracy cross platform Host-Based Intrusion Detection System capable of reliably detecting zero-day attacks. 2013.

10. Ахметханов Р. С., Дубинин Р. С., Куксова В. И. Анализ временных рядов в диагностике технических систем // Машиностроение и инженерное образование. 2013. N 2.

УДК 004.056.53
ГРНТИ 50.37.23

КРОССАРХИТЕКТУРНЫЙ ОБФУСКАТОР С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ПРОМЕЖУТОЧНОГО ПРЕДСТАВЛЕНИЯ LLVM IR

П. Н. Горбачев, В. А. Макеев, Е. А. Солопов

Академия Федеральной службы охраны Российской Федерации

В условиях активного развития современного общества и повсеместного внедрения новых технологий во все сферы деятельности человека крайне актуальным предстаёт вопрос по обеспечению информационной безопасности. Активное внедрение проприетарного программного обеспечения в СОИ различного уровня, а также импортозамещение используемого зарубежного программного обеспечения в пользу отечественных аналогов и реализаций, заставляют всерьёз задуматься над вопросами защиты программного обеспечения.

llvm ir, обфускация, защита от исследования, защита программного кода.

Существующие методы защиты программного обеспечения можно классифицировать по способу распространения и типу носителя лицензии следующим образом [1]:

1. Локальная программная защита.
2. Сетевая программная защита.
3. Защита при помощи электронных ключей
4. Привязка к параметрам компьютера и активация.
5. Защита кода от анализа.

Можно выделить отдельно средства защиты кода от анализа и использования в других программах. В частности, применяются обфускаторы – программы, необходимые для запутывания кода с целью защиты от его анализа, модификации и несанкционированного использования [2].

Большинство из приведенных выше методов защиты применяются и сегодня, но обладают целым рядом недостатков, среди которых: дороговизна, инертность (слабая гибкость алгоритмов защиты), высокая требовательность к уровню компетенций разработчика ПО и отсутствие универсальных решений для различных задач. Кроме того, широкий круг

применимости программных продуктов различного уровня определяют недееспособность дорогостоящих и сложных в реализации средств защиты ПО [3]. Таким образом, наиболее приоритетным является программная защита кода от анализа с использованием обфускаторов. На сегодняшний день существует целый ряд обфускаторов различного уровня, среди которых можно выделить:

– *ProGuard (https://www.proguard.sourceforge.net/);*
– *Dotfuscator (https://www.preemptive.com/);*
– *COBF (https://www.plexaure.de/);*
– *Semantic Designs (https://www.semanticdesigns.com/);*
– *Stunnix (http://stunnix.com/);*
– *StarForce (https://www.star-force.ru/).*

Однако стоит отметить, что каждый из данных обфускаторов не является универсальным в силу того, что внедряется и эксплуатируется на этапе компиляции исполняемого файла из исходного кода. В связи с этим, для реализации поставленной задачи, был выбран встроенный механизм обфускации универсальной системы компиляции, оптимизации и трансформации программ – *LLVM*.

Low Level Virtual Machine – проект программной инфраструктуры для создания компиляторов и сопутствующих им утилит, который состоит из набора библиотек для построения и управления промежуточным представлением [4]. Язык промежуточного представления кода *LLVM IR* является наиболее важным звеном системы. С его помощью появляется возможность полностью абстрагироваться от особенностей высокоуровневых языков программирования и архитектуры процессора. Также, использование *LLVM IR* [6] позволит обеспечить кроссплатформенность и взаимодействие с целым рядом архитектур: *ARM*, *x86*, *x86-64*, *PowerPC*, *MIPS*, *SPARC*, *RISC-V* и другие (включая *GPU* от *NVIDIA* и *AMD*). При проектировании компилятора существует огромное преимущество в компиляции исходного языка в промежуточное представление (*IR*, *intermediate representation*) вместо компиляции в целевую архитектуру (например, *x86*). Так как много техник оптимизации являются общими (например, удаление неиспользуемого кода, распределение констант), эти проходы оптимизации могут быть выполнены напрямую на уровне *IR* и использоваться всеми целевыми платформами.

Компилятор в составе *LLVM* представлен на рис. 1 и состоит из трёх частей: фронтенд, миддленд (промежуточное представление) и бэкенд [1, 3], каждая из них выполняет свою задачу, принимая на входе и/или отдавая на выходе *IR*. При этом:

– фронтенд: компилирует исходный язык в *IR*;
– миддленд: преобразовывает *IR*;
– бэкенд: компилирует *IR* в машинный код.

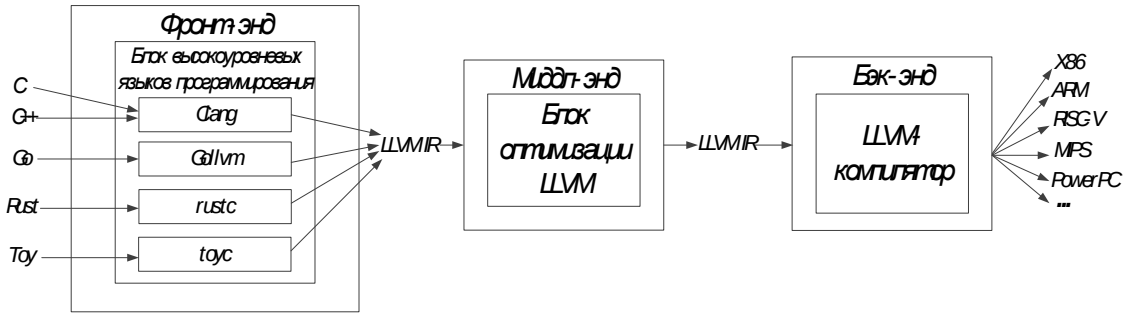


Рис. 1. Иллюстрация трансформации машинного кода в LLVM IR

На этапе промежуточного представления, появляется возможность осуществить встраивание пользовательских алгоритмов защиты программного обеспечения в виде автономных проходов, регистрируемых в качестве сторонних плагинов модульного оптимизатора и анализатора *LLVM – opt* [6].

Кроссархитектурный обфускатор реализован в формате нескольких плагинов, встроенных в opt, который принимает на вход байткод *LLVM* или же *LLVM IR* в качестве входных данных и выполняет на нем указанные оптимизационные или запутывающие преобразования, а также собирает данные, способствующие анализу кода. В завершении он выводит измененный байткод или результаты анализа без изменения семантики байткода. Кроссархитектурный обфускатор поддерживает несколько запутывающих преобразований, которые могут быть использованы совместно, в произвольном порядке или каскадным способом:

– добавление избыточности внутрь кода;

– кодирование строк;

– добавление базовых блоков для нелинейного усложнения графа потока управления.

Стоит отметить, что порядок использования различных запутывающих преобразований в связке с оптимизирующими проходами влияет на скорость выполнения программного кода [1]. На рис. 2 представлена временная диаграмма, которая доказывает, что наиболее оптимальным для задач обфускации является следующий порядок проходов: оптимизация, запутывающее преобразования и повторная оптимизация.

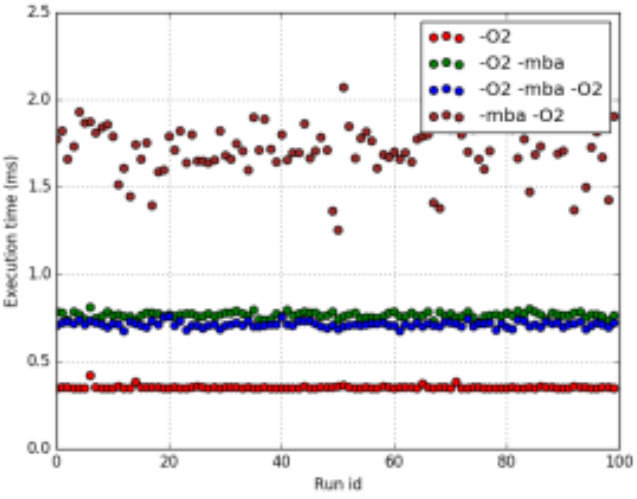


Рис. 2. Временная диаграмма зависимости времени выполнения программы от порядка следования проходов

Обфусцирующее преобразование, реализующее добавление базовых блоков в граф потока управления состоит из двух частей [5]. В первом блоке модуля осуществляется анализ содержимого базовых блоков на предмет выявления достижимых целочисленных значений, содержащихся в базовом блоке, т.е. выявляются все целочисленные значения, которые видны и могут быть исполнены в рамках текущего базового блока. Результат преобразования представлен на рис. 3, где в левой половине экрана оригинальный граф потока управления (*CFG*), а справа граф потока управления программы после одной итерации обфусцирующего преобразования.

В качестве демонстрации эффективности использования описанного подхода к защите программного кода от исследования на рис. 4 представлен отчёт от службы, осуществляющей анализ подозрительных файлов и ссылок на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ – *VirusTotal*. Слева результат после компиляции тестового экземпляра ВПО с использованием предложенного в статье обфусцирующего преобразования, справа обычная компиляция без обфусцирующих преобразований и оптимизации.

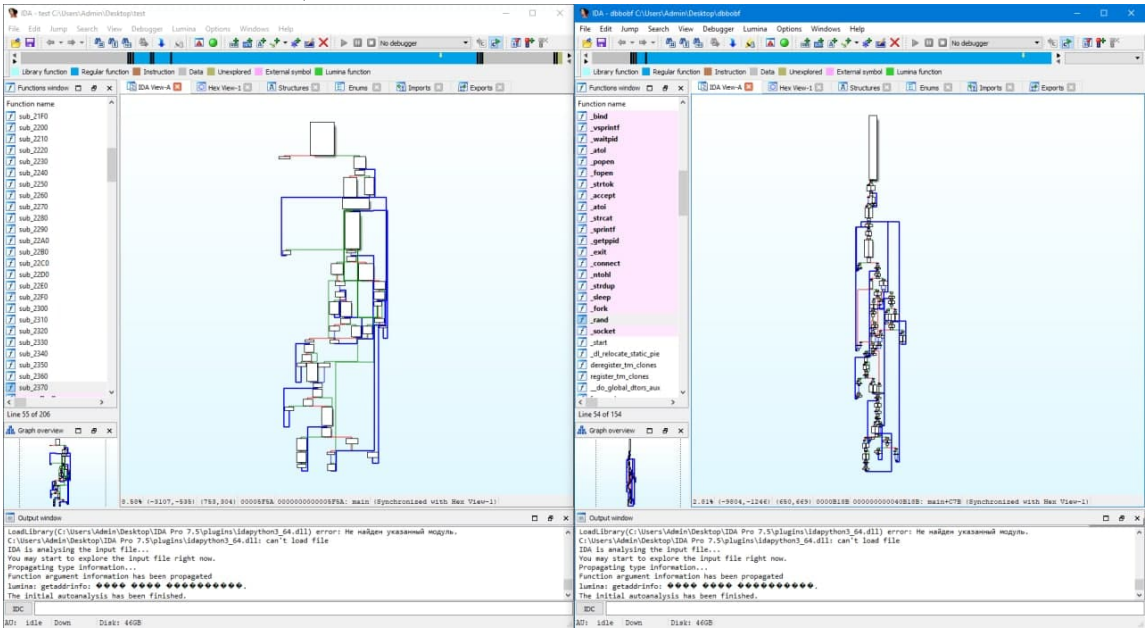


Рис. 3. Результат запутывающего преобразования
по добавлению базовых блоков в граф потока управления программы

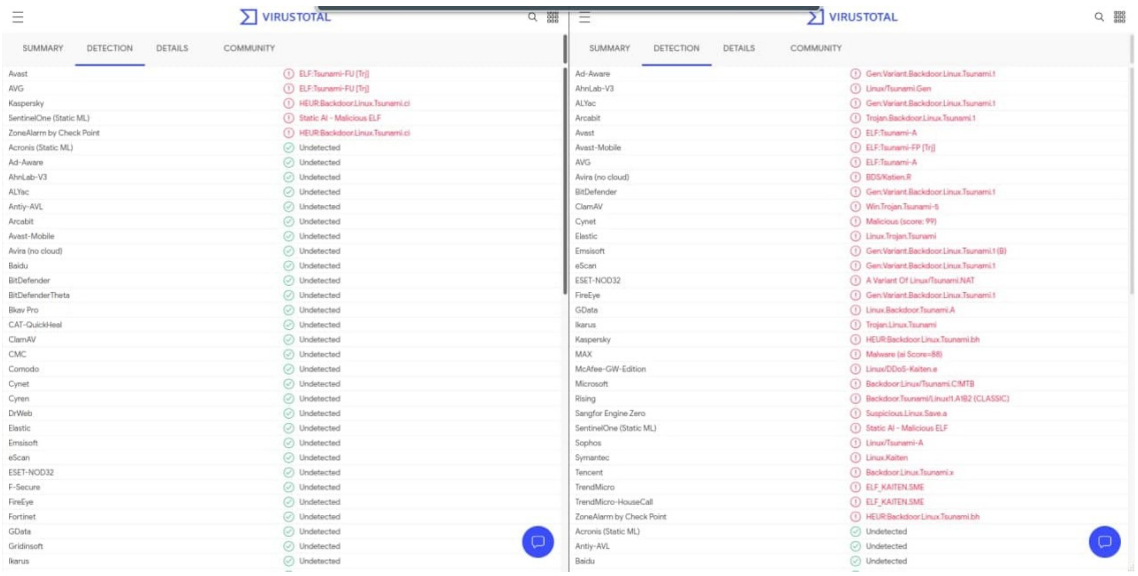


Рис. 4. Отчёт от службы *VirusTotal*

Таким образом, уменьшение обнаружений тестового ВПО в несколько раз говорит о том, что предложенное решение по защите ПО является эффективным.

Список используемых источников

1. Чернов А. В. Анализ запутывающих преобразований программ. URL: http://www.citforum.ru/security/articles/analysis/ (дата обращения: 11.02.2022).

2. Поздеев А. Г., Кривопалов В. Н., Ромашкин Е. В., Радченко Е. Д. Математические и программные средства обфускации программ // ПДМ. 2009. С. 52–53.

3. Косолапов Ю. В. Об обнаружении атак типа повторного использования исполняемого кода // Моделирование и анализ информационных систем. 2019. С. 213–228.

4. Нурмухаметов А. Р. Применение диверсифицирующих и обфусцирующих преобразований для изменения сигнатуры программного кода // Труды ИСП РАН. 2016. С. 93–104.

5. Борисов П. Д., Косолапов Ю. В. Модель экспериментального анализа стойкости алгоритмов обфускации // Современные информационные технологии и перспективы развития. Труды XXV научной конференции СИТО-2018. 2018. С. 37–39.

6. Борисов П. Д., Косолапов Ю. В. О выборе характеристик для оценки стойкости обфусцирующих преобразований // Современные информационные технологии: тенденции и перспективы развития. Труды XXVI научной конференции СИТО-2019. 2019. С. 42–44.

УДК 004.056.53
ГРНТИ 50.37.23

ТРАНСФОРМАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ APPLE IOS В ПРОМЕЖУТОЧНОЕ ПРЕДСТАВЛЕНИЕ LLVM IR

П. Н. Горбачев, В. А. Макеев, Е. А. Солопов

Академия Федеральной службы охраны Российской Федерации

iOS является второй по популярности мобильной операционной системой и считается ”наиболее безопасной” по сравнению с Android. Значительная часть этой репутации обусловлена тем фактом, что экосистема приложений находится под исключительным контролем Apple. Возможность для распространения вредоносных программ намного выше из-за обязательства зарегистрироваться в программе разработчика Apple, процесса проверки AppStore и возможности Apple централизованно отзывать приложения. Однако вредоносное ПО - не единственная угроза безопасности и конфиденциальности пользователей, что обуславливает необходимость в универсальном решении для анализа безопасности программного обеспечения Apple iOS.

apple ios, llvm ir, трансформация исполняемых файлов, технология анализа программного обеспечения.

Закрытый характер экосистемы приложений и тот факт, что приложения для *iOS* гораздо сложнее перепроектировать, чем приложения для *Android*, привлекли внимание многих исследователей и хакеров от *iOS* к платформам, которые легче оценивать и атаковать. Но приложения для *iOS* не более безопасны, чем их аналоги для *Android* [1]. В отличие от приложений *Android*, которые в основном состоят из байт-кода, безопасного для памяти, и которым присваивается отдельный идентификатор пользователя для каждого приложения, приложения *iOS* обычно запускаются под одной и той же учетной записью пользователя и ограничены песочницей, которая применяет к ним обязательные профили контроля доступа – механизм, который, как было показано, был ошибочным в прошлом [2].

Для пользователей внутренности приложения *iOS* остаются крайне неясными, и доверие к приложению зависит исключительно от процесса проверки *AppStore*, детали которого неизвестны общественности и проверку которого в прошлом обходили [3]. Таким образом, способы автоматического анализа приложений *iOS* на предмет уязвимостей срочно необходимы для повышения прозрачности для пользователя и укрепления доверия к экосистеме.

Автоматизированный реверс-инжиниринг приложений *iOS* – это сложный процесс, включающий несколько этапов (рис.):

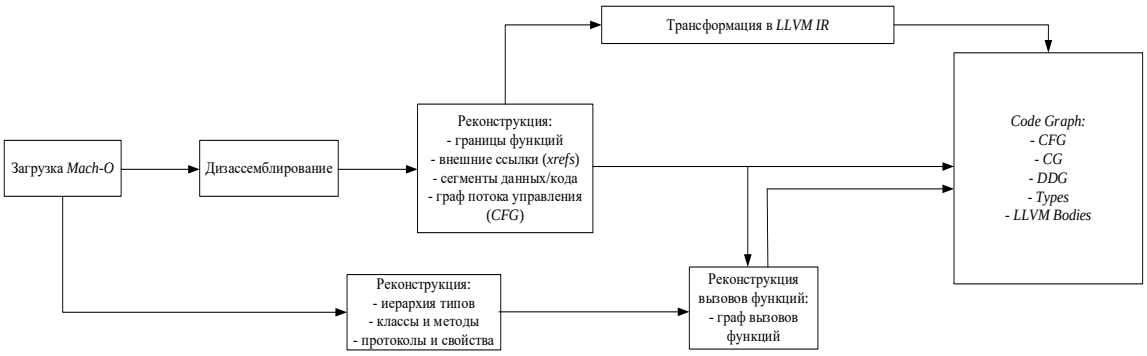


Рисунок. Процесс трансформации исполняемых файлов iOS

1. *Распаковка файла ".ipa" и загрузка исполняемого файла*. Процесс трансформации начинается с расшифрованного файла *".ipa"*, который либо напрямую экспортируется в виде архива из *XCode*, либо считывается с физического устройства. При установке из *Apple AppStore* разделы *Mach-O* зашифровываются с помощью открытого ключа, который присваивается учетной записи *Apple*, связанной с физическим устройством, соответствующий закрытый ключ которого управляется приложением *Secure Enclave TEE* на телефоне. Этот механизм является частью системы *Apple FairPlay DRM*, и способы его обхода известны с 2008 года. Поскольку расшифровка разделов уже выполняется загрузчиком двоичных файлов при сопоставлении разделов с сегментами памяти, достаточно просто загрузить приложение в память, выгрузить его сегменты открытым текстом и повторно собрать незашифрованный двоичный файл. Фактический процесс анализа начинается с извлечения двоичного файла *Mach-O* из файла *".ipa"*, сжатого в *zip*-формате, вместе с другими файлами, которые будут иметь отношение к анализу позже, такими как *"Info.plist"*. Двоичный файл *aarch64* извлекается из *fat Mach-O* и передается загрузчику, который анализирует команды загрузки двоичного файла для восстановления сегментов (*LC_SEGMENT*), таблиц символов (*LC_SYMTAB* и *LC_DYSYMTAB*) и границ функций (*LC_FUNCTION_ STARTS*). Обнаружение границ функций в двоичном двоичном двоичном объекте при отсутствии символов отладки является общеизвестно сложной проблемой, и современные дизассемблеры применяют эвристические подходы, такие как *BYTEWEIGHT* [4], *FID* или *FLIRT* [5], чтобы определить, где начинается функция

2. *Иерархии классов и селекторы*. Приложения для *iOS* написаны либо на *Swift*, либо на *Objective-C*, которые выполняются в двоичной среде выполнения *Objective-C*, но также могут включать библиотеки *C / C++* [6]. Таким образом, подмножество функций в вышеупомянутом списке функций

будет сопоставляться методам классов *Objective-C* или *Swift*, и восстановление этого сопоставления вместе с правильной иерархией классов имеет важное значение для создания чистого графика вызовов. Поскольку среда выполнения *Objective-C* нуждается в точной информации об иерархии классов для правильного разрешения вызовов методов, эта информация всегда должна содержаться в файле *Mach-O*, и мы можем извлечь ее из разделов файла.

Раздел *__objc_classlist* содержит список указателей на *class_t struct,* описывающий классы, содержащиеся в программе, по их суперклассу, метаклассу, размеру, протоколам, методам, переменным экземпляра и свойствам. Раздел *__objc_class ref*, напротив, содержит список структур класса *ref_t*, описывающих все классы, используемые программой во время выполнения.

Помимо классов, среда выполнения *Objective-C* поддерживает протоколы, которые не зависят от реализации и не зависят от класса определений методов и свойств. Знание протоколов, реализуемых приложением, помогает реверс-инженерам понять используемые *API* и функциональные возможности приложения. Информация о протоколе извлекается из соответствующих разделов *Mach-O* и включает ее в иерархию типов.

3. *Дизассемблирование*. Параллельно с извлечением иерархии типов начинается дизассемблирование двоичного файла, начиная с каждой границы функции, затем дизассемблированные функции трансформируются в графовое представление, которое может быть дополнительно обработано. Помимо определения границ сегмента и восстановления фактических инструкций и базовых блоков, включается отслеживание перекрестных ссылок, например, для разрешения локальных переменных и констант.

4. *Реконструкция графа вызовов*. Восстановление правильного графа вызовов является необходимым условием для любого точного межпроцедурного анализа. К сожалению, *Objective-C* имеет некоторые особенности, которые затрудняют реконструкцию графа вызовов. Будучи одним из первых объектно-ориентированных языков, поддерживающих динамическую привязку и диспетчеризацию на основе сообщений, в *Objective-C* нет такого понятия, как прямой вызов метода. Вызывающий объект создает только сообщение с указанием получателя, селектора и необязательных аргументов. Это сообщение передается диспетчеру *objc_msgSend* среды выполнения *Objective-C*, который отвечает за поиск получателя, поиск соответствующей реализации метода, соответствующей получателю, и выполнение вызова. Точное создание графа вызовов требует восстановления возможных значений аргумента приемника и селектора для всех вызовов *objc_msgSend*. Поскольку эти аргументы могут быть динамически заданы во время выполнения, возможно, даже с помощью предоставленных пользователем входных

значений, обычно их восстановление с помощью статического анализа невозможно. Однако, на практике восстановление этих аргументов возможно с высокой вероятностью успеха [7], поскольку компилятор *Objective-C/Swift* создает селекторы-указатели на строковые константы и приемники-указатели либо на класс, либо на экземпляр объекта. Обычно они назначаются регистрам в той же функции, что и вызов *objc_msgSend*, однако не обязательно рядом с вызовом и не всегда создаются одинаково. Таким образом, как только приемник и селектор были восстановлены, вышеупомянутая иерархия классов просматривается для получения адреса фактической реализации метода, и ребро от вызывающего абонента к этому адресу вставляется в граф вызовов.

5. *Представление трансформированных исполняемых файлов в суперграфе*. Информация, полученная в процессе обратного проектирования, должна быть объединена в единое представление, служащее для анализа. Традиционные платформы анализа программ используют фиксированные структуры данных с сильными зависимостями, которые нелегко расширить и которые охватывают только один уровень абстракции (например, ассемблер, объектно-ориентированные конструкции или проблемы на уровне синтаксического языка). Для большинства случаев использования статического анализа исходного кода это не является препятствием. Однако для бинарного анализа нужно предположить, что отдельные результаты этапов обратного проектирования являются неполными, непоследовательными или даже отсутствуют.

Таким образом, отдельные результаты этапов обратного проектирования нужно объединить в расширяемое представление, которое позволяет проводить анализ неполной информации на разных уровнях абстракции, явно жертвуя полнотой и, в зависимости от анализа, также надежностью. Хотя читателю это может показаться недостатком, отмечается, что надежность и полнота - это две крайности, которые не могут быть достигнуты идеально одновременно. Для анализа реалистичных программ для пользователя гораздо важнее, чтобы инструмент вообще мог работать с программой, оставаясь при этом «настолько надежным и полным, насколько это возможно» [8, 9].

6. *Построение суперграфа*. Начальный граф строится на основе входных данных этапов обратного проектирования (фронтэндов), а затем расширяется дальнейшими проходами для построения суперграфа. Этот суперграф является основой для фактических модулей анализа, которые выполняют запросы исследования графа. Корень суперграфа – это узел *PROGRAM*, представляющий двоичный файл *Mach-O* приложения. Его свойства содержат такие значения, как права и содержимое из файла *“Info.plist”*. Узел *PROGRAM* имеет доступ ко всем функциям, реализованным и импортированным двоичным файлом. Импортированные внешние

функции имеют набор свойств *IS EXT* и адрес (*EA*), равный -1, в то время как функции, реализованные приложением, имеют тело своей функции, хранящееся в *LLVM IR*. Также фиксируются потоки данных, добавляя ребра, указывающие на каждое использование ячейки памяти или регистра, к инструкции, определяющей ее значение. Следовательно, эта базовая графовая модель отображает график потока управления (*CFG*), график вызовов (*CG*) и график зависимости данных (*DDG*) вместе с дополнительной информацией, такой как тела функций *LLVM IR* и метаданные приложения. Просто обрабатывая граф и не добавляя дополнительной информации, это представление позволяет построить дерево прямого доминирования (*FDT*) и график зависимости программы (*PDG*).

Таким образом, для преодоления неудачных и неполных результатов трансформации бинарных файлов в *LLVM IR*, не нужно полагаться на одно конкретное промежуточное представление, а использовать расширяемое представление на основе графа, которое заполняется из различных фронтэндов обратного проектирования. Это представление допускает недостающую информацию и позволяет проводить статический анализ в форме запросов обхода и исследования графа.

Список используемых источников

1. Egele, M., Kruegel, C., Kirda, E., Vigna, G., Egele, M., Kruegel, C., Kirda, E., Vigna, G., "PiOS: Detecting Privacy Leaks in iOS Applications", 2011.

2. Deshotels, L., Deaconescu, R., Chiroiu, M., Davi, L., Enck, W., Sadeghi, A.R. "SandScout. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security – CCS", 2016.

3. Wang, T., Lu, K., Lu, L., Chung, S.P., Lee, W., "Jekyll on ios: When benign apps become evil", 2013.

4. Bao, T., Burket, J., Woo, M., Turner, R., Brumley, D., "Byteweight: Learning to recognize functions in binary code", 2015.

5. Hexrays, "IDA F.L.I.R.T. Technology: In-Depth", 2015.

6. Feichtner, J., Missmann, D., Spreitzer, R., "Automated Binary analysis on iOS", Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks – WiSec, 2018.

7. Jakub Bˇreˇcka, "A decompiler for Objective-C", 2016.

8. Machiry, A., Spensky, C., Corina, J., Stephens, N., Kruegel, C., Vigna, G.., "DR. CHECKER: A soundy analysis for Linux kernel drivers", 2017.

9. Rawat, S., Mounier, L., Potet, M., "LiSTT: an investigation into unsound incompleteyet practical result yielding static taintflow analysis", 2014.

УДК 378.147
ГРНТИ 49.01.21; 50.45.29; 50.51.03

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЛЕКЦИОННОГО МАТЕРИАЛА НА ПРИМЕРЕ ГЕОИНФОРМАЦИОННЫХ ДИСЦИПЛИН

Н. Н. Громова[1], А. А. Нестеров[1], Ю. А. Степкина[2], А. В. Шестаков[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский государственный экономический университет

Дальнейшее развитие методологии переменной локации контента учебного материала представлено на примере цифровой трансформации лекционного материала геоинформационных дисциплин. Теоретические подходы базируются на авторской пространственной модели ядра трансформации в виде статических и динамических QR-кодов, а практические – на средствах доступа обучающихся к цифровым ресурсам.

учебные материалы, образовательный и дидактический контент, QR-коды.

Актуальность смещения контента лекционного материала посредством цифровой трансформации в доступные для обучающихся электронные (цифровые) ресурсы значительно возрастает в условиях динамически развивающихся информационных и телекоммуникационных технологий и экосистем, например, исследованных в [1].

Методологию цифровой трансформации информативности учебного материала в образовательной деятельности вуза в педагогической системе на примере печатного авторского учебного пособия [2] можно представить моделями смещения контента или моделями без смещения (рис. 1 и рис. 2).

Основными концептами педагогической системы являются: *Q* – преподаватель; *C* – студент (обучающийся); *F* – функциональные отношения через учебный материал (№ 1, № 3 и № 4 на рис. 1), включая ссылки на источники (№ 5 и № 6 на рис. 1) или дополнительный материал (№ 8 на рис. 2), в доступном информационном ресурсе. В модели смещения контента учебного материала дополнительный контент представляется по запросу обучаемого (№ 6 на рис. 2), который трансформируется ядром, научно обоснованным на основе системы знаний о технологиях и содержании (TPACK, Technology Pedagogical and Content Knowledge), посредством динамических или статических *QR*-кодов, как обращение (№ 7 на рис. 2) к заблаговременно выбранным преподавателем (№ 2 и № 3 на рис. 2) материалам (№ 8 на рис. 2) в доступных информационных ресурсах.

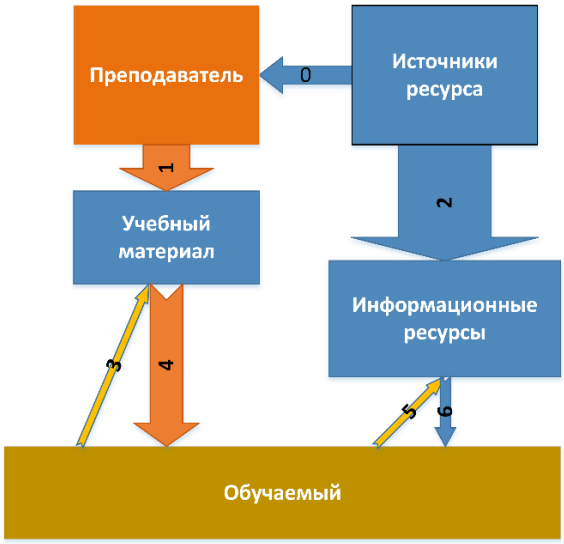


Рис. 1. Модель без смещения контента учебного материала

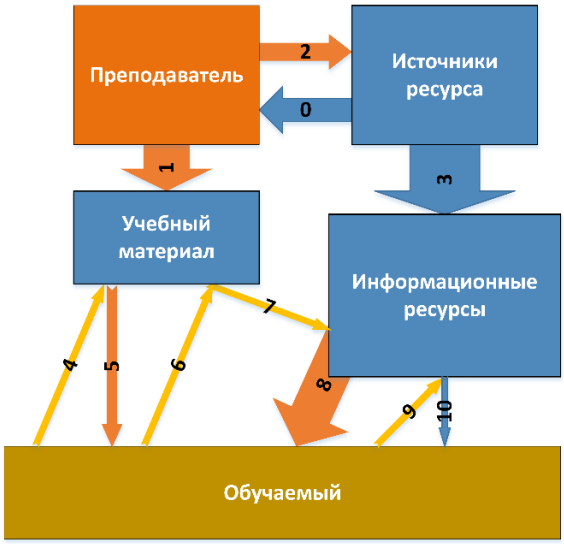
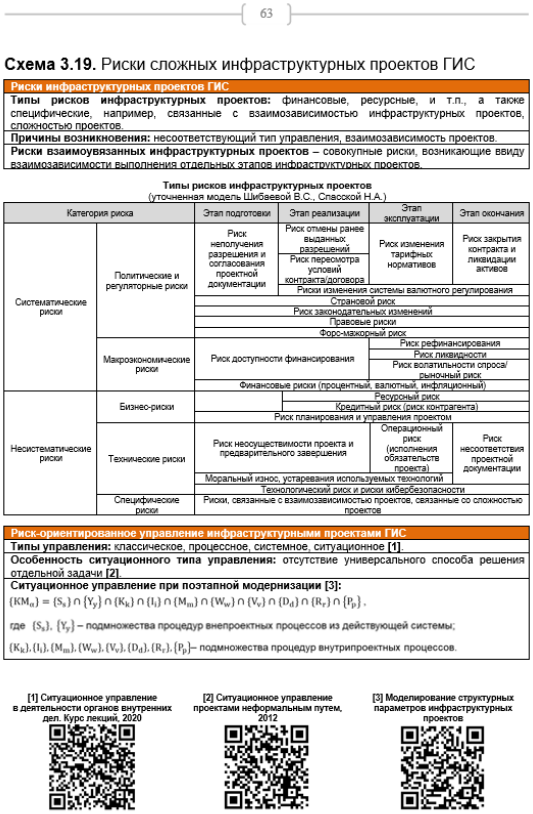


Рис. 2. Модель смещения контента учебного материала

Примеры трансформации контента учебного материала в электронные ресурсы из [2] представлены на рис. 3 и рис. 4.



63

Схема 3.19. Риски сложных инфраструктурных проектов ГИС

Риски инфраструктурных проектов ГИС

Типы рисков инфраструктурных проектов: финансовые, ресурсные, и т.п., а также специфические, например, связанные с взаимозависимостью инфраструктурных проектов, сложностью проектов.

Причины возникновения: несоответствующий тип управления, взаимозависимость проектов.

Риски взаимоувязанных инфраструктурных проектов – совокупные риски, возникающие ввиду взаимозависимости выполнения отдельных этапов инфраструктурных проектов.

Типы рисков инфраструктурных проектов
(уточненная модель Шибаевой В.С., Спасской Н.А.)

Категория риска		Этап подготовки	Этап реализации	Этап эксплуатации	Этап окончания
Систематические риски	Политические и регуляторные риски	Риск неполучения разрешения и согласования проектной документации	Риск отмены ранее выданных разрешений	Риск изменения тарифных нормативов	Риск закрытия контракта и ликвидации активов
			Риск пересмотра условий контракта/договора		
			Риски изменения системы валютного регулирования		
			Страновой риск		
			Риск законодательных изменений		
			Правовые риски		
			Форс-мажорный риск		
	Макроэкономические риски	Риск доступности финансирования		Риск рефинансирования	
				Риск ликвидности	
				Риск волатильности спроса/ рыночный риск	
		Финансовые риски (процентный, валютный, инфляционный)			
Несистематические риски	Бизнес-риски		Ресурсный риск		
			Кредитный риск (риск контрагента)		
		Риск планирования и управления проектом			
	Технические риски	Риск несоответствия проекта и предварительного завершения		Операционный риск (исполнения обязательств проекта)	Риск несоответствия проектной документации
		Моральный износ, устаревания используемых технологий			
		Технологический риск и риски кибербезопасности			
	Специфические риски	Риски, связанные с взаимозависимостью проектов, связанные со сложностью проектов			

Риск-ориентированное управление инфраструктурными проектами ГИС

Типы управления: классическое, процессное, системное, ситуационное **[1]**.

Особенность ситуационного типа управления: отсутствие универсального способа решения отдельной задачи **[2]**.

Ситуационное управление при поэтапной модернизации [3]:

$\{KM_0\} = \{S_x\} \cap \{Y_y\} \cap \{K_k\} \cap \{I_i\} \cap \{M_m\} \cap \{W_w\} \cap \{V_v\} \cap \{D_d\} \cap \{R_r\} \cap \{P_p\}$,

где $\{S_x\}$, $\{Y_y\}$ – подмножества процедур внепроектных процессов из действующей системы;

$\{K_k\}$, $\{I_i\}$, $\{M_m\}$, $\{W_w\}$, $\{V_v\}$, $\{D_d\}$, $\{R_r\}$, $\{P_p\}$– подмножества процедур внутрипроектных процессов.

[1] Ситуационное управление в деятельности органов внутренних дел. Курс лекций, 2020

[2] Ситуационное управление проектами неформальным путем, 2012

[3] Моделирование структурных параметров инфраструктурных проектов

Рис. 3. Трансформация контента в электронные источники литературы (пример)

98

Схема 5.17. Статистическая отчетность: Форма № 4-ОС

Форма № 4-ОС «Сведения о текущих затратах на охрану окружающей среды»

Годовая форма статистического наблюдения № 4-ОС «Сведения о текущих затратах на охрану окружающей среды» утверждена для отчета за 2021 год (Приказ Росстата от 28.07.2021 № 451) **[1]**.

Первичные статистические данные по формам федерального статистического наблюдения предоставляются в соответствии с указаниями по их заполнению по адресам, в сроки и с периодичностью, которые указаны на бланках этих форм **[1]**.

Предоставляют юридические лица, физические лица, занимающиеся предпринимательской деятельностью без образования юридического лица (индивидуальные предприниматели), осуществляющие природоохранную деятельность (полный перечень респондентов приведен в указаниях по заполнению формы федерального статистического наблюдения): территориальному органу Росстата в субъекте Российской Федерации по установленному им адресу **[1]**.

Наименование направлений природоохранной деятельности:
– охрана атмосферного воздуха и предотвращение изменения климата;
– сбор и очистка сточных вод;
– обращение с отходами;
– защита и реабилитация земель, поверхностных и подземных вод;
– защита окружающей среды от шумового, вибрационного и др. видов физического воздействия;
– обеспечение радиационной безопасности окружающей среды;
– сохранение биоразнообразия и охрана природных территорий;
– научно-исследовательская деятельность и разработка по снижению негативных антропогенных воздействий на окружающую среду;
– другие направления деятельности в сфере охраны окружающей среды **[1]**.

Не отражаются в форме № 4-ОС затраты на проведение мероприятий:
– по охране здоровья, улучшению условий труда и повышению техники безопасности, реализованные по техническим соображениям, но дающие положительный экологический эффект;
– по непосредственному использованию природных ресурсов (например, водоснабжение; мониторинг загрязнения питьевой воды; платежи за водопользование по договорам);
– по предотвращению или борьбе с последствиями стихийных бедствий и природных катастроф.

Не включаются текущие затраты
– по прогнозу (профилактике) и устранению последствий засухи, заморозков, землетрясений, лавин, оползней;
– строительству, модернизации и реконструкции объектов по охране окружающей среды;
– затраты на мероприятия, осуществляемые главным образом в целях удешевления используемых видов топлива, сырья и материалов, общего снижения издержек производства или по оказанию соответствующих услуг, повышения качества выпускаемой продукции, которые могут иметь также некоторый экологический эффект;
– приобретение основных фондов природоохранного назначения.

[1] Приказ Росстата от 28.07.2021 № 451 Текущие затраты на охрану окружающей среды форма № 4-ОС

[2] Федеральный закон № 7-ФЗ от 10.01.2002 Об охране окружающей среды

[3] Экологические услуги (пример)

Рис. 4. Трансформация контента в электронные ресурсы нормативных документов (пример)

Концепция регламентированного смещения образовательного и дидактического контента учебного материала в доверенные цифровые электронные ресурсы впервые была реализована в [2], а формальное ее описание впервые дано в [3] на множестве отношений (K) как:

$$K = <Q, C, F\{S, P \rightarrow T, W\}>, \quad (1)$$

где S, W, P, T – подмножество структурных компонент и контента учебного материала и информационных ресурсов, компонент TRACK и ядра трансформации соответственно.

Графическое представление модели цифровой трансформации контента учебного материала на множестве отношений (K) приведено на рис. 5, составляющие которой и их функциональные отношения детально описаны в [3].

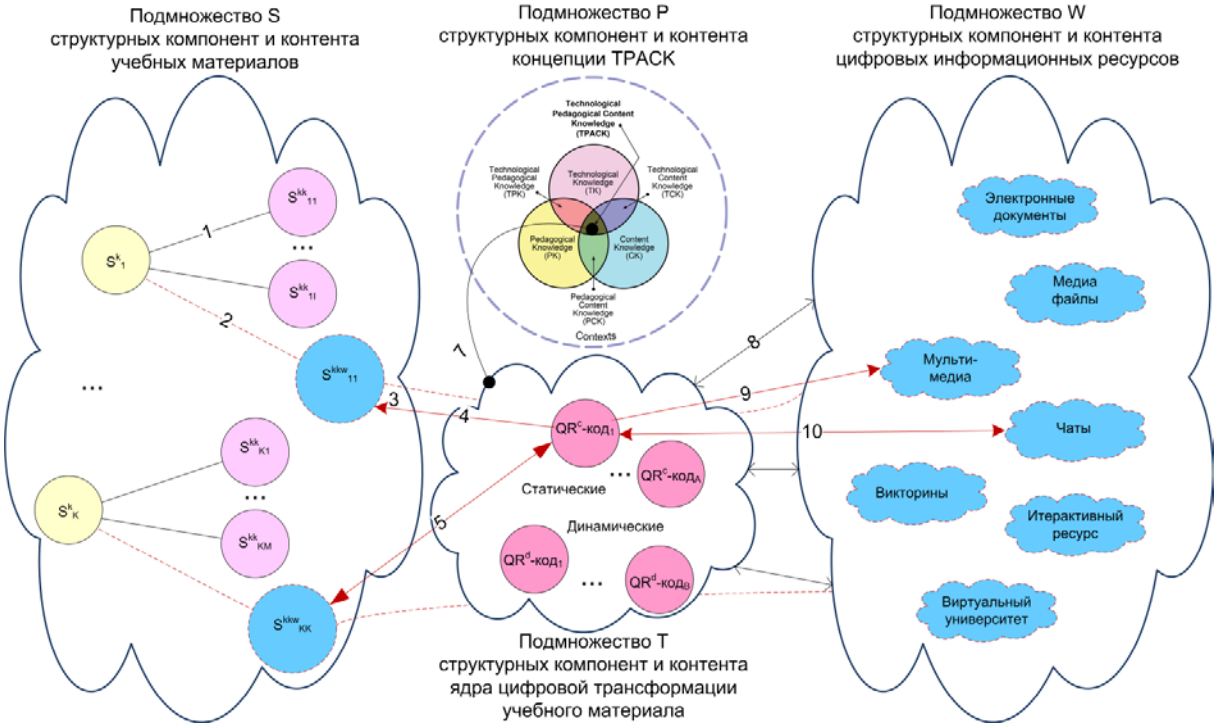


Рис. 5. Модель цифровой трансформации контента учебного материала

Относительно лекционной формы проведения занятия, следует отметить различные формы ее реализации, используемые в современном образовании: очная форма, дистанционная форма, при которой лектор общается со студентами, используя открытые и доступные платформы (например, Moodle, Zoom, Coursera, Open edX, Google meet и др.), а также смешанная форма организации лекционного занятия, при которой лектор и часть студентов находятся в учебной аудитории, а остальная часть подключается к лекции через указанные выше платформы.

Основной особенностью подачи лекционного материала (рис. 6) в отличии от печатного (рис. 2) является дополнение речевого контента иллюстративным материалом (№ 5 и № 6 на рис. 6) и интерактивное взаимодействие обучающихся с преподавателем (№ 7 на рис. 6), а при использовании технологий цифровой трансформации контента учебного материала в цифровые информационные ресурсы - возможность обучающихся при помощи личных средств доступа (№ 8 и № 9 на рис. 6) получать по запросу дополнительный контент из доверенных информационных ресурсов (№ 10 на рис. 6) в различных формах визуализации, и одновременно участвовать в учебных мероприятиях иных итеративных форм обучения (№ 13 и № 14 на рис. 6) заранее подготовленных преподавателем (№ 2, № 4, №11, № 12 на рис. 6).

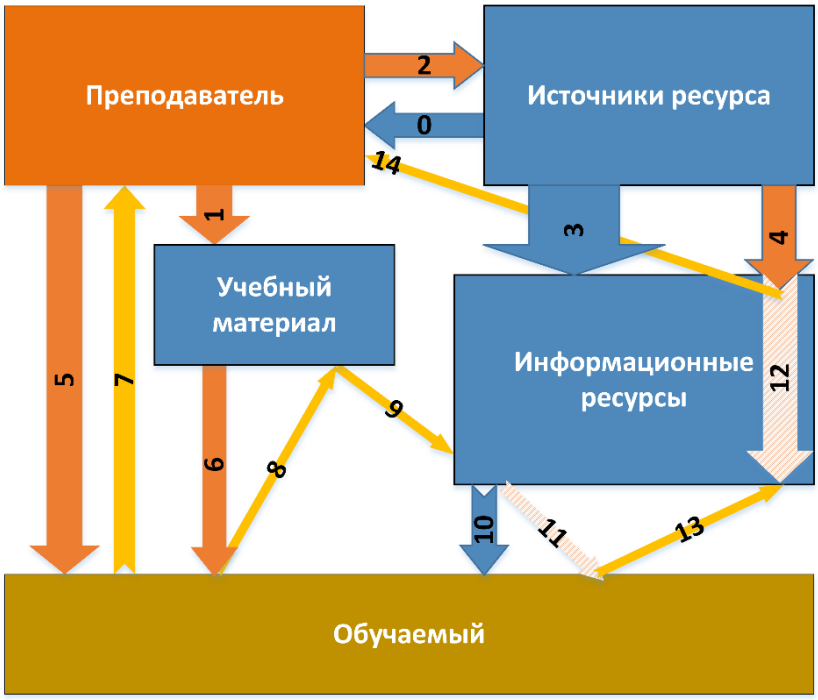


Рис. 6. Модель смещения контента лекционного материала

Характеристики структурного наполнения элементов пространственной модели цифровой трансформации контента учебного материала в зависимости от выбранной формы проведения лекционного занятия приведены в таблице 1.

ТАБЛИЦА 1. Характеристики контента лекционного материала

Элемент пространственной модели	Контент для различных форм организации лекционного занятия		
	Очная	Дистанционная	Смешанная
Подмножество структурных компонент и контента учебного материала (S)	– печатно-звуковой контент; – информационно-виртуальный контент; – коммуникация (взаимодействие в процессе обсуждения по заданной тематике)	– печатно-звуковой контент; – информационно-виртуальный контент требует наличия дополнительных девайсов у обучающихся; – коммуникация студентов возможна в создаваемых чатах, сессионных залах	–печатно-звуковой контент; –информационно-виртуальный контент требует наличия дополнительных девайсов у обучающихся; –коммуникация студентов в полном объеме невозможна
Подмножество TRACK (P)	Остается неизменным при реализации различных форм организации лекционного занятия		
Подмножество ядра цифровой трансформации учебного материала (T)	Остается неизменным (представлено компонентами QRc и QRd – статическими и динамическими QR-кодами)	Требует дополнения подмножества компонент гиперссылками	Требует дополнения подмножества компонент гиперссылками
Подмножество структурных компонент и контента существующих цифровых информационных ресурсов (W)	Медиа файлы Чаты Электронные документы Мультимедиа Интерактивный ресурс Виртуальный университет Викторины	Для перехода в информационные ресурсы требуются средства доступа обучающихся и дополнение подмножества компонент T гиперссылками	

Формат перевернутого обучения (flipped learning) предполагает самостоятельное изучение лекционного материала студентами с последующим его обсуждением на занятии [4]. Закрепление материала на лекции осуществляется посредством создания преподавателем условий для применения усвоенных знаний и выработки необходимых умений студентами. Компонентами подмножества W являются интерактивные тесты и опросники (Mentimeter, Kahoot, Onlinetestpad, Quizziz), ресурсы по созданию диаграмм и графиков (Chart Go, Diagrams.net, InVision Freehand), виртуальные доски (Conceptboard, Miro, Writeboard, Stormboard и др.).

Предлагаемая концепция цифровой трансформации информативности учебного материала может быть применена для лекционного материала, в том числе, для формата перевернутого обучения.

Результаты получены в прикладных научных исследованиях СПбГУТ по субсидии Минцифры России из госбюджета на финансовое обеспечение государственного задания на выполнение работ в 2022 году.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. Шестаков А. В., Фролова К. А., Плетнев Я. А. Геоинформационные системы в управлении и мониторинге техногенных объектов. Схемы и QR-ссылки: учебное пособие. СПб: Любавич, 2021. 100 с. ISBN 978-5-907440-62-3.

3. Шестаков А. В., Громова Н. Н., Степкина Ю. А. Цифровая трансформация информативности учебного материала для образовательной деятельности вуза // Международный научный журнал. 2021. № 5.

4. Bergmann J., Sams A. Flipped Learning: Gateway to Student Engagement. International Society For Technology In Education: Eugene, Oregon and Washington, DC, 2014. 169 pp. ISBN 978-1-56484-344-9.

УДК 004.891.2
ГРНТИ 20.23.17

ВЫБОР МЕТРИКИ ДЛЯ КЛАСТЕРИЗАЦИИ КАТЕГОРИАЛЬНЫХ ДАННЫХ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В реальных (да и в научных задачах) возникает необходимость в кластеризации данных смешанного типа – например, когда одна половина данных – числовые, а вторая половина – категориальные. По отдельности данные задачи решаются стандартными способами, однако решение задачи кластеризации смешанных данных представляет некоторые трудности, связанные в основном со сложностью расчета величины расстояния между наблюдениями. В работе исследуются вопросы оптимального выбора метрики для решения задачи кластеризации многомерных векторов. Особое внимание уделено наличию категориальных компонент. Исследования основаны на анализе существующих подходов, таких как использование в качестве метрики расстояния Гауэра и их программных реализаций.

алгоритмы машинного обучения, кластеризация, сходство/различие векторов, расстояние Гауэра.

Алгоритмы кластеризации предназначены для идентификации групп схожих векторов и традиционный акцент делается на числовых данных. Как следствие, многие существующие алгоритмы посвящены этому типу данных, хотя комбинация числовых и категориальных данных более распространена в большинстве практических прикладных задач.

Кластеризацию категориальных данных можно отнести к задачам, которые не имеют однозначного решения. Главный вопрос здесь состоит в том, как оцифровывать категории. Существующие подходы основаны на использовании матрицы несходства (*dissimilarity*), которая строится с использованием расстояния между векторами [1–4]. Эта матрица определяет насколько далеко друг от друга находятся разные точки в наборе данных. Очевидно, использование различных метрик и способов численного представления категориальных данных существенно влияет на результат. Расстояние Гауэра имеет тенденцию отдавать предпочтение наблюдениям, которые в большей степени совпадают по категориальным компонентам, меньше заботясь о расстояниях между вещественными компонентами векторов.

Несбалансированный вклад различных типов переменных еще больше усугубляется, когда количество категориальных переменных увеличивается. Это поведение можно изменить только путем принятия адекватной схемы взвешивания, однако выбор веса останется в высшей степени субъективным и совсем непростым в случае нескольких переменных смешанного типа.

Классический подход [3], предложенный для вычисления расстояния между векторами смешанного типа использует выражение:

$$d(x_i, x_j) = \sum_{m=1}^{q}(x_i^m - x_j^m)^2 + \lambda \sum_{m=q+1}^{p} \delta(x_i^m, x_j^m),$$

где m – индекс по всем переменным в наборе данных от 1 до p, из них первые q переменных являются числовыми, а остальные (p-q) переменных являются категориальными. Отметим, что $\delta(a, b) = 0$ для $a = b$ и $\delta(a, b) = 1$ для $a \neq b$, а $d()$ – соответствует взвешенной сумме евклидова расстояния между двумя точками в метрическом пространстве и простому расстоянию сопоставления для категориальных переменных (то есть подсчету несовпадений). Параметр λ позволяет управлять компромиссом между влиянием числовых и категориальных переменных. Для больших значений λ влияние категориальных переменных увеличивается.

Рассмотрим векторы из одних категориальных переменных. Примем некоторый базовый вектор x_0, у которого все компоненты равны нулю, за

начало отсчета. Расстояние между категориальными переменными оценивается по бинарному признаку их совпадения или несовпадения. Тогда расстояние любого вектора x от базового будет равно числу его ненулевых компонент. В этой ситуации расстояния двух векторов x_a и x_b, у которых не совпадает одинаковое количество категориальных переменных, от базового вектора будут равны $\boldsymbol{d}(\boldsymbol{x_0}, \boldsymbol{x_a}) = \boldsymbol{d}(\boldsymbol{x_0}, \boldsymbol{x_b})$.

Важно подчеркнуть, что это равенство справедливо независимо от того какие именно компоненты не совпадают. Точно также расстояние между двумя произвольными векторами будет одинаково, если и только если у них не совпадает одинаковое число компонент вне зависимости от их индекса.

Возьмем в качестве поясняющего примера результаты опроса респондентов о качестве товара, в результате которого были получены следующие категории ответов: *good*, *bad*, *usual*, *terrible*, *middling* и *beautiful*. Очевидно, что подобные категории допускают естественное ранжирование, например от *beautiful – good – usual – middling – bad – terrible* или в противоположную сторону, с последующей индексацией рангов. Для приведенного примера можно заметить, что уровень *usual* и *middling* вряд ли существенно отличаются, поэтому для них целесообразно использовать один индекс.

Таким образом, для приведенного примера логично проиндексировать категории, например, так: (1) *beautiful* – (2) *good* – (3) *usual* – (3) *middling* – (4) *bad* – (5) *terrible*.

Очевидно, порядок продвижения от *beautiful* к *terrible* или наоборот, для кластеризации особого значения не имеет. Для балансировки вклада количественных и категориальных переменных, а также различного числа уровней ранжирования естественным продолжением процедуры подготовки исследуемых данных будет их нормализация. Классический вариант заключается в масштабировании таким образом, чтобы среднее значение равнялось нулю, а стандартное отклонение равнялось единице. Таким образом, m-ая компонента вектора принимает значение:

$$\boldsymbol{x^m} \rightarrow \frac{\boldsymbol{x^m} - \sum_{i=1}^{N} \boldsymbol{x^i}/\boldsymbol{N}}{\boldsymbol{x^m_{max}} - \boldsymbol{x^m_{min}}},$$

где N – общее число рангов (индексов). В таблице 1 приведены масштабированные значения компонент, рассчитанные для $N = 5$.

ТАБЛИЦА 1. Масштабированные значения компонент

Ранги	(1) *beautiful*	(2) *good*	(3) *usual*	(3) *middling*	(4) *bad*	(5) *terrible*
Значения	-0.466666	-0.266666	-0.066666	-0.066666	0.133333	0.333333

Практически, после ранжирования, вычисление расстояния между всеми ранжированными категориями можно осуществлять также, как и для числовых данных:

$$\boldsymbol{d(x_i, x_j) = \sum_{m=1}^{p}(x_i^m - x_j^m)^2},$$

Покажем целесообразность использования предложенного подхода на простом примере. Сформируем вектор *grade* из 1000 результатов опроса с указанными вероятностями: *grade = sample*(*c*('*good*', '*bad*', '*terrible*', '*middling*', '*beautiful*'), 1000, *replace = T, prob = c*(0.4, 0.3, 0.2, 0.05, 0.05)). Из всего многообразия библиотек кластеризации возьмем библиотеки *cluster* и *fpc* [7, 8]. С помощью функции *daisy*() вычислим матрицу несходства Гауэра для вектора *grade* и разобьем его на три кластера на основе этой матрицы. Результат такого разбиения представлен в третьем столбце таблицы 2.

ТАБЛИЦА 2. Результаты разбиения

Характеристика	Неупорядоченное ранжирование		Упорядоченное ранжирование	
cluster.number	2.00	3.00	2.00	3.00
n	1000.00	1000.00	1000.00	1000.00
within.cluster.ss	0.42	0.25	0.67	0.33
average.within	0.06	0.04	0.08	0.05
average.between	0.32	0.30	0.31	0.30
wb.ratio	0.18	0.13	0.27	0.18
*dunn*2	3.74	2.19	2.84	2.98
Cluster-1 size	700.00	410.00	550.00	500.00
Cluster-2 size	300.00	300.00	450.00	450.00
Cluster-3 size	0.00	290.00	0.00	50.00

Проиндексируем вектор *grade* в соответствии с таблицей 1 и с помощью функции *cluster* разобьем его на три кластера. Результат такого разбиения представлен в последнем столбце таблицы 2.

Поясним полученные результаты. В сформированном векторе *grade* категориальные данные распределились следующим образом: *good* – 410, *bad* – 210, *middling* – 50, *terrible* – 290 и *beautiful* – 40. В первом случае три кластера включают следующие категории: *Cluster*-1 (*good*), *Cluster*-2 (*bad, middling, beautiful*) и *Cluster*-3 (*terrible*). Во втором случае, при использовании упорядоченного ранжирование, разбиение категорий следующее: *Cluster* -1 (*bad, terrible*), *Cluster*-2 (*beautiful, good*) и *Cluster*-3 (*middling*). Таким образом, упорядоченное ранжирование позволяет обеспечить объединение

в одном кластере близких не только по расстоянию, но и по смыслу категорий.

Список используемых источников

1. Gower J. C., Legendre P. Metric and Euclidean properties of dissimilarity coefficients // Journal of Classification, 1986. № 3. pp. 5–48.

2. Gower J. C. A general coefficient of similarity and some of its properties // Biometrics, 1971. № 27. pp. 623–637.

3. Huang Z. Extensions to the k-Means Algorithm for Clustering Large Data Sets with Categorical Values // Data Mining and Knowledge Discovery. 1998. № 2. pp. 283–304.

4. D'Orazio M. Distances with mixed type variables some modified Gower's coefficients. URL: https://arxiv.org/abs/2101.02481 (дата обращения: 30.01.2022).

5. Budiaji W. kmed: Distance-Based K-Medoids. URL: https: // cran.r-project.org/web/packages/ kmed/vignettes/kmedoid.html (дата обращения: 30.01.2022).

6. Szepannek G. clustMixType: User-Friendly Clustering of Mixed-Type Data in R // The R Journal, 2018. № 10/2. pp. 200–208.

7. Package 'cluster'. URL: https://cran.r-project.org/web/packages/cluster/cluster.pdf (дата обращения: 30.01.2022).

8. Package 'fpc'. URL: https://cran.r-project.org/web/packages/fpc/fpc.pdf (дата обращения: 30.01.2022).

УДК 004.8
ГРНТИ 81.81.07

ИСПОЛЬЗОВАНИЕ ЧАСТИЧНОГО РЕЗЕРВИРОВАНИЯ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБУЕМЫХ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При анализе параметров системной надёжности учитывается структура системы, состав и взаимодействие входящих в неё элементов, возможность перестройки структуры и алгоритмов её функционирования при отказах отдельных элементов. В работе рассматриваются вопросы оценки количества нерезервируемых элементов системы, позволяющие получить требуемые значения показателей надежности путем резервирования оставшейся части системы. Приводится оценка выигрыша по количеству элементов по сравнению с использованием традиционных методов резервирования.

надежность, безотказность, показатели надежности, система, резервирование.

Одной из важнейших проблем при проектировании, производстве и эксплуатации информационных систем (ИС) является проблема обеспечения надежности. Надёжность ИС определяется надёжностью её элементов, надёжностью программного обеспечения, а также использованием средств контроля и восстановления системы.

Одним из наиболее эффективных средств обеспечения требуемого уровня надежности ИС является структурное резервирование элементов системы [1]. Однако условия эксплуатации современных систем часто не позволяют полностью резервировать элементы системы вследствие наличия жестких ограничений по весу и габаритам в подвижных частях объектов.

В связи с этим, возникает необходимость рассмотреть возможность резервирования лишь части элементов системы, обеспечив при этом требуемые значения показателей надежности для всей системы.

Рассмотрим метод повышения надежности системы за счет использования дополнительных элементов, избыточных по отношению к минимально необходимому количеству элементов, для выполнения требуемых функций с целью сохранения работоспособного состояния системы при отказе одного или нескольких элементов, причем резервированию подвергаются не все элементы системы, а лишь их определенная часть.

При решении задачи используется постоянно подключенный резерв и общее резервирование части ИС. Вероятность безотказной работы системы подчиняется экспоненциальному закону распределения, система невосстанавливаемая, интенсивность отказов для каждого элемента λ и общее количество элементов системы n – заданы.

Требуется обеспечить вероятность безотказной работы системы Pс $\geq P_{\text{треб}}$.

Представим ИС в виде последовательно соединения двух частей системы. Одна из частей будет резервироваться, вторая часть системы останется без изменений (рис. 1).

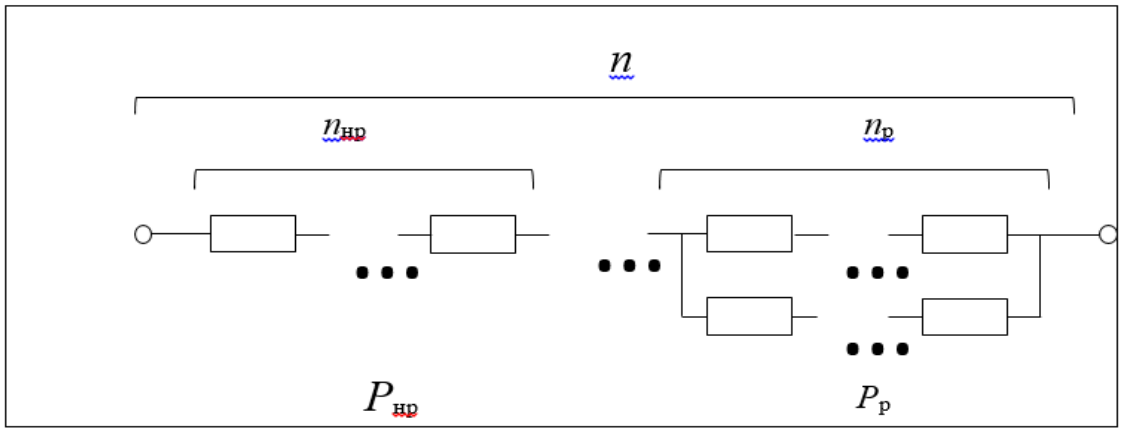


Рис. 1. Структура системы при частичном резервировании

В этом случае вероятность безотказной работы системы можно представить в виде следующего выражения [2]:

$$P_{\text{с}}(t) = P_{\text{нр}}(t) \cdot P_{\text{р}}(t),$$

откуда можно определить вероятность безотказной работы зарезервированной части ИС:

$$P_{\text{р}}(t) = \frac{P_{\text{с}}(t)}{P_{\text{нр}}(t)}.$$

Следовательно, для нерезервированной части системы должно выполняться следующее неравенство:

$$P_{\text{нр}}(t) > P_{\text{с}}(t) \geq P_{\text{треб,}} \text{ и } P_{\text{нр}}(t) = e^{-n_{\text{нр}} \cdot \lambda \cdot t} > P_{\text{треб}}.$$

Последнее выражение позволяет определить требования к количеству элементов нерезервированной части системы.

Количество элементов в этой части системы определяется выражением:

$$n_{\text{нр}} < \frac{-\ln(P_{\text{треб}})}{\lambda \cdot t}.$$

Если определить $n_{\text{нр1}} < n_{\text{нр}}$, то вероятность безотказной работы данной части системы составит

$$P_{\text{нр1}}(t) = e^{-n_{\text{нр1}} \lambda t}.$$

Вероятность безотказной работы зарезервированной части системы должна составить

$$P_{\text{зр1}}(t) = \frac{P_{\text{треб}}}{P_{\text{нр1}}(t)} = \frac{P_{\text{треб}}}{e^{-n_{\text{нр1}} \lambda t}}.$$

Вероятность безотказной работы резервируемой части системы до ее резервирования составляет

$$P_{\text{р1}}(\text{t}) = e^{-(n - n_{\text{нр1}}) \lambda t}.$$

Определим кратность резервирования данной части системы исходя из условия [3]

$$P_{\text{зр1}}(t) = 1 - \left(1 - P_{\text{р1}}(t)\right)^{m+1},$$

следовательно

$$m = \frac{\ln(1 - P_{\text{зр1}}(t))}{\ln(1 - P_{\text{р1}}(t))} - 1 = \frac{\ln(1 - \frac{P_{\text{треб}}}{e^{-n_{\text{нр1}}\lambda t}})}{\ln(1 - e^{-(n-n_{\text{нр1}})\lambda t})} - 1.$$

Полученный результат необходимо округлить до ближайшего большего целого числа.

Пример. Рассмотрим решение задачи со следующим вариантом исходных данных: n = 1035; $\lambda = 1{,}1 \cdot 10^{-6}$ 1/ч; t = 250 ч; $P_{\text{треб}}(t) = 0{,}97$.

$$P_{\text{р}}(250) = \frac{P_{\text{треб}}(250)}{P_{\text{нр}}(250)} = \frac{0{,}97}{P_{\text{нр}}(250)} \text{ и } P_{\text{нр}}(250) > 0{,}97$$

$$P_{\text{нр}}(250) = e^{-n_{\text{нр}} \cdot \lambda \cdot 250} > 0{,}97.$$

Количество элементов в этой части системы определяется выражением

$$n_{\text{нр}} < \frac{-\ln(0{,}97)}{\lambda \cdot t} = \frac{0{,}030459}{1{,}1 \cdot 10^{-6} \cdot 250} = 110{,}7608.$$

Если определить $n_{\text{нр1}}$ = 50, то вероятность безотказной работы данной части системы составит

$$P_{\text{нр1}} = e^{-n_{\text{нр1}}\lambda t} = e^{-50 \cdot 1{,}1 \cdot 10^{-6} \cdot 250} = 0{,}986344.$$

Вероятность безотказной работы зарезервированной части системы должна составить

$$P_{\text{зр1}} = \frac{P_{\text{треб}}}{P_{\text{нр1}}} = \frac{0{,}97}{0{,}986344} = 0{,}98342962.$$

Вероятность безотказной работы резервируемой части системы до ее резервирования составляет

$$P_{\text{р1}} = e^{-(n-n_{\text{нр1}})\lambda t} = e^{-985 \cdot 1{,}1 \cdot 10^{-6} \cdot 250} = 0{,}762712.$$

Определим кратность резервирования данной части системы исходя из условия

$$P_{\text{зр1}} = 1 - (1 - P_{\text{р1}})^{m+1} = 0{,}98342962,$$

следовательно

$$m = \frac{\ln(1-P_{\text{зр1}})}{\ln(1-P_{\text{р1}})} - 1 = \frac{-4{,}293584}{-1{,}14385} - 1 = 1{,}98480596.$$

Для проверки полученного результата рассчитаем вероятность безотказной работы системы для выбранного варианта резервирования.

Вероятность безотказной работы резервируемой части системы после ее резервирования с кратностью $m = 2$ составит

$$P_{\text{зр1}} = 1 - (1 - P_{\text{р1}})^{2+1} = 1 - (1 - 0{,}762712)^3 1 - 0{,}013361 = 0{,}986639.$$

Для всей системы вероятность безотказной работы определяется следующим образом

$$P_{\text{с}} = P_{\text{нр1}} \cdot P_{\text{зр1}} = 0{,}986344 \cdot 0{,}986639 = 0{,}973166.$$

Таким образом, двукратное резервирование только части проектируемой системы позволяет удовлетворить поставленные требования по ее надежности.

Представляет интерес оценить величину выигрыша в количестве элементов системы при частичном резервировании элементов.

Решение рассматриваемой задачи обеспечения требуемого значения вероятности безотказной работы при резервировании всей системы позволяет определить общее количество элементов зарезервированной системы $n_{\text{ро}}$.

$$n_{\text{ро}} = n \cdot m_{\text{о}},$$

где $m_{\text{о}}$ – кратность резервирования системы, значение которой определяется как [1]:

$$m_{\text{о}} = \frac{\ln(1-P_{\text{треб}})}{\ln(1-P_{\text{с}})} - 1 = \frac{-3{,}50656}{-1{,}39552} - 1 = 1{,}512721 \approx 2,$$

$$P_{\text{с}} = e^{-\text{n}\lambda t} = e^{-1035 \cdot 1{,}1 \cdot 10^{-6} \cdot 250} = 0{,}752712.$$

Общее количество элементов системы составляет

$$n_{ро} = n\cdot(m_о+1_)=1035\cdot 3 = 3105.$$

При частичном резервировании общее количество элементов системы составляет

$$n_{рч} = n_{нр1}+n_р\cdot(m+1)=50+985\cdot 3 = 3005.$$

При этом, общее количество элементов ИС (с учетом резервных) оказывается на $\Delta n = 100$ элементов меньше, чем общее количество элементов ИС при общем резервировании системы на тех же условиях.

Рассмотрим поведение Δn (рис. 2) при изменении количества элементов не резервируемой части ИС в разрешенных пределах ($n_{нр} < 110$).

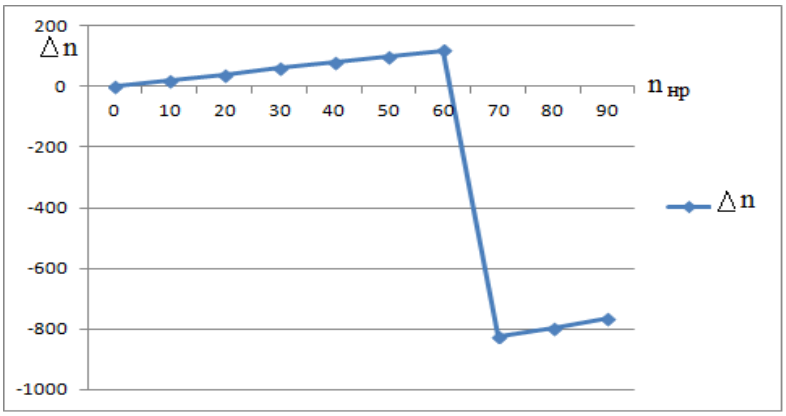


Рис. 2. Зависимость выигрыша в количестве элементов ИС при частичном резервировании системы

Очевидно, что Δn имеет разрыв при значении $n_{нр}$, где величина m изменяет свое значение с $m = 2$ на $m = 3$, а величину $n_{нр}$, обеспечивающую максимальный выигрыш по количеству используемых элементов системы, можно определить исходя из следующего уравнения

$$[1-\left(1-e^{-(n-n_{нр})\lambda t}\right)^{2+1}]\cdot e^{-n_{нр}\lambda t} = 0{,}97,$$

которое несложно решить графически (рис. 3).

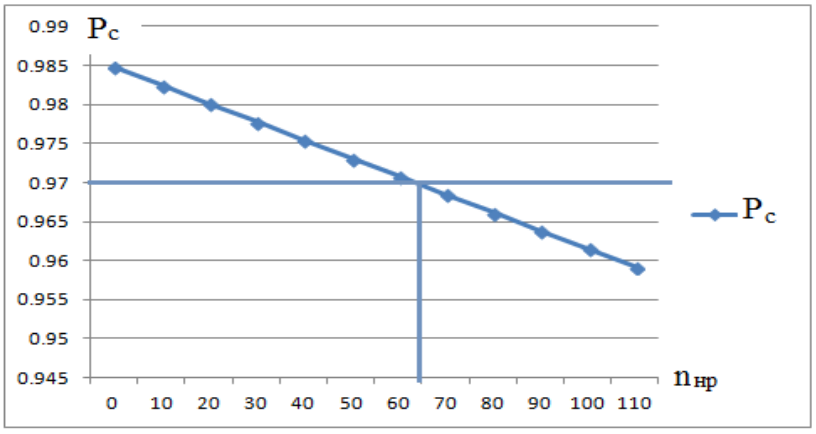


Рис. 3. Определение оптимального значения количества нерезевируемых элементов системы

Полученные результаты могут быть использованы при решении задач резервирования систем в условиях ограничения на габариты и массу используемых для построения систем элементов.

Список используемых источников

1. Острейковский В. А. Теория надежности: Учеб. для вузов. Москва: Высш. шк., 2003.

2. Половко А. М., Гуров С. В. Основы теории надежности. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2006.

3. Половко А. М., Маликов И. М., Жигарев А. Н., Зарудный В. И. Сборник задач по теории надежности. М.: Сов. радио, 1972.

УДК 004.891.2
ГРНТИ 82.05.21

СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ВЫБОРЕ СТРУКТУРИРОВАННЫХ ФИНАНСОВЫХ ПРОДУКТОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Принятие верного решения об инвестиции – это сложный процесс, включающий в себя несколько этапов: сбор информации; поиск и нахождение путей решения; выбор лучшей альтернативы. Современные достижения в области информационных технологий позволяют лицу, которое принимает решения, сократить временные и иные затраты на выбор лучшей альтернативы, а инвестору – выбрать лучшее из полученных

вариантов. В работе рассматривается интеллектуальная система поддержки принятия решений, которая создана специально для работы с такими сложными производными инструментами как опционы и помогает потенциальному инвестору выбрать лучший вариант из предложенного списка решений.

финансовый анализ, технический анализ, фундаментальный анализ, интеллектуальная система поддержки принятия решений.

Сложность структуры, недостаточно проработанная научная база, отсутствие эффективных моделей оценки и справедливого ценообразования – основные проблемы российского рынка структурированных финансовых продуктов. В этих условиях возникает необходимость в разработке системы поддержки принятия решения инвестора при выборе структурированных продуктов, которая анализирует входной список инструментов, моделирует динамику цен базовых активов, входящих в их состав, оценивает их стоимостные параметры, а также формирует рекомендации для лица, принимающего решения. Отсутствие такой системы негативно сказывается на спросе инвесторов к сложным финансовым инструментам.

Опцион – это право купить или продать базовый актив по определенной цене в будущем. Опцион – это гибкий производный инструмент, который дает дополнительные возможности для инвесторов, преследующих самые разные цели. Существует два вида опционов: опцион «колл», дающий право, но не обязательство произвести покупку определенного актива по фиксированной цене и опцион «пут», дающий право продажи определенного актива по фиксированной цене [1].

Для удобства формирования цепочки опционов для базового актива введено понятие «страйк». Оно представляет собой деление шкалы цены базового актива на определенные промежутки, которые, как правило, равны целым значениям или имеют цену деления 0.5 Нужно отметить, что такой принцип деления шкалы не является жестким правилом, так как существуют недорогие инструменты, «страйки» которых могут иметь более мелкую цену деления. В каждом случае спецификация инструмента сверяется на сайте биржи, где торгуется этот инструмент. На каждом «страйке» всегда торгуются оба вида опционов – «колл» и «пут», которые можно как купить, так и продать. В общем виде сделки с опционами представлены на рис. 1.

Для работы со сложными производными инструментами создана система поддержки принятия решения, приведенная на рис. 2. Она предназначена специально для работы с опционами и помогает потенциальному инвестору выбрать лучший вариант из предложенного списка. Основные цели такой системы [2]:

- первичный анализ и обработка исходных данных;
- оценка стоимостных параметров продукта;
- определение скрытых комиссий;

– помощь в выборе продукта с наилучшим прогнозом риска и доходности.

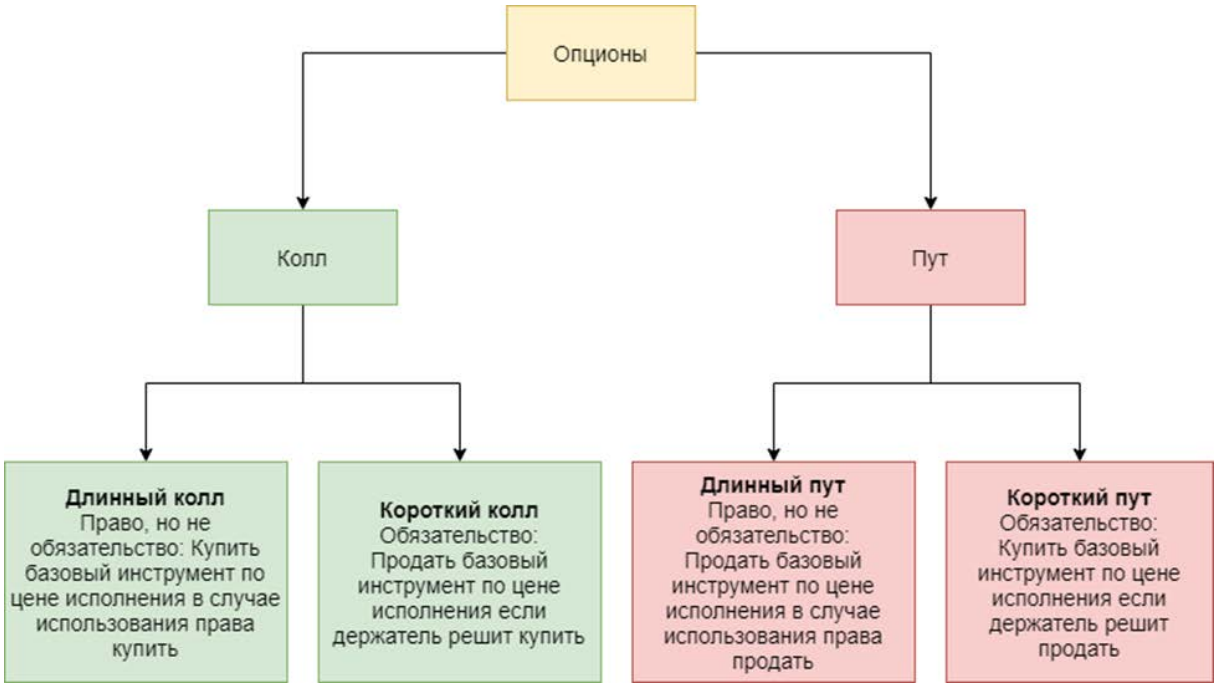


Рис. 1. Виды сделок с использованием опционов

На первом этапе представленной СППР происходит сбор и анализ входных данных, таких как:

– список продуктов, полученный от эмитента;

– рекомендации специалистов в области анализа финансовых инструментов;

– данные о поведении базовых активов (БА), которые лежат в основе производных инструментов;

– состояние финансового рынка в данный момент.

Исходные данные наполняют базу данных и знаний, которая уже содержит в себе мнения экспертов и рекомендации, а также исторические оценки СППР. В базе данных сохраняется всю полученная информация о текущих и уже подвергшихся анализу инструментах.

Рис. 2. Архитектура системы поддержки принятия решения при выборе структурированных финансовых продуктов

Программная система состоит из двух модулей: модуль расчета теоретических цен опционов и модуль прогнозирования поведения комплексной опционной стратегии и расчета общих параметров сделки.

Интерфейс модуля расчета теоретических цен изображен на рис. 3.

135,00	Underlying Price
16-Apr-21	Today's Date
30,00%	Historical Volatility
21-May-21	Expiry Date
0,30%	Risk Free Rate
0,00%	Dividend Yield
35	*DTE*
0,10	*DTE in Years*

		Call Options									Put Options								
		Theoretic	Market	Implied	Option Greeks							Theoret	Market	Implied	Option Greeks				
Strike Prices		Price	Price	Volatility	Delta	Gamma	Vega	Theta	Rho		Strike Prices	Price	Price	Volatility	Delta	Gamma	Vega	Theta	Rho
110,00	ITM	25,09	25,05	26,23%	0,99	0,0025	0,0131	-0,0065	0,1038		110,00	OTM	0,05	0,05	29,68%	-0,01	0,0025	0,0131	-0,0056	-0,0016
115,00	ITM	20,23	20,21	29,40%	0,96	0,0066	0,0345	-0,0157	0,1051		115,00	OTM	0,20	0,21	30,37%	-0,04	0,0066	0,0345	-0,0147	-0,0051
120,00	ITM	15,61	15,63	30,33%	0,91	0,0134	0,0700	-0,0309	0,1023		120,00	OTM	0,57	0,63	30,81%	-0,09	0,0134	0,0700	-0,0299	-0,0127
125,00	ITM	11,41	11,50	30,82%	0,81	0,0216	0,1134	-0,0494	0,0939		125,00	OTM	1,37	1,50	31,12%	-0,19	0,0216	0,1134	-0,0484	-0,0259
130,00	ITM	7,83	7,95	30,78%	0,68	0,0287	0,1503	-0,0651	0,0800		130,00	OTM	2,79	2,95	31,03%	-0,32	0,0287	0,1503	-0,0640	-0,0447
135,00	ATM	5,02	6,00	35,88%	0,52	0,0318	0,1666	-0,0719	0,0625		135,00	ATM	4,98	5,50	33,12%	-0,48	0,0318	0,1666	-0,0708	-0,0669
140,00	OTM	2,99	3,35	32,26%	0,37	0,0300	0,1573	-0,0678	0,0445		140,00	ITM	7,95	8,35	32,51%	-0,63	0,0300	0,1573	-0,0666	-0,0897
145,00	OTM	1,66	1,78	30,95%	0,24	0,0246	0,1287	-0,0554	0,0289		145,00	ITM	11,61	11,78	31,27%	-0,76	0,0246	0,1287	-0,0542	-0,1101
150,00	OTM	0,85	0,93	30,83%	0,14	0,0177	0,0926	-0,0398	0,0172		150,00	ITM	15,81	15,93	31,28%	-0,86	0,0177	0,0926	-0,0386	-0,1266
155,00	OTM	0,41	0,45	30,69%	0,08	0,0113	0,0593	-0,0255	0,0094		155,00	ITM	20,36	20,41	30,77%	-0,92	0,0113	0,0593	-0,0242	-0,1392
160,00	OTM	0,18	0,20	30,50%	0,04	0,0065	0,0342	-0,0147	0,0047		160,00	ITM	25,14	25,20	31,70%	-0,96	0,0065	0,0342	-0,0134	-0,1487

Рис. 3. Интерфейс модуля расчета теоретических цен опционов

Входные данные для заполнения первого модуля берутся из открытых источнков – как правило это сайты бирж, на которых торгуются инструменты. Входные данные, которые используются, как константы для уравнений – это последняя цена базового инструмента *S* (underlying price), цена исполнения «страйк» (strike price) – все расчеты производятся для каждого страйка, так как на каждом из них всегда торгуется пара опционов «колл» и «пут». Также необходимо ввести дату экспирации опциона – она нужна для вычисления времени жизни опциона в долях года, например, 25/365 = 0.07. Безрисковая процентная ставка (RiskFreeRate) также может быть получена на любом сайте зарубежных и отечественных бирж. Историческая волатильность вычисляется по модели Блэка-Шоузла [3] на основе исторических данных закрытия торгов для базового инструмента. Нужно отметить, что в формуле вычисления исторической волатильности задается окно времени (временного периода). Для инвестора это субъективный фактор, который может влиять на теоретическую стоимость опциона. Как правило, окно составляет 20 дней, но инвестор сам вправе менять этот период исходя из своих соображений.

Рис. 4. Индикация шкалы для опционов «колл»

Рис. 5. Индикация шкалы для опционов «пут»

Пользователю необходимо заполнить столбец цен исполнения (strike prices) на основе шага страйков для данного конкретного базового инструмента. Индикация шкалы ITM-ATM-OTM для опционов «колл» выглядит следующим образом (рис. 4).

Индикация шкалы ITM-ATM-OTM для опционов «пут» выглядит следующим образом (рис. 5).

Следующим шагом в работе программной модели является вычисление теоретических цен опционов «колл» и «пут». На рис. 6 отражен алгоритм вычисления теоретических цен опционов:

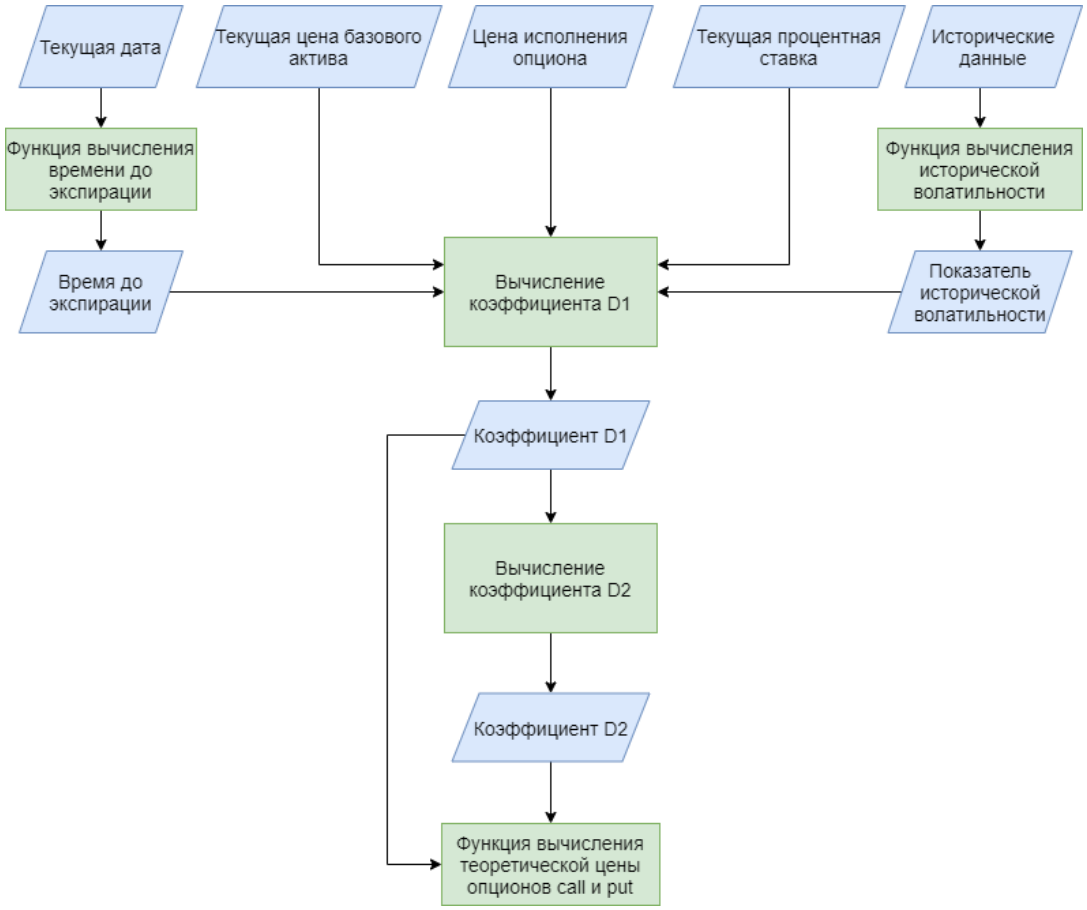


Рис. 6. Алгоритм вычисления теоретических цен опционов

Таким образом, на основании теории ценообразования опционов и рациональных действий лица, принимающего решения, возможно использование действующего прототипа системы поддержки принятия решений, основанной на математических алгоритмах ценообразования опционов, не требующей дорогостоящего внедрения технологий искусственного интеллекта и постоянного сопровождения базы знаний. Разработка позволит увеличить эффективность управления финансовыми продуктами в условиях рыночной экономики.

Список используемых источников

1. Натенберг, Шелдон. Опционы. Волатильность и оценка стоимости. Стратегии и методы опционной торговли. М.: Альпина паблишер, 2021. 539 с.

2. Что такое система поддержки принятия решений: виды, методы, возможности. URL: https://fisgroup.ru/blog/fis_dss_opisanye_systemy/ (дата обращения: 22.03.2022).

3. Математика опционов или модель Блэка-Шоулза. URL: https://habr.com/ru/post/552194/ (дата обращения: 22.03.2022).

УДК 004.891.2
ГРНТИ 20.53.19

ФОРМИРОВАНИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОДБОРА ПЕРСОНАЛА С ПРИМЕНЕНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А. А. Гунина, М. В. Котлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Определены ключевые задачи информационной системы подбора профессиональных кадров. Представлен спектр параметров, необходимых для решения задачи выбора соискателя. Определены основные элементы модели информационной системы, предусматривающей реализацию сценариев размещения вакансии со стороны организации, представления резюме со стороны соискателя и сопоставления требований работодателя со знаниями, умениями и компетенцией соискателя. Рассмотрены возможности применения методов искусственного интеллекта для решения задачи поиска профессиональных кадров. Представлена модель информационной системы.

соискатель, интеллектуальный подбор, облако параметров, модели, массив вакансий.

В условиях развития цифровой экономики, решение задачи подбора персонала не может достигаться без интеграции современных инфокоммуникационных технологий, включая методы искусственного интеллекта. Опыт проведения собеседований в условиях пандемии, а также текущий рост востребованности в профессиональных кадрах подводят к необходимости проектирования информационной системы, которая позволит подобрать наиболее подходящего сотрудника для решения поставленных задач. В настоящее время реализовано достаточно большое количество систем, позволяющих пользователю разместить резюме и просмотреть список актуальных вакансий, однако ни одна из существующих систем не учитывает личностные качества соискателя и не делает процесс подбора вакансий автоматизированным.

Новый подход к формированию перечня вакансий для соискателя строится не только на соответствии требованиям профессиональных стандартов и запросам компании, но и учитывает параметры скрытой мотивации, уровня гармонии и типа личности пользователя. Таким образом, главной задачей информационной системы становится интеллектуальный подбор соискателей, наиболее подходящих под требования компании, а со стороны пользователя, формируется актуальный массив вакансий.

В основе концепции интеллектуального подбора лежит спектр параметров, формирующийся на основе требований текущего нормативно-правового поля в области трудового права, расширенного анализа вакансий различных отраслей и изучения портфолио и резюме соискателей (рис. 1).

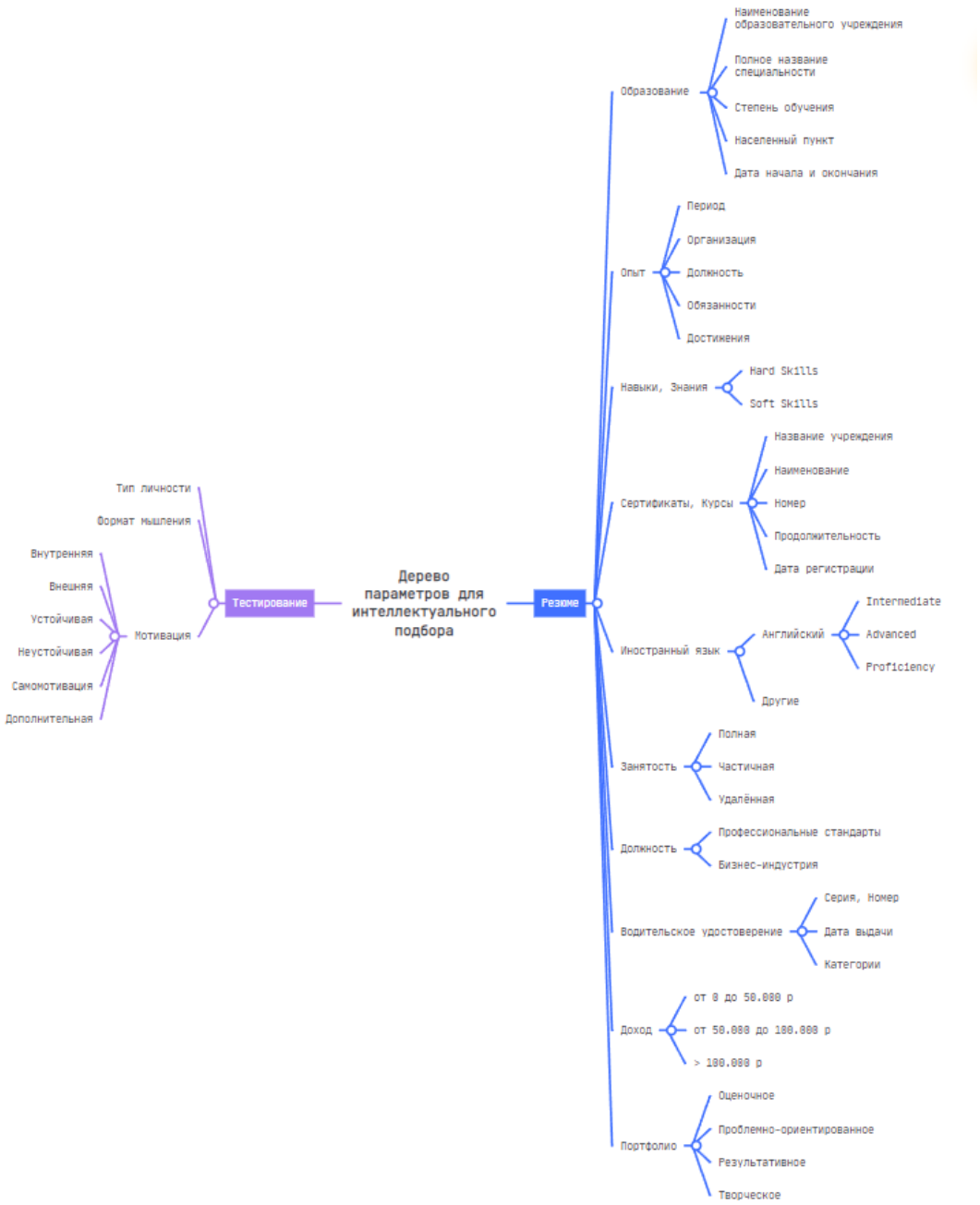


Рис. 1. Дерево параметров интеллектуального подбора персона

Облако параметров, на которых строится алгоритм подбора соискателей и вакансий демонстрирует вариативность исходных данных, таких как разнообразное портфолио, наличие нескольких базовых образований, возможность претендовать на несколько должностей в рамках различных междисциплинарных направлений и т. д. Данный аспект значительно усложняет

процедуру формирования массива вакансий для соискателя. Однако при формировании ряда моделей, определяющих концепцию принятия решения на основе исходных данных и запросов пользователя, а также интеграции подхода с применением технологии искусственного интеллекта позволит реализовать формирование требуемой выборки с элементом ранжирования результата. В основе каждой модели закладывается аналитико-онтологический подход, а выбор модели в каждом случае определяется системой (рис. 2)

Интеграция технологии искусственного интеллекта в процесс сравнения онтологический моделей соискателя и вакансий позволит обеспечить формирование релевантного массива вакансий для соискателя.

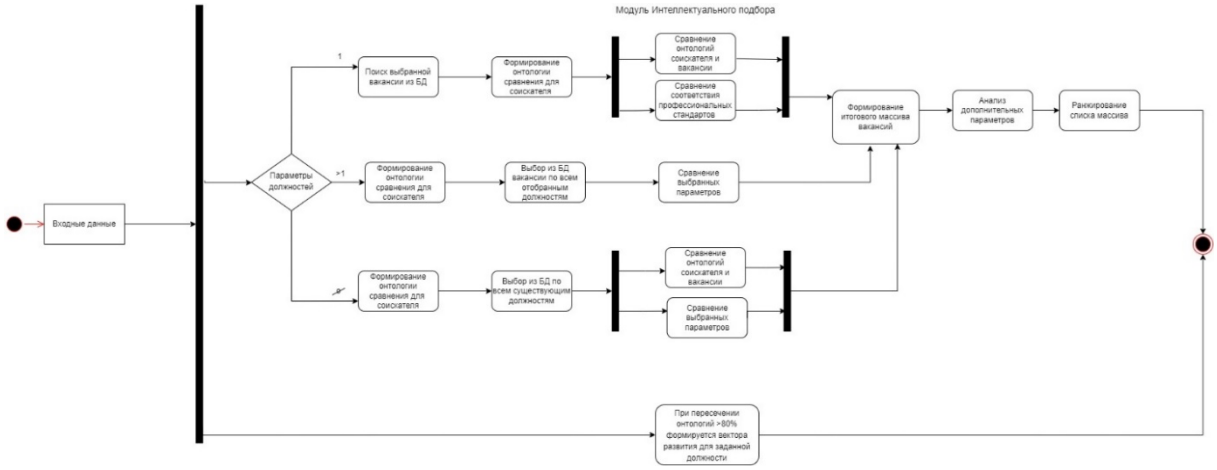


Рис. 2. Модель системы

Для выполнения ранжирования вакансий по степени соответствия, необходимо проанализировать характеристики и выявить компоненты сравнения вакансии и резюме. Оценка соответствия резюме и вакансии описывается следующей формулой.

$$v_i = \alpha_1 * E_i + \alpha_2 * L_i + \alpha_3 * S_i, i = \overline{1, N},$$

где i – порядковый номер онтологии вакансии, N – количество вакансий, v_i – оценка i-й вакансии, a – поправочные коэффициенты для компонентов оценки вакансии, $Ei,\ Li,\ Si$ – оценки компонентов «Обязанности», «Требования», «Навыки» i-й вакансии [1, 2].

При формировании итогового ранжированного списка вакансий, система разбивает объекты на классы актуальных рабочих мест. Кластерный анализ, с помощью исходных данных, предоставляет возможность распределить данный список на категории. Вместе с тем, в данной системе используется аналитико-онтологический подход соответствия выборки компонентов соискателя и вакансии, что позволяет более тщательно подойти

к вопросу формирования списка. Одновременно с этим система определяет оптимальный процент соответствия с помощью интеграции интеллектуального подхода, анализа параметров личностных навыков и профессиональных стандартов, что в совокупности обеспечивает повышение уровня комфортного климата в компании, и позволяет подобрать индивидуальный подход к каждому соискателю в соответствии с запросами к системе.

Список используемых источников

1. Математика и междисциплинарные исследования 2021 URL: http://www.psu.ru/files/docs/science/books/sborniki/mmi-2021 (дата обращения: 11.03.2022).

2. Муравьева-Витковская Л. А. Моделирование интеллектуальных систем: учеб.-метод. пособие. Санкт-Петербург: Изд-во НИУ ИТМО, 2012. 145 с.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

РАСШИРЕННОЕ ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ МОДЕЛИРОВАНИЕ ПЛАНИРОВЩИКОВ ДЛЯ УПРАВЛЕНИЯ КРУПНО-ГРАНУЛЯРНЫМИ ПРОЦЕССАМИ

Б. Б. Дамдинов, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Выделены перспективы развития и широкой востребованности мягких архитектур интеллектуальных информационных систем. Рассмотрены различные аспекты значимости интеллектуального управления крупно-гранулярными процессами в информационных системах с мягкой архитектурой. Представлена роль планировщика действий в интеллектуальных информационных системах с мягкой архитектурой. Проанализированы современные достижения в области исследования планировщиков действий. Выявлены преимущества расширенного объектно-ориентированного моделирования планировщиков действий. Раскрыты ключевые особенности предложенных объектно-ориентированных моделей планировщиков действий.

архитектура, крупно-гранулярный процесс, планировщик действий, модель, моделирование.

По мере цифровой трансформации различных сфер деятельности в процессе развития цифровой экономики непрерывно возрастает спрос на многокомпонентное программное обеспечение как системного, так и прикладного назначения. В силу высокой интенсивности происходящих обновлений в технологических профилях информационных инфраструктур и возникающих изменений на рынке труда, предлагаемой продукции, услуг и спроса на них усиливается конкуренция среди компаний и организаций, занимающихся разработкой и сопровождением многокомпонентного программного обеспечения для ресурсов информационных инфраструктур. В связи с этим проявляется объективная необходимость в обеспечении высокой гибкости функциональных спецификаций многокомпонентного программного обеспечения для ресурсов информационных инфраструктур, быстрой расширяемости реализуемых им функций, требуемого качества его функционирования и управляемости бизнес-процессами в контексте предметных областей выполняемой деятельности.

Специфика подобных условий сопровождения жизненного цикла многокомпонентного программного обеспечения для ресурсов информационных инфраструктур широко отображается в архитектуре сервис-ориентированных систем [1].

По мере наращивания технологической оснастки сопровождения жизненного цикла сервис-ориентированных систем сформировался новый вектор их развития в контексте автоматизации их гибкости по отношению к изменениям в окружающей среде, связанный с введением в их архитектуру средств искусственного интеллекта для управления интеграцией сервисов [2–6].

Управление интеграцией сервисов средствами искусственного интеллекта в условиях априорной неопределенности знаний о поведении окружающей среды является основной отличительной особенностью мягких архитектур сервис-ориентированных систем [7].

Благодаря подключению средств искусственного интеллекта к управлению интеграцией сервисов предоставляется возможность повышения степени гибкости сервис-ориентированных систем по отношению к изменениям во внешней среде, что несомненно согласуется с повышением востребованности интеллектуального многокомпонентного программного обеспечения ресурсов информационных инфраструктур.

В мягкой архитектуре сервис-ориентированных систем процесс функционирования каждого из сервисов является крупно-гранулярным процессом. По этой причине большое внимание уделяется исследованию интеллектуального управления крупно-гранулярными процессами в информационных системах с мягкой архитектурой. В контексте обеспечения требуемых гарантий качества функционирования интеллектуальных

сервис-ориентированных разрабатываются и раскрываются ключевые процедуры генерации соответствующего модельно-аналитического интеллекта [5–7].

Не менее значимым для управления интеграцией сервисов средствами искусственного интеллекта в условиях априорной неопределенности знаний о поведении окружающей среды является выбор планировщика действий, ассоциируемых с функциональностью сервисов.

В [8] представляется нейросетевой подход к преодолению априорной неопределённости при оптимальном планировании действий интеллектуальных информационных агентов для мягких архитектур сервис-ориентированных систем. В представляемом в [8] подходе критерии эффективности планирования конфигурации интеллектуальной сервис-ориентированной системы определяются посредством преобразования показателей качества, оцениваемых в системе мониторинга, отслеживающей его результативность. Подобное условие требует накопленного опыта внедрения планировщиков в интеллектуальные сервис-ориентированные системы.

Однако на начальных этапах жизненного цикла интеллектуальных сервис-ориентированных систем с мягкой архитектурой, где интеграцией занимаются интеллектуальные агенты, требуются знания о временных затратах на планирование действий по интеграции. В связи с этим предлагается расширение формализаций для преодоления априорной неопределённости при оптимальном планировании действий интеллектуальных информационных агентов для мягких архитектур сервис-ориентированных систем.

Предлагаемая модификация подхода осуществляется посредством расширенного объектно-ориентированного моделирования планировщиков действий для управления крупно-гранулярными процессами. В этом случае не понадобится развёртка системы мониторинга, что характерно для начальных этапов жизненного цикла интеллектуального многокомпонентного программного обеспечения.

Расширенное объектно-ориентированное моделирование планировщиков действий для управления крупно-гранулярными процессами выполняется путем реализации следующих этапов:

– структурное описание планировщиков действий;

– формирование базиса планировщиков действий;

– построение обобщенного алгоритма планирования действий;

– разработка обобщенной объектно-ориентированной модели планирования действий;

– расширение обобщенной объектно-ориентированной модели планирования действий посредством отображения стохастических характеристик потоков управления и операций;

– выбор методов анализа расширенной обобщенной объектно-ориентированной модели планирования действий;

– анализ расширенной обобщенной объектно-ориентированной модели планирования действий;

– формирование профилей динамических характеристик планировщиков из выделенного базиса.

Построение и анализ расширенной обобщенной объектно-ориентированной модели планирования действий осуществляется в базисе проверенных и исследованных формализаций, представленных в [5–7].

Предложенное расширение формализаций для преодоления априорной неопределённости при оптимальном планировании действий интеллектуальных информационных агентов для мягких архитектур сервис-ориентированных систем позволяет сгенерировать новое математическое обеспечение, ориентированное на управление гарантиями их качества.

Список используемых источников

1. Птицына Л. К., Смирнов Н. Г. Разработка и анализ моделей интеграции сервис-ориентированных средств в гетерогенных сетях // Научно-технические ведомости СПбГПУ 6.1 (138). 2011. С. 71–81.

2. Птицына Л. К., Кондратьев Д. А., Эльсабаяр Шевченко Н. Концептуальные модели интеллектуализации сервис-ориентированных архитектур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. Т. 2. С. 108–113.

3. Птицына Л. К., Кондратьев Д. А., Эльсабаяр Шевченко Н. Н. Интеллектуальные профили сервис-ориентированных архитектур // Труды учебных заведений связи. 2016. Т. 2, № 2. С. 72 – 77.

4. Птицына Л. К., Птицын А. В. Интеллектуальное конфигурирование сервис-ориентированных систем // Информационные системы и технологии в моделировании и управлении : сборник материалов IV Всероссийской научно-практической конференции с международным участием (21-23 мая 2019 г.) / отв. редактор К. А. Маковейчук. Симферополь : ИТ «АРИАЛ», 2019. С. 48-51.

5. Птицына Л. К. Методология генерации модельно-аналитического интеллекта сервис-ориентированных систем с гарантиями качества // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2017. Т. 3. С. 351–354.

6. Ptitsyna L. K., Shevchenko N. E. S., Belov M. P., Ptitsyn A. V. Planning Architecture of Service-oriented Systems under Uncertainty // Proceedings of 2020 23rd International Conference on Soft Computing and Measurements. SCM 2020, 2020. pp. 101–104.

7. Птицына Л. К., Эль Сабаяр Шевченко Н., Белов М. П., Птицын А. В. Математическое обеспечение мягких архитектур сервис-ориентированных систем в условиях неопределённости // XXIV Международная конференция по мягким вычислениям и измерениям (SCM-2021). Сборник докладов. Санкт-Петербург. 26–28 мая 2021 г. СПб.: СПбГЭТУ «ЛЭТИ». С. 121–124.

8. Ptutsyna L. K., El Sabayar Shevchenko N., Belov M. P., Ptitsyn A. V. A neural network approach to overcoming a priori uncertainty in optimal action planning of intelligent information agents for soft architectures of service-oriented systems // Proceedings of 2021 2nd International Conference on Neural Networks and Neurotechnologies, NeuroNT 2021. 2. 2021. pp. 31–34.

УДК 004.77
ГРНТИ 49.33.29

ИСПОЛЬЗОВАНИЕ MAC АДРЕСОВ ДЛЯ ИДЕНТИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ ПОЯВЛЕНИЯ НЕИЗВЕСТНЫХ УСТРОЙСТВ В СЕТИ

Ю. В. Денисова, Д. Ю. Петров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время вопрос внедрения систем сетевой безопасности на предприятиях является наиболее востребованным, поэтому в статье рассматривается внедрение системы безопасности локальной сети с использованием MAC адресов.

Таким образом идентификация и предупреждение включает в себя элементы анализа сети с использованием различных способов, уведомление об обнаруженных неизвестных устройствах и предотвращение их функционирования внутри локальной сети. Это направлено на снижение количества неизвестных устройств и повышение безопасности сети.

локальные сети, MAC-адреса, информационная безопасность.

Для осуществления процесса повышения безопасности ЛВС: предлагается использовать мониторинг MAC-адресов путем получения их:

– из таблицы MAC-адресов коммутатора;

– со специализированного сервера сканирования сети с использованием ARP-протокола;

– с использованием сетевого анализатора трафика.

В коммутаторе динамически формируется таблица MAC-адресов полученная из кадров. Когда коммутатор получает кадр, на котором не указан адрес назначения, он делает широковещательную рассылку на все порты за исключением порта получателя. Когда узел назначения отвечает, коммутатор добавляет актуальный MAC адрес источника и номер порта в таблицу адресов. Затем коммутатор переадресует все последующие кадры через единственный без широковещательной рассылки на все порты [1].

Получение актуальной таблицы MAC-адресов коммутатора может быть осуществлено с помощью применения команды запроса вывода таблицы на коммутаторе [2].

На коммутаторах компании D-link вывод таблицы коммутации можно осуществить с помощью команды: "show fdb". Пример таблицы MAC-адресов приведен на рис. 1.

```
DES-3200-10:5#sh fdb
Command: show fdb

Unicast MAC Address Aging Time  = 300

VID  VLAN Name                        MAC Address       Port Type
---- -------------------------------- ----------------- ---- ---------------
1    default                          00-02-21-21-39-1C  1   Dynamic
1    default                          00-02-21-21-39-1E  3   Dynamic
1    default                          00-26-5A-39-39-E8 CPU  Self

Total Entries  : 3
```

Рис. 1. Извлечение таблицы с устройства D-link

Для коммутаторов компании Cisco вывод таблицы MAC-адресов осуществляется при помощи команды привилегированного режима: "show mac address-table". Пример вывода таблицы MAC-адресов приведен на рис. 2.

Специализированный сервер сканирования сети с использованием ARP-протокола определения соотношения IP-адреса устройства с его физическим адресом. Формирование записи в таблице осуществляется в момент, когда устройство рассылает широковещательный ARP запрос с целью получить MAC-адрес устройства.

```
Switch#show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000d.bdd7.a920    DYNAMIC     Fa0/2
   1    00e0.a3a9.5576    DYNAMIC     Fa0/3

Switch#
```

Рис. 2. Извлечение таблицы с устройства Cisco

Для реализации сканирования сети планируется применение утилиты ARP Scan рис. 3. Утилита отображает все активные на данный момент устройства локальной сети. Сканирование осуществляется с помощью команды: "arp-scan --interface=ИНТЕРФЕЙС --localnet" [3]

```
sergiy@sergiy-pc:~$ sudo arp-scan --interface=enp24s0 --localnet
Interface: enp24s0, type: EN10MB, MAC: 00:d8:61:16:a5:a5, IPv4: 192.168.0.102
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     b0:be:76:43:21:41       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.101   74:d4:35:00:b1:ef       GIGA-BYTE TECHNOLOGY CO.,LTD.

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.989 seconds (128.71 hosts/sec). 2
responded
```

Рис. 3. Сканирование с помощью ARP-Net

С использованием сетевого анализатора трафика. Из способов обнаружения устройств в локальной вычислительной сети можно применять различного рода программы или устройства сканирования сети посредством перехвата сетевого трафика, передаваемого для других устройств [4].

Пример реализации процесса анализа сетевого трафика приведен на рис. 4.

Для осуществления получения MAC-адресов используется фильтр ARP, а также извлечение из кадра MAC-адреса источника, в дальнейшем, данная информация перенаправляется на сервер с целью анализа и сверки.

Получение MAC-адресов устройств необходимо для реализации следующего алгоритма, связанного с идентификацией и предупреждением неизвестных устройств сети.

Анализ и выявление постороннего устройства предлагается с использованием составления матриц в ранжированном порядке MAC-адресов.

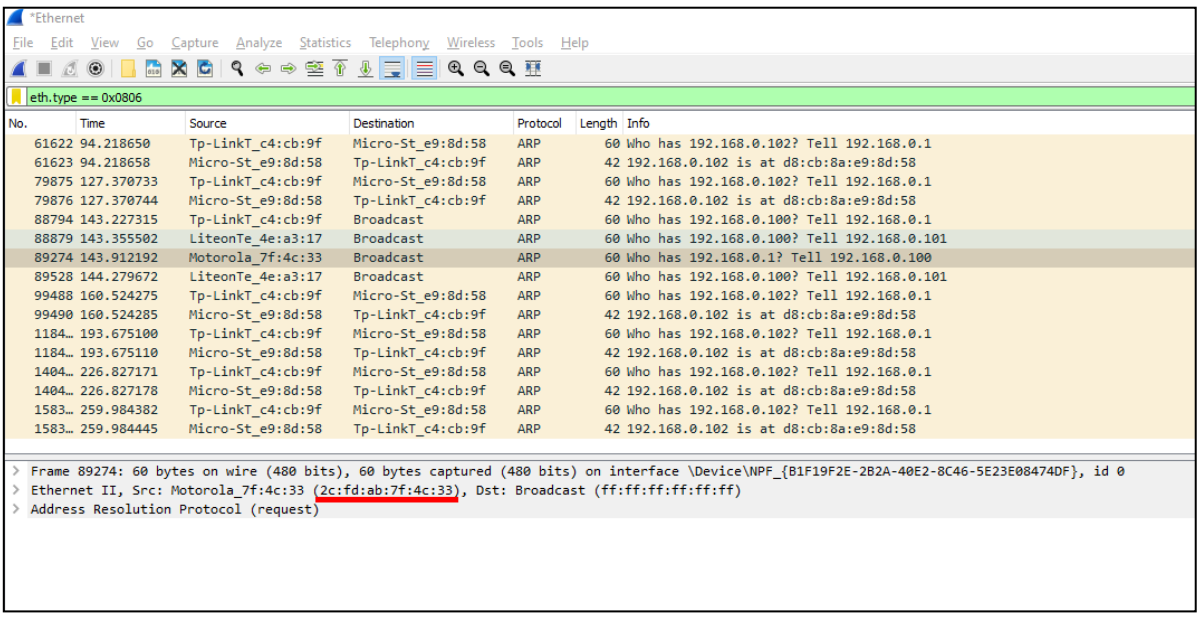


Рис. 4. Извлечение MAC-адреса с помощью анализатора сет

Алгоритм работы искусственного интеллекта работает в следующем режиме.

Первоначально задается матрица константа, с которой, в дальнейшем, возникает сопоставление матрицы переменной, полученной программой в результате анализа MAC-адресов сети, а также сложения таблиц в одну супертаблицу.

Следующий шаг запускает процесс сопоставления матриц, в результате которого, достигается обнаружение MAC-адресов (измененных или не существующий) ранее в сети.

Вычисление предполагается выполнять с использованием одного из методов искусственного интеллекта, функции которого:

– определить производителя по MAC-устройству;

– оповестить о нарушении администратора сети.

Для определения производителя по MAC-устройству, полученный, в результате работы искусственного интеллекта, адрес, проверяется в, сформированной ранее, базе данных с целью получения информации о производителе.

Вся информация о конкретном адресе формируется подразделением Institute of Electrical and Electronics Engineers, именно оно выделяет конкретные регистрационные номера компаниям для пользования.

При оповещении о нарушении администратора сети, в случае, если был обнаружен неизвестный адрес, запускается режим оповещения администратора сети, в целях снижения времени реагирования, оповещение осуществляется одновременно несколькими способами:

– оповещение высылается в виде логов на сервер мониторинга сети;

– отправляется сообщение в качестве Email системному администратору;

– осуществляется SMS сообщение на мобильное устройство.

Автоматически заблокировать устройство на сервере

Для реализации блокирования устройства в сети применяется реализация списка управления доступом на ключевых коммутаторах сети, тем самым ограничивая доступ к сети устройству нарушителя [5]. Варианты реализации функционирования системы блокировки получения трафика приведены на рис. 5–7.

Рис. 5. Блокирования получение трафика на коммутаторах Cisco

```
DGS-1210-28/ME:5# config access_profile profile_id 1 add access_id 1 ethernet destination_mac 60:02:92:25:ec:66 port 2 deny
Command: config access_profile profile_id 1 add access_id 1 ethernet destination_mac 60:02:92:25:ec:66 port 2 deny

Success.
```

Рис. 6. Блокирование получения трафика на коммутаторах D-link

```
[R2-acl-adv-onlypc4-5]rule 100 deny ip source any destination any
```

Рис. 7. Блокирование получения трафика на коммутаторах Huawei

Последовательность выполнения данной функции приведена на рис. 8.

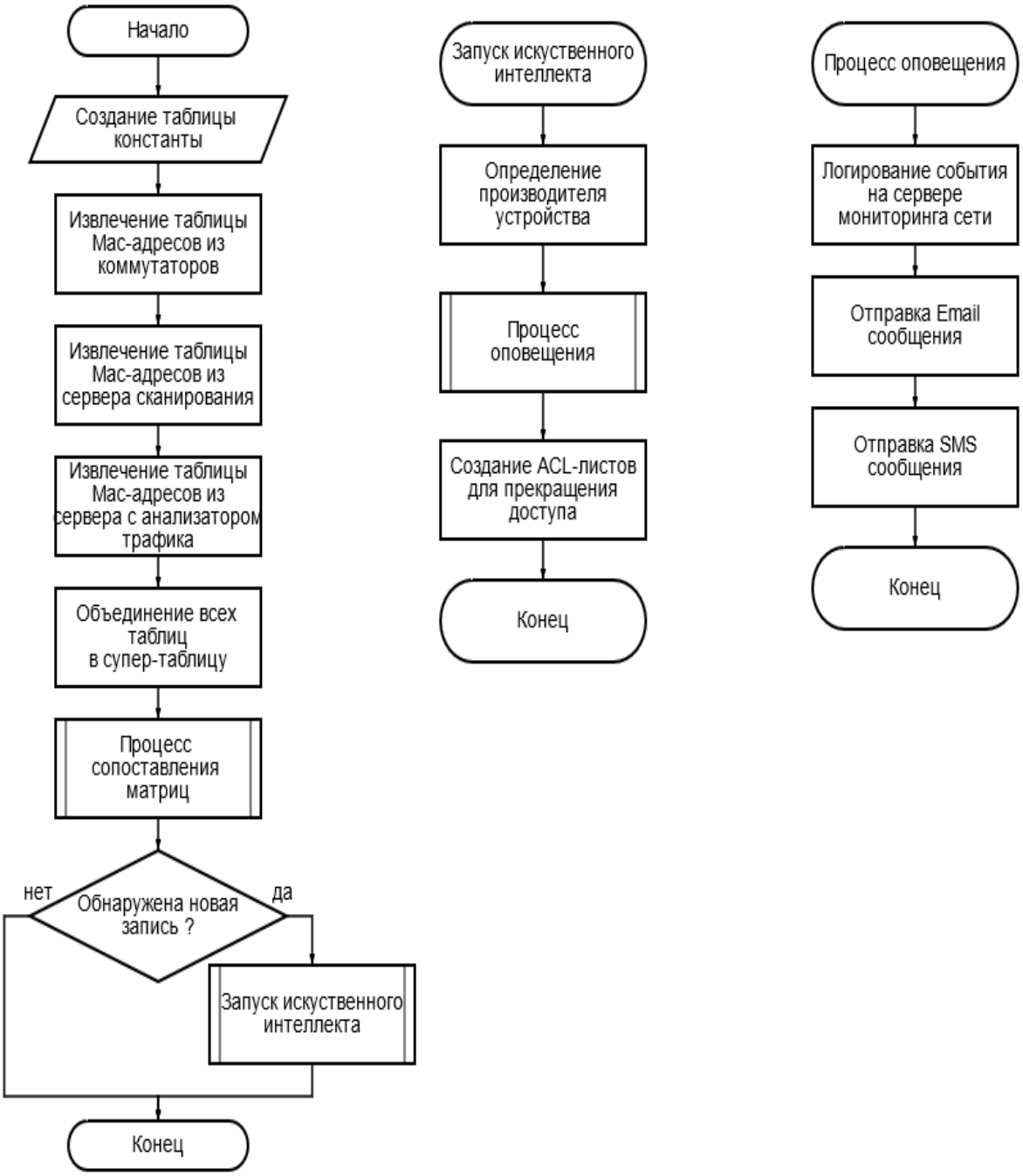


Рис. 8. Последовательность выполнения функции

В результате было приведены способы мониторинга уровня доступа в ЛВС, анализ и выявление посторонних устройств, а также оповещение в случае возникновения инцидентов.

Данная технология необходима в тех случаях, когда безопасность ЛВС имеет наибольших приоритет и может применяться в сетях с чувствительной информацией.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети, принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 с.

2. Танненбаум Э., Уезеролл Д. Компьютерные сети 5-е изд. СПб.: Питер, 2012. 960 с. ISBN 978-5-459-00342-0

3. Трабельси З., Хаяви К., Мэтью С. Сетевые атаки и защита практическое руководство: пер. с англ.: Condor, 2013, 475 с. ISBN 978-1-4665-1797-4

4. Куракин А. С., Жуковский А. В., Зозуля Е. И. Экспертные системы комплексной оценки безопасности объекта: учебное пособие / Под ред. профессора, д.т.н. Ю. А. Гатчина. СПб. : НИУ ИТМО, 2016. 25 с.

5. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1640-822, 3-е изд. : Пер. с англ. М. : ООО “И.Д. Вильямс”, 2013 720 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом М. Д. Поведайко.

УДК 621.397
ГРНТИ 28.23.15

ПРОЕКТИВНОЕ СОВМЕЩЕНИЕ ТЕЛЕВИЗИОННЫХ ИЗОБРАЖЕНИЙ С ПРЕДВАРИТЕЛЬНЫМ СОПОСТАВЛЕНИЕМ ОСОБЫХ ТОЧЕК НА ОСНОВЕ ЛОГАРИФМИЧЕСКИ-ПОЛЯРНОЙ СИСТЕМЫ КООРДИНАТ

А. А. Диязитдинова

Поволжский государственный университет телекоммуникаций и информатики

В многокамерных системах технического зрения одной из актуальных задач является проективное совмещение телевизионных изображений по данным, полученным в ходе натурной съемки. В отличие от совмещения с использованием тест-объекта (как

правило, шахматной доски) данная задача осложняется проблемой сопоставления реперных точек, по которым рассчитываются параметры проективного преобразования. Использование метода полного перебора определяет огромное количество вариантов сопоставления, время проверки которых не удовлетворяет требованиям по настройке систем видеонаблюдения. Для уменьшения количества вариантов был предложен алгоритм, который реализует эвристическую процедуру выбора проверенных точек и процедуру предварительного сопоставления на основе логарифмически-полярной системы координат.

проективный, совмещение, сопоставление, логарифмически-полярный, изображение.

В системах видеоаналитики и видеосистемах промышленного назначения в последние десятилетия стали применяться многокамерные системы технического зрения.

Многокамерные системы технического зрения отличаются от систем видеонаблюдения тем, что съемка кадров различными камерами проводится синхронно. В данных содержится временная метка, позволяющая проводить обработку изображений, снятых в одно и то же время. Эта особенность расширяет функциональные возможности подобных систем.

На их основе можно разрабатывать системы видеонаблюдения с расширенным полем зрения и с высокой разрешающей способностью [1, 2]. Для реализации таких функциональных возможностей необходимо проводить совмещение изображений, получаемых от различных камер.

Параметры совмещения оцениваются в ходе специальной процедуры настройки. В поле зрения камер устанавливается тест-объект (как правило, шахматная доска), по которому определяются реперные точки. Использование тест-объекта обеспечивает автоматическое сопоставление реперных точек на изображениях. По координатам реперных точек оцениваются параметры совмещения.

Однако существуют такие ситуации, при которых установка тест-объекта невозможна. Пример 1: многокамерная система располагается на высотном здании, и установка тест-объекта является сложной технической и дорогостоящей процедурой. Пример 2: многокамерная система стоит на транспортном средстве, настройка которой проводится в лабораторных условиях; в случае замены одной из камер возникает необходимость демонтажа и повторной настройки, что является экономически нецелесообразной процедурой.

Для подобных ситуаций необходима разработка метода совмещения изображений по данным, снятым в ходе натурной видеосъемки. Дополнительным требованием к методу совмещения является обработка без участия человека (примечание: параметры совмещения рассчитываются по реперным точкам, которые может указать человек на изображении; однако такой способ приводит к зависимости работы системы от действий конкретного человека, что противоречит идее работы промышленных автономных систем).

Разработке метода и алгоритма совмещения телевизионных изображений по данным, снятым в ходе натурной съемки, посвящено данное исследование.

В ходе проведения предварительных работ стоял вопрос выбора подходящей математической модели для совмещения. В качестве вариантов рассматривались:

– аффинная модель;

– проективная модель;

– модель эластичного преобразования.

Результаты анализа показали, что в ряде случаев аффинная модель не позволяет качественно совмещать изображения. Если оптические оси камер образуют угол, то возникают искажения следующего вида: прямые, которые параллельны на одном изображении, не будут являться параллельными на втором изображении. Аффинная модель сохраняет свойство параллельности прямых линий. По этой причине данная модель не подходит для решения рассматриваемой задачи.

Проективная модель и модель эластичного преобразования обеспечивали практически идентичный результат, однако, проективная модель является более простой: содержит только 8 параметров, в то время как количество параметров в эластичной модели параметров намного больше и их количество зависит от количества совмещаемых фрагментов изображений. Для упрощения разработки методики была выбрана проективная модель.

Проективная модель описывается выражением:

$$x' = \frac{h_{11}x + h_{12}y + h_{13}}{h_{31}x + h_{32}y + 1},\ y' = \frac{h_{21}x + h_{22}y + h_{23}}{h_{31}x + h_{32}y + 1}.$$

Для оценки параметров ($h_{11}, h_{12}, ..., h_{32}$) достаточно иметь 4 точки.

В качестве реперных точек использовались особые точки, вычисленные с помощью детектора Harris [3].

Первоначальная идея использования метода полного перебора для проверки всех возможных вариантов сопоставления точек оказалось нереализуемой на практике.

При использовании 4 точек для совмещения количество вариантов описывается выражением:

$$V = C_M^4 \cdot A_N^4,$$

где C – количество сочетаний, A – количество размещений, M – количество точек на первом изображении, N – количество точек на втором изображении.

Если количество точек M и N будет порядка 1 000 (в реальности особых точек может быть больше), то количество вариантов V будет больше 10^{22}. Если время проверки одного варианта будет 10^{-2}с, то время обработки составит приблизительно $3 \cdot 10^{13}$ лет.

Чтобы время совмещения удовлетворяло требованиям по настройке систем видеонаблюдения [4], было разработано две процедуры:

– эвристическая процедура выбора проверяемых особых точек;

– процедура предварительного сопоставления на основе логарифмически-полярной системы координат.

Первая процедура реализует выбор четырех точек $(x_1, y_1)\ldots(x_4, y_4)$ на изображениях, которые будут удовлетворять следующим ограничениям:

– $y_2 > y_1$;
– $x_3 > x_1$;
– $y_3 > y_1$;
– $x_4 > x_1$;
– $r_{13} \cdot m1 < r_{12} < r_{13} \cdot m2$;
– $r_{13} \cdot m1 < r_{14} < r_{13} \cdot m2$;
– $R1 < r_{13} < R2$;
– $k_{14} < k_{13} < k_{12}$;

где $r_{12} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$, $r_{13} = \sqrt{(x_1 - x_3)^2 + (y_1 - y_3)^2}$,

$r_{14} = \sqrt{(x_1 - x_4)^2 + (y_1 - y_4)^2}$. $k_{12} = \frac{y_1 - y_2}{x_1 - x_2}$, $k_{13} = \frac{y_1 - y_3}{x_1 - x_3}$, $k_{14} = \frac{y_1 - y_4}{x_1 - x_4}$

(примечание: для изображения с размером 1280×720 пикселей использовались следующие параметры: $m1 = 0{,}333$, $m2 = 0{,}666$; $R1 = 200$ пикселей, $R2 = 500$ пикселей).

На рис. 1 показаны иллюстрации заданных ограничений.

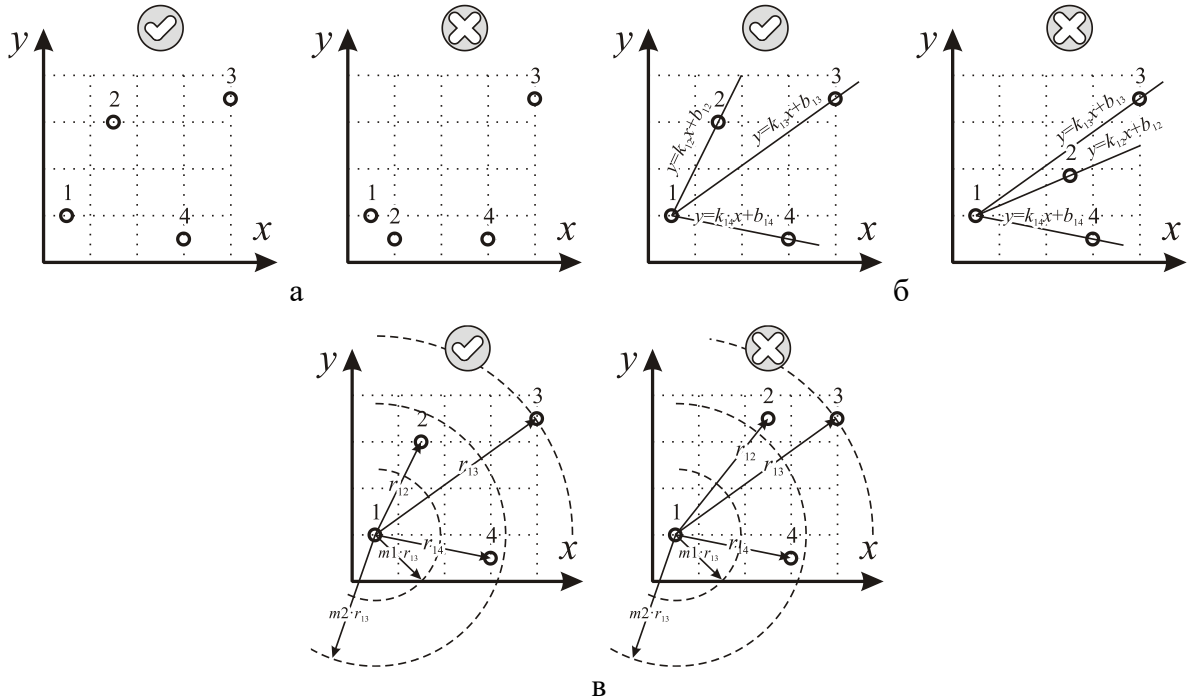


Рис. 1. Ограничения:
(а) на взаимное расположение точек, (б) по углу, (в) по расстоянию

Вторая процедура позволяет для каждой точки первого изображения поставить в соответствие возможные точки второго изображения, которое определяется по фрагментам в окрестности этих точек. Для обеспечения инвариантности к повороту и масштабу фрагменты изображений представляются в логарифмически-полярном виде. В таком представлении отличия по углу и масштабу эквивалентны смещениям [5–9]. На рис. 2 показан пример представления с использование логарифмически-полярной системы координат.

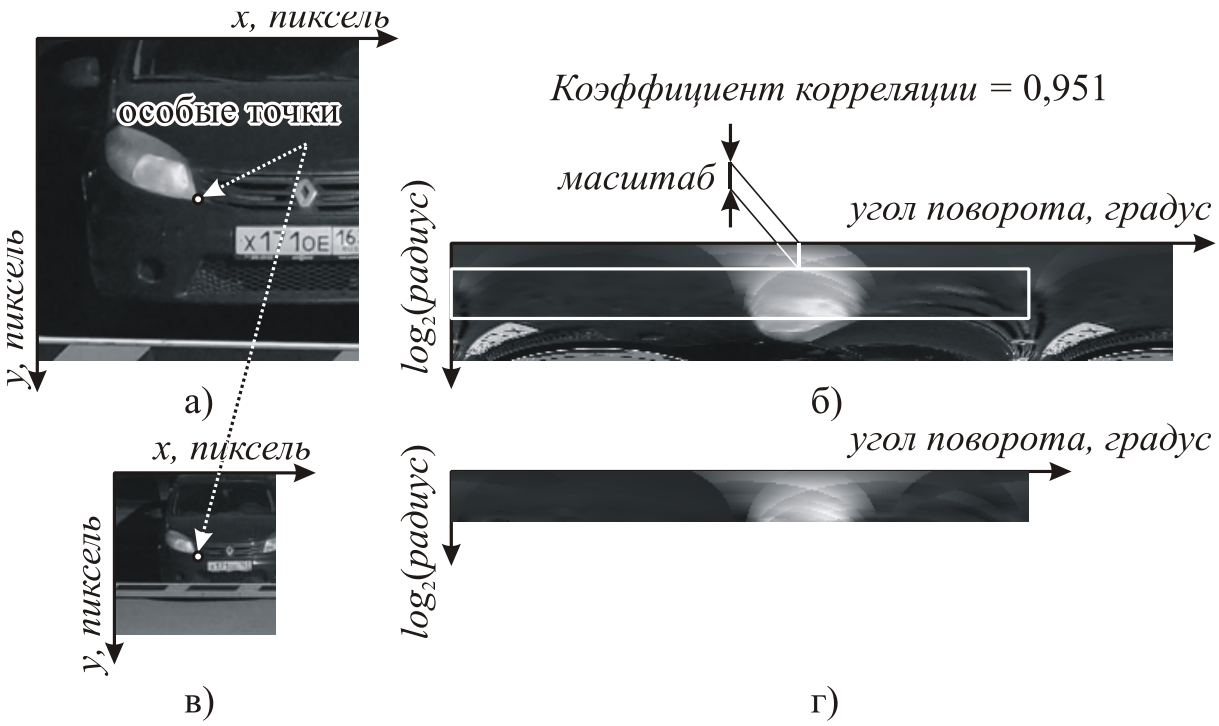


Рис. 2. Сравнение фрагментов в логарифмически-полярной системе координат

Разработанный алгоритм представлен на рис. 3.

При количестве особых точек порядка 2 000 на совмещаемых изображениях время обработки не превышало 45 минут на персональном компьютере с процессором Intel Core i7.

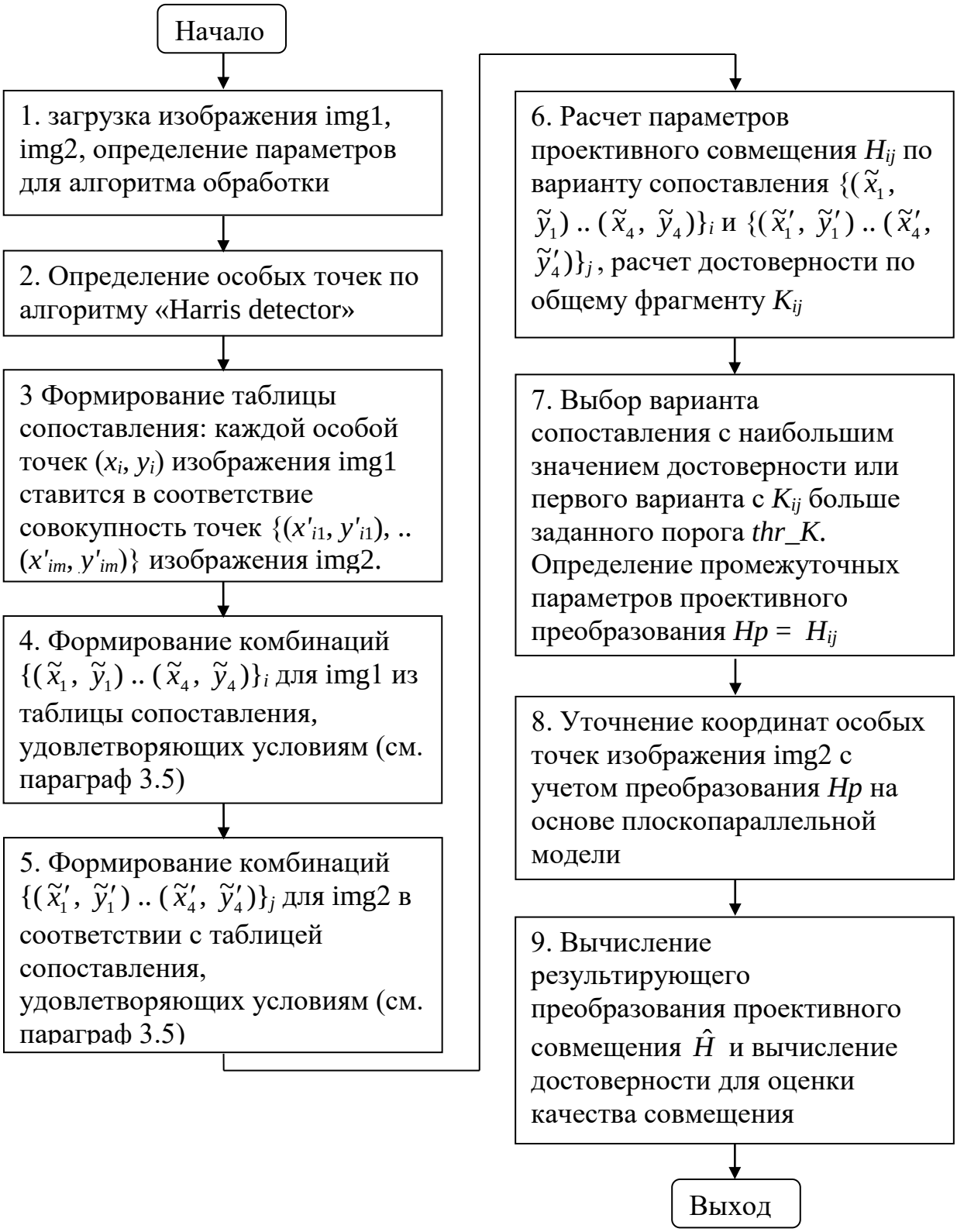
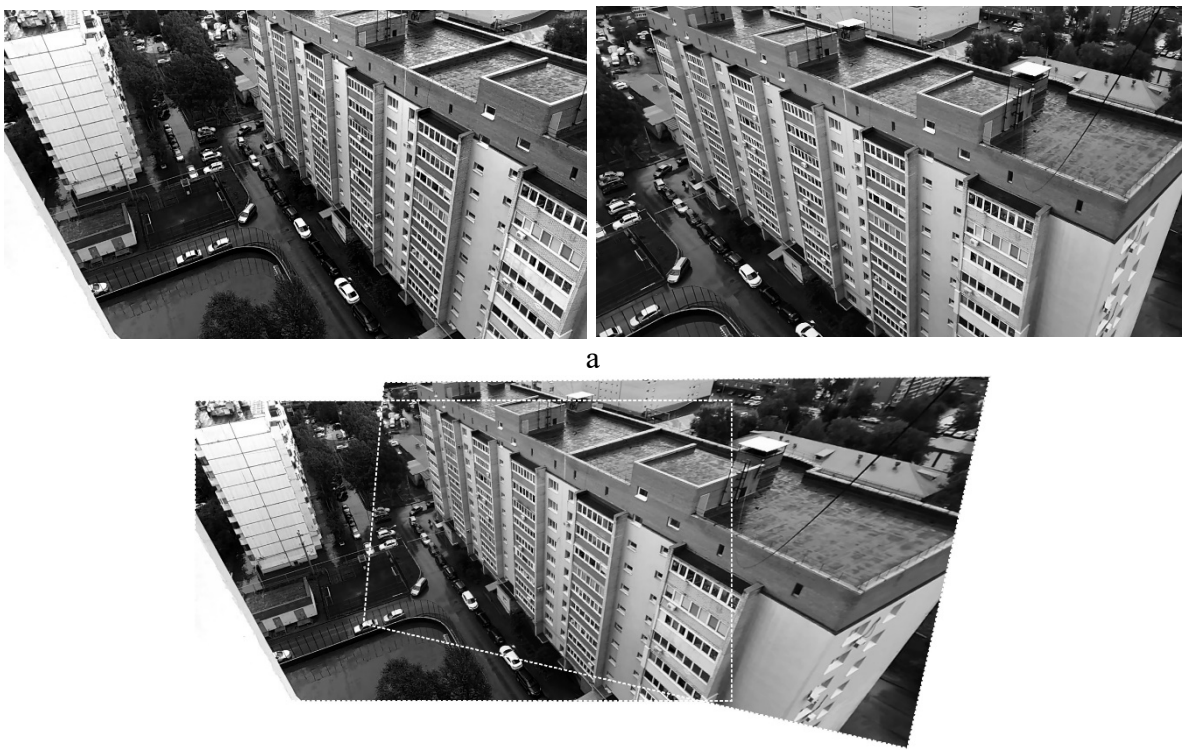


Рис. 3. Разработанный алгоритм совмещения

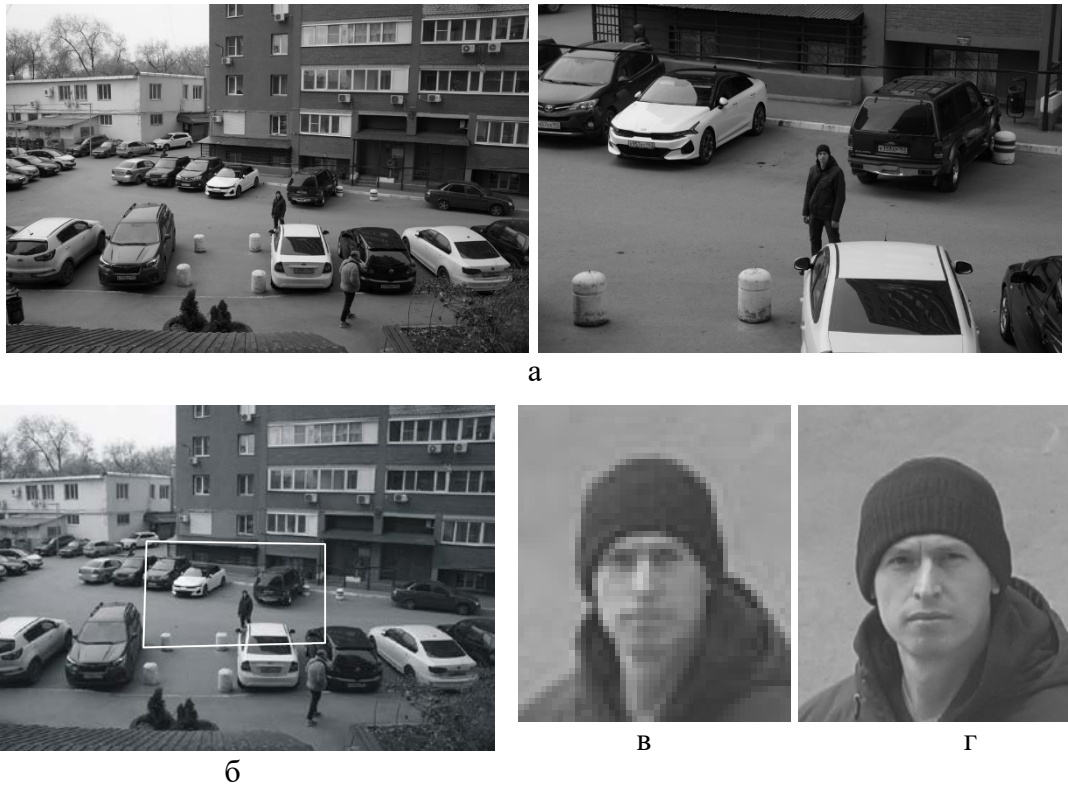
На рис. 4 и рис. 5 показаны примеры работы алгоритма.



а

б

Рис. 4. Съемка периметра наблюдения системой, установленной на высотном здании: (а) исходные изображения, (б) результат совмещения



а

б в г

Рис. 5. Съемка периметра наблюдения за двором жилого дома: (а) исходные изображения, (б) результат совмещения, результат увеличения в (в) однокамерной системе и (г) многокамерной системе

Как можно видеть из рис. 4 и рис. 5, алгоритм обеспечивает корректное совмещение изображений. Также на рис. 5 показан результат увеличения при использовании однокамерной (см. рис. 5в) и многокамерной системы (см. рис. 5г). Использование многокамерного режима позволяет в значительной степени повысить разрешающую способность фрагмента изображения.

Разработанный алгоритм позволяет в автоматическом режиме совмещать изображения многокамерных систем видеонаблюдения и может быть использован предприятиями, специализирующихся на разработке охранных и измерительных систем.

Список используемых источников

1. Осипов О. В., Диязитдинова А. А. Совмещение сигналов для повышения качества телевизионного изображения многокамерной системы видеонаблюдения // Радиотехника. 2020. Т. 84. N 12 (23). С. 72–78.

2. Диязитдинова А. А. Повышение помехоустойчивости при оценке параметров проективного совмещения телевизионных сигналов // Физика волновых процессов и радиотехнические системы. 2021. Т. 24. N 1. С. 58–66.

3. Harris C., Stephens M. A combined corner and edge detector // Proceedings of the 4th Alvey Vision Conference, Manchester, 31 August-2 September 1988. Manchester: 1988. pp. 147–151.

4. EN 50132-7:2012 - Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines. 2012. 64 c.

5. Мясников Е. В. Определение параметров геометрических трансформаций для совмещения портретных изображений // Компьютерная оптика. 2007. Т. 31. N 3. С. 77–82.

6. Reddy B.S., Chatterji B.N. An FFT-based technique for translation, rotation, and scale-invariant image registration // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1996. N 5 (8). pp. 1266–1270.

7. Wolberg G., Zokai S. Robust image registration using log-polar transform // Proc. IEEE International Conference on Image Processing. 2000. N 1. pp. 493–496.

8. Kuglin, C. D., Hines, D. S. The phase correlation image alignment method // Proc. International Conference on Cybernetics and Society. 1975. N 1. pp. 163–165.

9. Brown L. G. A survey of image registration techniques // ACM Computing Surveys. 1992. N 24 (4). pp. 325–376.

Статья представлена
заведующей кафедрой информационных систем и технологий ПГУТИ,
доктором технических наук, доцентом Н. И. Лимановой.

УДК 004.942
ГРНТИ 20.15.05

ПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ВЫБОРА СТРАТЕГИЙ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ СВЯЗИ

М. М. Добрышин, Ю. А. Левичева, А. Н. Реформат

Академия Федеральной службы охраны Российской Федерации

Совершенствование способов применения компьютерных атак в отношении корпоративных сетей связи интегрированных в мировое информационное пространство требует соответствующего развития и систем обеспечения информационной безопасности. Анализ общих подходов проектирования подобных систем выявил недостаток: недостаточно обоснованный выбор оптимального состава и структуры этой системы. Для устранения указанного недостатка сформулирована последовательность оценки эффективности, основанная на отклонении нормированных значений от требуемых значений и предложение по построению стратегии защиты на основе генетического алгоритма.

система обеспечения информационной безопасности, эффективность, генетический алгоритм.

Пусть существует задача по выбору оптимальной структуры построения системы обеспечения информационной безопасности (СОИБ) фрагмента корпоративной сети связи, который максимизирует такие свойства информации как конфиденциальность, целостность, доступность. Свойствами СОИБ будем считать следующие: своевременность, оперативность, полнота, модернизируемость, устойчивость, ресурсопотребление [1]. Эти же свойства предлагается применить к составляющим элементам СОИБ – средств защиты (СЗ).

ТАБЛИЦА 1. Исходные данные

Вариант средства защиты	Своевременность	Оперативность	Полнота	Модернизируемость	Устойчивость	Ресурсопотребление
$СЗ_1$	c_1	o_1	p_1	M_1	y_1	r_1
$СЗ_2$	c_2	o_2	p_2	M_2	y_2	r_2
$СЗ_3$	c_3	o_3	p_3	M_3	y_3	r_3
…	…	…	…	…	…	…
$СЗ_n$	c_n	o_n	p_n	M_n	y_n	r_n

Далее вводят нормируемые параметры $c_{норм}$, $o_{норм}$, $p_{норм}$, $m_{норм}$, $y_{норм}$, $r_{норм}$ установленные ГОСТ, техническим заданием и т. д. В соответствии с этими параметрами исключаем варианты построения СОИБ не удовлетворяющие параметрам:

$$c_{норм} \leq c_m, \text{ где } m=1..n,$$

$$o_{норм} \leq o_m, \text{ где } m=1..n,$$

$$p_{норм} \leq p_m, \text{ где } m=1..n,$$

$$M_{норм} \leq M_m, \text{ где } m=1..n,$$

$$y_{норм} \leq y_m, \text{ где } m=1..n,$$

$$r_{норм} \geq r_m, \text{ где } m=1..n.$$

Находим абсолютное отклонение ($k_m`$, $o_m`$, $d_m`$, $M_m`$, $y_m`$, $r_m`$) значения каждого параметра от идеального значения:

$$c_m` = |1 - c_m|,$$

$$o_m` = |1 - o_m|,$$

$$p_m` = |1 - p_m|,$$

$$M_m` = |1 - M_m|,$$

$$y_m` = |1 - y_m|,$$

$$r_m` = |1 - r_m|.$$

Затем, чтобы получить обобщенную численную оценку каждого варианта построения СОИБ, производим мультипликативную свертку:

$$E_v^{'} = \prod\{c`_m, o`_m, p`_m, M`_m, y`_m, r`_m\},$$

На основе произведенных подсчетов выбирают наилучший вариант построения СОИБ. Критерий принятия решения – минимальное значение мультипликативной свертки:

$$E_v^{'} \rightarrow \min.$$

Таким образом при имеющихся средствах защиты находят вариант построения СОИБ, минимально отличающийся от СОИБ с идеальными параметрами.

Затем для лучшего варианта СОИБ начинается поиск лучшей стратегии защиты в условиях разнородных атак. Разные СЗ, входящие в имеющийся

вариант СОИБ, направлены на противодействие конкретному виду ИТВ, в следствии чего по-разному обеспечивают реализацию требований, предъявляемых к свойствам защищаемой информации (конфиденциальности, целостности, доступности).

Компьютерные атаки (КА) чаще всего являются комплексными, т. е. состоящими из нескольких видов ИТВ. Для построения эффективной СОИБ необходимо не только использовать СЗ предназначенные для противодействия ИТВ данной КА, но и объединять имеющиеся СЗ в систему, получая новые свойства таких комбинаций.

Стратегии защиты формируются перебором всех возможных вариантов построения из имеющихся СЗ.

ТАБЛИЦА 2. Обеспечение свойств информации

	$КА_1$			$КА_2$			…		
	Конф.	Цел.	Дост.	Конф.	Цел.	Дост.	Конф.	Цел.	Дост.
Стратегия 1	a_1	b_1	c_1	d_1	i_1	f_1	g_1	h_1	j_1
Стратегия 2	a_2	b_2	c_2	d_2	i_2	f_2	g_2	h_2	j_2
…	$a...$	$b...$	$c...$	$d...$	$i...$	$f...$	$g...$	$h...$	$j...$
Стратегия w	a_w	b_w	c_w	d_w	i_w	f_w	g_w	h_w	j_w

Применив генетический алгоритм (ГА) [2] к обозначенным стратегиям, можно не только найти насколько каждая стратегия подходит для отдельного вида КА (значение функции приспособляемости для каждой КА), но и применив скрещивание получить значение приспособляемости каждой стратегии к конкретной комбинированной КА с учетом новых свойств, возникающих при объединении СЗ в систему (функция приспособляемости с учетом новых свойств). Для примера приведена таблица 3. Исходные данные взяты из таблицы 2; числовые значения целостности, конфиденциальности, доступности информации имеют случайные значения, взятые для демонстрации примера.

Проведя таким образом исследование для всех возможных видов КА и комбинаций объединения КА, возможно построить СОИБ, обеспечивающую защиту от наиболее актуальных угроз [3] для защищаемого фрагмента корпоративной сети связи с учетом новых свойств, появляющихся за счет эмерджентности системы, образуемой при объединении СЗ. Рассмотренный подход частично реализован в патенте РФ на изобретение [4].

ТАБЛИЦА 3. Пример проведения расчета

	$КА_1$		$КА_2$	
Функция приспособляемости: конф*цел*доступ	a_1 (0.8) b_1 (0.8) c_1 (0.8)		d_1 (0.7) i_1 (0.9) f_1 (0.9)	Первое поколение
Функция приспособляемости	0,512		0,567	Среднее качество поколения: 0,5359
	$КА_1$+$КА_2$			
	a1 (0.8) *i1* (0.9) *f1* (0.9)		*d1* (0.7) *b1* (0.8) *f1* (0.9)	Второе поколение
Функция приспособляемости с учетом новых свойств	0,648		0,504	Среднее качество поколения: 0,576

Список используемых источников

1. Добрышин М. М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия тульского государственного университета. Технические науки. 2021. N 9. С. 113–121.

2. Панченко Т. В. Генетические алгоритмы : учебно-методическое пособие / под ред. Ю. Ю. Тарасевича. Астрахань : Издательский дом «Астраханский университет», 2007. 87 с.

3. Белов А. С., Добрышин М. М., Борзова Н. Ю. Формирование модели угроз информационной безопасности на среднесрочный период / Приборы и системы. Управление, контроль, диагностика. 2021. № 7. С. 41–48.

4. Макаров В. Н., Гречишников Е. В., Добрышин М. М., Климов С. М., Манзюк В. В., Локтионов А. Д. Способ выбора и обоснования тактико-технических характеристик системы защиты от групповых разнородных компьютерных атак на среднесрочный период / Патент РФ на изобретение № 2760099 22.11.2021 Бюл. № 33 Заявка 2020124308, от 22.07.2020. Патентообладатель: Академия ФСО России. G06F 21/57 (2013.01).

УДК 004.514
ГРНТИ 50.41.29

АНАЛИЗ СОВРЕМЕННОГО УРОВНЯ РАЗВИТИЯ ТЕХНОЛОГИЙ СОЗДАНИЯ ИНТЕРАКТИВНОГО ВИЗУАЛЬНОГО КОНТЕНТА

Н. К. Елисеев, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные технологии передачи данных позволяют просматривать визуальный контент на разных платформах: от эфирного телевидения до видеосервисов в сети Интернет. Одним из способов повышения заинтересованности пользователей при просмотре видео является добавление интерактивных компонентов в видео контент. Однако различие интерфейсов устройств воспроизведения обусловили создание различных принципов взаимодействия человека с интерактивным контентом.

В статье представлена классификация технологий передачи медиаконтента, выполнен сравнительный анализ существующих технологий взаимодействия человека с интерактивным визуальным контентом на разных платформах, приведены примеры реализации интерактивного видеоконтента. В работе сформулированы требования к универсальному интерфейсу взаимодействия человека с интерактивным контентом. Полученные результаты могут быть полезны при создании интерфейсов, основанных на единых принципах взаимодействия с интерактивным визуальным контентом.

интерактивизация, интерактивный медиаконтент, классификация, взаимодействие, человеко-машинный интерфейс, пользовательский интерфейс.

Современные устройства просмотра медиаконтента, к которым относятся: телевизоры, «умные» экраны, интерактивные доски, телефоны, планшеты и пр., достигли высокого уровня развития, их интерфейсы совершенствуются незначительно. В настоящее время начинается процесс усиленной интерактивизации визуального контента и адаптации существующих технологий и интерфейсов устройств просмотра (например, телевизионных пультов, сенсорных экранов смартфонов и т. п.) к интерактивному контенту. Исследование интерактивных технологий и интерфейсов, с помощью которых человек получает возможность взаимодействовать с медиаконтентом, обладает высокой актуальностью.

Под контентом в настоящей статье понимается совокупность всей информации, представленной на каком-либо ресурсе. Медиаконтент – контент, содержащий визуальную информацию. Интерактивность – понятие, раскрывающее характер и степень взаимодействия между объектами или субъектами. Также под понятием «интерактивность» понимается принцип

организации системы, при котором цель достигается информационным обменом между элементами этой системы.

По мере развития науки и техники сформировались различные технологии доставки медиаконтента потребителю. Все способы передачи визуального контента также получили и свои методы обратной связи с пользователем (интерактивности). В результате исследования технологии передачи видеоконтента были разделены на 2 вида: передача с помощью телевизионной сети и всемирной информационной компьютерной сети (интернет). Трансляция посредством ТВ сети была поделена на «классическое телевидение», не имеющее каналов обратной связи, и «интерактивное телевидение», для использования которого, помимо ТВ сигнала, необходимо соединение устройства просмотра с интернетом. Интернет-трансляции были разделены на «IPTV» и «OTT». Термин OTT означает доставку видеосигнала от провайдера контента на устройство пользователя (приставку, компьютер, мобильный телефон) по сетям передачи данных, часто без прямого контакта с оператором связи, в отличие от традиционных услуг IPTV, которые предоставляются, как правило, только через управляемую самим оператором сеть с гарантированным качеством обслуживания. В верхней части рисунка 1 схематично представлены выделенные способы передачи медиаконтента пользователю.

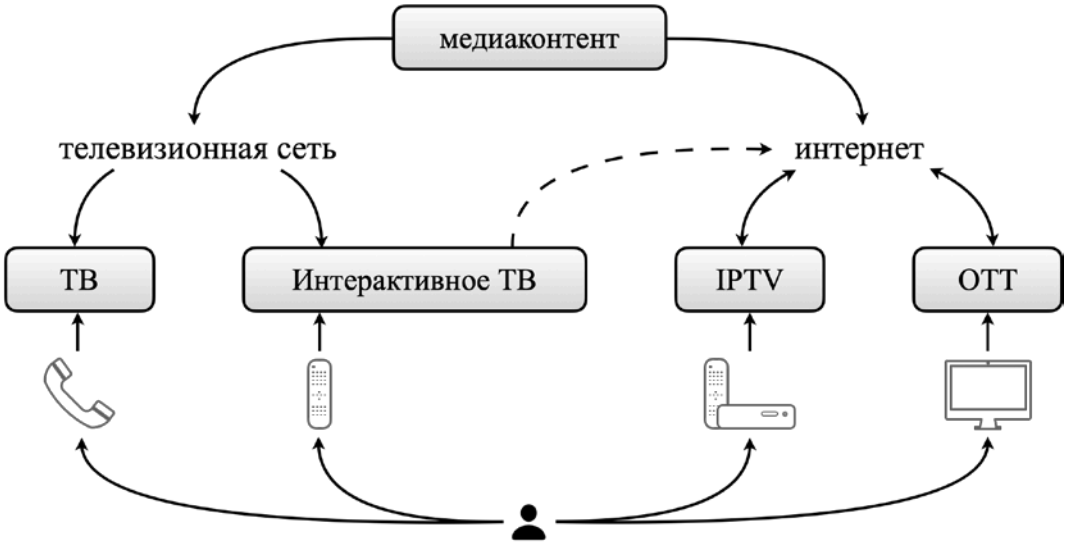


Рис. 1. Схема передачи медиаконтента

Однако интерфейс взаимодействия пользователя с интерактивными компонентами медиаконтента различается в зависимости от способа передачи сигнала. Рассмотрим технологии интерактивизации визуального контента при каждом способе передачи.

«Классическое» телевидение (ТВ) представляет собой технологию, предназначенную для передачи на расстояние движущегося изображения [1]. Из-за отсутствия технологий обратной связи для взаимодействия с контентом пользователю приходится совершать звонки в телевизионную студию, пользоваться почтой, смс-голосованием и т. п.

Интерактивное телевидение – технология, предназначенная для передачи на расстояние медиаконтента, однако, в отличие от «классического» ТВ технология имеет каналы обратной связи и может отправлять, принимать и визуализировать информацию, полученную из интернета. Самыми популярными на данный момент технологиями интерактивизации видеоконтента, используемыми в интерактивном ТВ, можно назвать системы: Ceefax/Teletext, HbbTV, BBC RedButton+. Технология HbbTV работает следующим образом: в определённое время эфира шоу на экране ТВ появляется оповещение с призывом нажать на определённую кнопку телевизионного пульта и совершить интерактивное действие. Навигация по интерактивным элементам происходит также при помощи пульта. Выбор телезрителей может непосредственно влиять на сюжет программ. Например, пользователь может сделать прогноз или проголосовать за любимого участника ТВ шоу, ответить на те же вопросы, что и участники шоу, узнать новости вне зависимости от транслируемой телевизионной программы. Пример реализации технологии представлен на рисунке 2: во время шоу в определённый момент всплывает баннер с предложением нажать красную кнопку на пульте, после нажатия на которую открывается страница голосования. Также телеканал может показывать рекламу, интегрированную в телевизионный контент. Например, во время просмотра трейлера нового кинофильма по телевизору пользователь может открыть интерактивное окно и приобрести билет в кино со скидкой [2].

Рис. 2. Пример реализации технологии HbbTV (пользовательский интерфейс)

IPTV (Internet Protocol Television) – технология (стандарт) передачи медиаданных через защищённую управляемую сеть, контролируемую операторами цифрового кабельного телевидения, по протоколу IP. IPTV существенно отличается от «классического» и интерактивного телевидения. Во-

первых, потребитель IP-телевидения запрашивает и получает медиаконтент через интернет-протокол (IP), то есть через обычный интернет кабель, а не через ТВ кабель или спутник. Во-вторых, в отличие от предыдущих видов передачи, где контент транслируется в режиме реального времени, при передаче через IPTV есть возможность хранить контент на серверах передающей стороны, что позволяет пользователям запрашивать контент через интернет в любое время [3]. Использование IPTV больше похоже на просмотр видео в интернете, чем на просмотр традиционных ТВ каналов. Отличительной особенностью IPTV стала возможность просмотра телепрограмм с любого мобильного устройства: планшет, смартфон, ноутбук. Однако просмотр IPTV через телевизор возможен только через устройство, поддерживающее стандарт Smart TV, либо через телевизионную приставку, подключаемую к телевизору.

Помимо передачи телевизионных каналов и интерактивизации медиаконтента с помощью звонков пользователей в студию, смс-голосования и пр., IPTV предлагает следующие интерактивные услуги:

1. Video on Demand (видео по запросу – VoD) – технология, позволяющая пользователю смотреть телевизионные программы на экране телевизора или другого устройства. С помощью VoD пользователь может сразу выбрать любимую программу или фильм. Эта технология передаёт содержимое с помощью телеприставки, компьютера или других устройств в режиме реального времени и загружает телевизионные программы, которые можно просматривать позже. Также существуют расширения технологии VoD: True VoD и Near Video on Demand (NVoD). True VoD – особый тип видео по запросу, где каждый пользователь может получить отдельный видеопоток, который находится под их контролем. Пользователи могут запускать, останавливать, делать паузы и пересылать содержимое видео. NVoD похож на True VoD, но в этом случае зрители не имеют никакого контроля над отдельным видеопотоком [3].

2. Time-shifted TV (сдвинутое по времени телевидение) – технология для просмотра прямых трансляций позже по времени. Пользователи могут воспроизводить и возобновлять трансляции по своему усмотрению. Опция перемотки также предоставляется для телевизионных программ.

3. TV on Demand (телевидение по запросу – TVoD) – технология, позволяющая записывать выбранные телевизионные каналы и программы для их дальнейшего просмотра в удобное время.

OTT (Over The Top Technology) – технология передачи на расстояние медиаданных через глобальную телекоммуникационную сеть (интернет). OTT телевидение позволяет смотреть телеканалы, отдельные фильмы или программы через интернет по протоколу HTTP на любом удобном устройстве без привязки к интернет-провайдеру. OTT даёт возможность использо-

вать такие интерактивные функции, как: видео по запросу, отложенный просмотр, а также возможность вещания через мобильные устройства и гаджеты [4]. Мировыми лидерами в области OTT телевидения являются Netflix, Disney+, Amazon Prime Video и прочие видеохостинги.

В OTT TV реализованы интерактивные услуги IPTV, стремительно развиваются онлайн-сервисы (QR-коды и машинное зрение, открытые и закрытые опросы, возможность выбора реакции на медиаконтент и пр.), а также добавляется поддержка дополненной реальности (AR), т. е. пользователь может взаимодействовать с виртуальными объектами (например, прикоснуться на экране планшета к изображению щенка и увидеть, как он завиляет хвостом в ответ) и т. п. [5]. Вариантов применения интерактивных элементов в дополненной реальности огромное множество.

Таким образом, можно сделать вывод, что технология OTT менее требовательна к оборудованию и программному обеспечению и не зависит от материальной базы интернет-провайдера, как это происходит при использовании IPTV. Гибкость алгоритмов трафика также выгодно выделяет OTT на фоне IPTV. Кроме того, для него характерна специальная технология, которая адаптирует сигнал к конкретной скорости интернета.

Разные подходы к реализации интерактивности при взаимодействии с медиаконтентом продиктованы закономерными процессами исторического развития науки. Различные технологии взаимодействия с медиаконтентом создают уникальные сценарии взаимодействия с каждым конкретным устройством (смартфон, планшет, телевизор, «умный» экран и пр.) и технологией (HbbTV, VoD, OTT и пр.). Следовательно, интерфейс взаимодействия с каждым устройством, в том числе пользовательский, различается. Ниже представлены разработанные требования к универсальному интерфейсу взаимодействия с интерактивным контентом, позволяющие упростить и качественно улучшить пользовательский опыт.

Универсальный интерфейс взаимодействия человека с интерактивным контентом должен: быть независимым от оператора сети, иметь модули подключения к популярным интернет-платформам, персонифицировать интерактивную рекламу. Система должна иметь функционал: участия в опросах, голосованиях, телевикторинах; активации заказа товаров во время его рекламы; активации перехода на сторонние ресурсы по желанию пользователя; оценивания просматриваемого контента и возможности им длиться в социальных сетях; записи трансляций и просмотра контента по запросу; выбора дополнительных ракурсов просмотра и получения дополнительной информации о контенте; а также иметь одинаковые пользовательские сценарии взаимодействия на разных устройствах.

Список используемых источников

1. Телевидение // Wikipedia. URL: https://ru.wikipedia.org/wiki/Телевидение (дата обращения: 10.02.2022).

2. Технологии HBB TV на Smarty Middleware // Microimpuls. Комплексные решения для OTT и IPTV. URL: https://www.microimpuls.com/hbbtv-with-smarty.html (дата обращения: 11.02.2022).

3. IPTV // Энциклопедия Lanmarket. URL: https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/iptv.html (дата обращения: 10.02.2022).

4. Различие между OTT и IPTV телевидением // Gadgetstyle. URL: https://www.gadgetstyle.com.ua/ 49885-ott-vs-iptv-features-overview/ (дата обращения: 12.02.2022).

5. Недяк А. В., Рудзейт О. Ю., Зайнетдинов А. Р. Внедрение технологий дополненной реальности в информационную систему предприятия // Отходы и ресурсы. 2020. Т. 7. № 2. С. 7.

УДК 004.427
ГРНТИ 20.53.21

УНИВЕРСАЛЬНЫЙ ФАЙЛОВЫЙ ИНТЕРФЕЙС К СИСТЕМЕ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

Д. А. Ермолаев, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлен обзор систем обмена мгновенными сообщениями с несовместимыми интерфейсами доступа, затронуты сложности создания агрегатора этих систем. Разработка единого интерфейса доступа позволит абстрагировать эти несовместимые интерфейсы для конечного программиста и упростить создание программ доступа к системам обмена мгновенными сообщениями. Описана концепция систем обмена мгновенными сообщениями, которые имеет иерархическую структуру, что обуславливает выбор интерфейса иерархической файловой системы в качестве универсального интерфейса к таким продуктам. Проведён анализ структуры систем обмена мгновенными сообщениями и предложена организация универсального файлового интерфейса к ним.

мгновенное сообщение, интерфейс, контейнер, программирование.

Одним из основных способов общения в глобальной сети Интернет на сегодняшний день являются системы обмена мгновенными сообщениями. Эти системы, несмотря на свою принципиальную схожесть, зачастую используют несовместимые форматы сообщений и протоколы обмена сообще-

ниями. Каждая система предоставляет одну или несколько реализаций клиентского приложения, способных работать только с данной системой. Такое положение дел приводит к необходимости использования нескольких приложений, предоставляющих одинаковый или почти одинаковый набор функций [1].

Для решения данной проблемы возможно использовать два подхода: синхронизацию сообщений между несколькими системами для использования их при помощи клиента одной из систем либо создание нового клиентского приложения, способного взаимодействовать с несколькими системами. При использовании любого из вышеупомянутых подходов разработчику приложения приходится решать задачу интеграции нескольких сервисов. Важно при этом обеспечить расширяемость системы, так как список систем обмена мгновенными сообщениями не ограничен. Наиболее простым решением для расширяемости приложения является вынесение кода, отвечающего за взаимодействие с системой, в отдельный модуль. Такой модуль должен предоставлять единообразный интерфейс доступа к системе и абстрагировать логику приложения от неё. Предметом данной статьи является описание такого интерфейса.

Всякая система обмена мгновенными сообщениями организует их в иерархическую структуру. В любой конкретной системе каждый уровень может носить своё особое название. Так, в системе Discord (рис. 1) эти уровни называются «серверами», «каналами» и «ветками»; в системе Telegram – «беседы» и т. д. [2]. В обобщённом виде такой уровень будет именоваться «контейнером». Каждый контейнер может содержать в себе сообщения и/или контейнеры более низкого уровня [3].

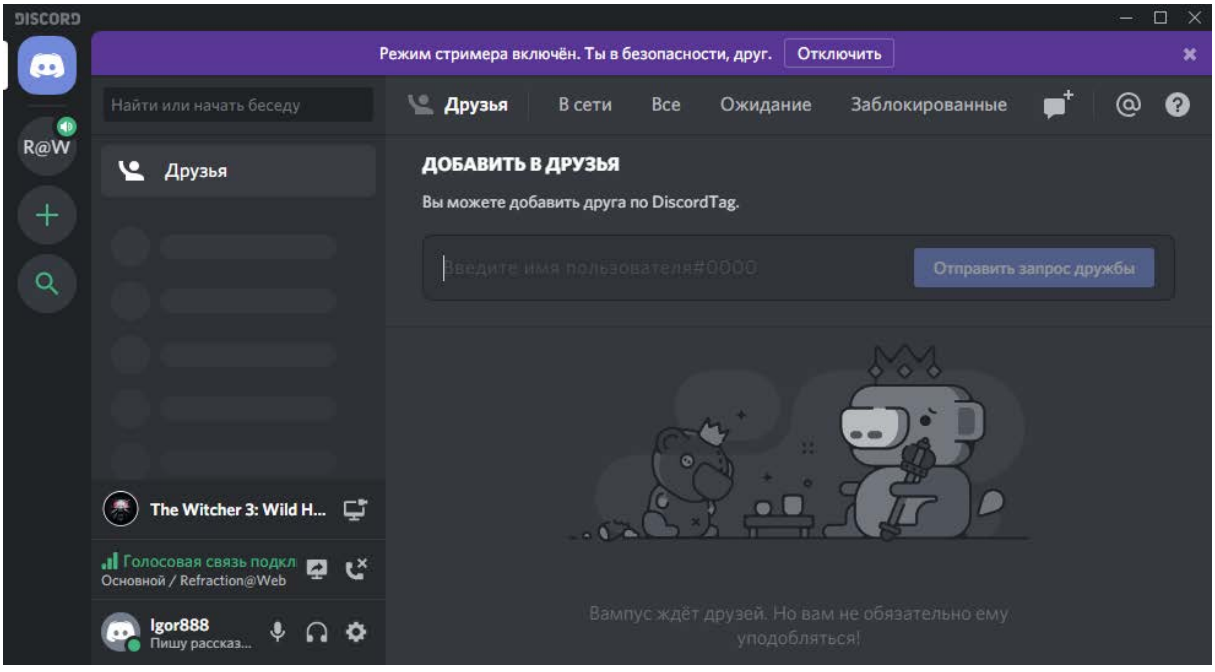


Рис. 1. Интерфейс Discord.

Сообщения системы обмена мгновенными сообщениями могут содержать в себе текст, вложения и метаинформацию. Вложения могут быть сформированы ссылками, размещёнными в тексте, или быть специальными вложениями системы. Пусть текст и вложения рассматриваются как однотипные «части» сообщения.

В рамках любого контейнера обмениваются сообщениями несколько пользователей. Всякое сообщение имеет автором одного из этих пользователей. Некоторые части сообщений также могут иметь авторов. В системе также хранятся некоторые данные пользователей, такие как уникальный идентификатор пользователя, имя пользователя, статус, дополнительная информация.

Для единообразного представления этой структуры в целях применения с любыми языками программирования возможно использовать файловый интерфейс. Такой интерфейс реализуется специальной программой – сервером виртуальных файлов, который позволяет отобразить свою иерархию файлов в пространство имён клиентского процесса. При обращении к файлам, предоставляемым этим сервером, последний осуществляет некоторые внутренние процессы и возвращает в ответ на обращение данные. Поскольку процедуры для обработки файлов присутствуют в любом языке программирования, файловый интерфейс обеспечивает языконезависимое межпроцессное взаимодействие [4, 5].

Основу файлового интерфейса должна составить иерархия системы обмена мгновенными сообщениями. Естественно представление иерархии контейнеров в виде вложенных директорий. Каждый уровень вложенности контейнера соответствует одному из уровней вложенности директорий. Внутри каждого контейнера располагаются другие контейнеры, сообщения и служебные файлы и директории. Для всех директорий должна быть предусмотрена специальная схема именования, позволяющая отличать их друг от друга.

Каждое сообщение должно представляться директорией, содержащей в себе части сообщения и служебные файлы и директории. Части представляются в виде директорий, содержащих файл, представляющий поток данных части, и служебные файлы. В сообщениях и частях автор представляется служебной директорией, содержащей информацию о пользователе.

Пользователи в каждом контейнере содержатся в служебной директории, в которую вложены директории, содержащие информацию о пользователе. В каждой такой директории содержатся местное имя пользователя (которое может отличаться от глобального), аватар пользователя, статусная информация.

Для особого именования директорий в рамках файлового интерфейса можно использовать различные подходы. Наиболее простым способом яв-

ляется именование основных директорий иерархии – контейнеров, сообщений, пользователей, частей – именем, состоящим из наименования уровня вложенности в системе и, через точку, уникальным в рамках своего контейнера идентификатором. Специальные директории при таком подходе можно назвать именем, не содержащим точку.

Схематически приведённая выше структура отображена на рис. 2.

Такая структура обеспечит простой поиск по файловой системе стандартными инструментами операционной системы. Реализация межпроцессного взаимодействия между модулями приложения позволит создавать эти модули с использованием любых языков программирования и библиотек, не привязывая их к используемому основным приложением функционалу. Такой подход естественным образом упростит расширение системы новыми модулями при появлении новых систем обмена мгновенными сообщениями и позволит заниматься разработкой таких модулей широкому кругу разработчиков.

Реализация системы позволит облегчить и ускорить доступ к сервисам мгновенных сообщений, которые, в свою очередь, могут быть востребованы как для личного общения, так и для решения бизнес-задач.

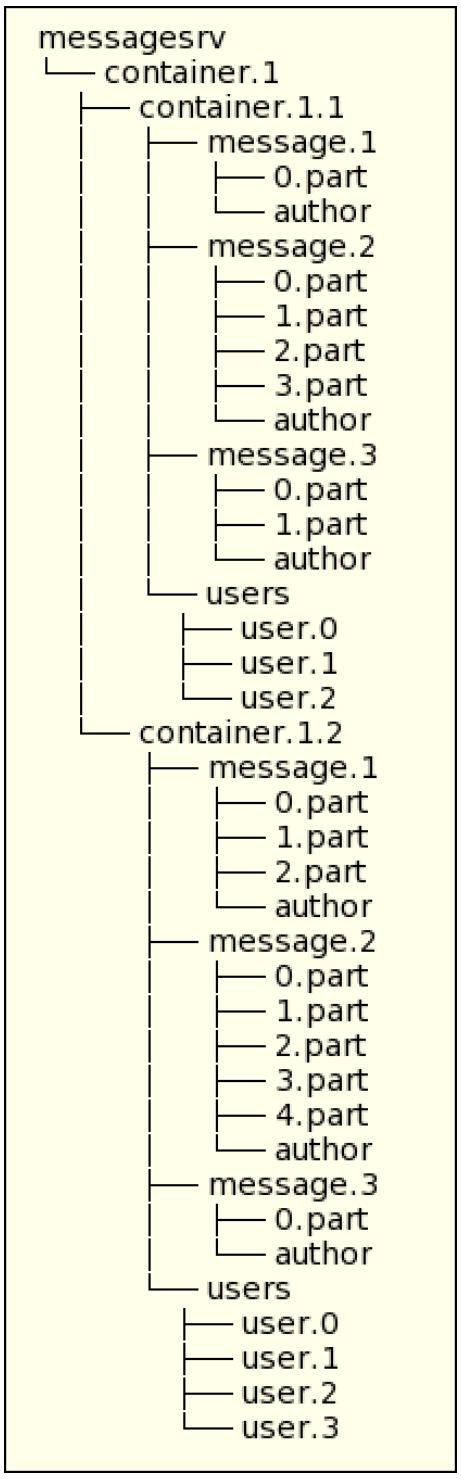


Рис. 2. Схематическое изображение иерархии файлового интерфейса

Список используемых источников

1. Макаров Д. Г., Тимофеева Д. А. Мессенджеры как система мгновенного обмена сообщений // Актуальные научные исследования в современном мире. 2020. N 11-2 (67). С. 47–49.

2. Alex G. Discord – что это и как пользоваться? Обзор программы. URL: https://4gconnect.ru/discord-chto-eto (дата обращения: 30.03.2022).

3. Положий Г. А., Тосунова А. Р., Сафарьян О.А., Черкесова Л.В. Сравнительный анализ систем обмена мгновенными сообщениями // Молодой исследователь Дона. 2020. N 4 (25). С. 59–63.

4. Pike R., Presotto D., Thompson K., Trickey H. Designing Plan 9 // Dr. Dobb's Journal Volume 16 Issue 1 Jan. 1991. pp. 49–60.

5. Killian T. J. «Processes as Files» // USENIX Summer Conference Proceedings. Salt Lake City, Utah, 1984.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.89
ГРНТИ 28.23.37

СИСТЕМА АВТОМАТИЧЕСКОЙ РАЗМЕТКИ АУДИОКНИГ И ДРУГИХ АУДИОДАННЫХ

К. Э. Есалов[1], А. С. Попонин[1], И. И. Триандафилиди[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения

В настоящее время огромную популярность приобрели аудиокниги и аудиоподкасты, что дает возможность собрать аудиоданные для обучения нейронных сетей. Такие данные отлично подойдут для обучения нейронных сетей, связанных с задачей автоматического распознавания речи и синтеза речи. В данной работе описано, как малыми силами можно создать систему автоматической разметки аудиокниг или аудиоподкастов.

ИИ, нейронные сети, обработка естественной речи, нейрокогнитивные архитектуры.

1 Введение

В настоящее время огромную популярность приобрели аудиокниги и аудиоподкасты, что дает возможность собрать аудиоданные для обучения нейронных сетей. Такие данные отлично подойдут для обучения нейронных сетей, связанных с задачей автоматического распознавания речи и синтеза речи. В данной работе описано, как малыми силами можно создать систему автоматической разметки аудиокниг или аудиоподкастов.

2 Архитектура системы

Идеальным решением при проектировании системы автоматической разметки аудиоданных будет пайплайн, состоящий из *VAD (Voice Active Detection), ASR (Automatic Speech Recognition) и AudioTagging моделей.*

3 VAD

Для реализации рассматриваемой задачи прежде всего необходимо получить возможность извлекать из входного аудиопотока речь, отбрасывая компоненты к ней не относящиеся. Таковыми могут быть затяжные паузы, фоновые шумы, смех, кашель и т. д.

Для обучения *VAD* модели обучающие данные должны включать в себя как минимум два класса: речь и не-речь. Общее количество данных небольшое, около 15–20 часов. Однако в результате проведенных экспериментов было выявлено, что деления на 2 класса недостаточно, процент ошибки у модели весьма высок. В связи с чем было принято решение сформировать три класса данных: *Speech, background noise, silence*. Пример анализа аудиофрагментов представлен на рис. 1.

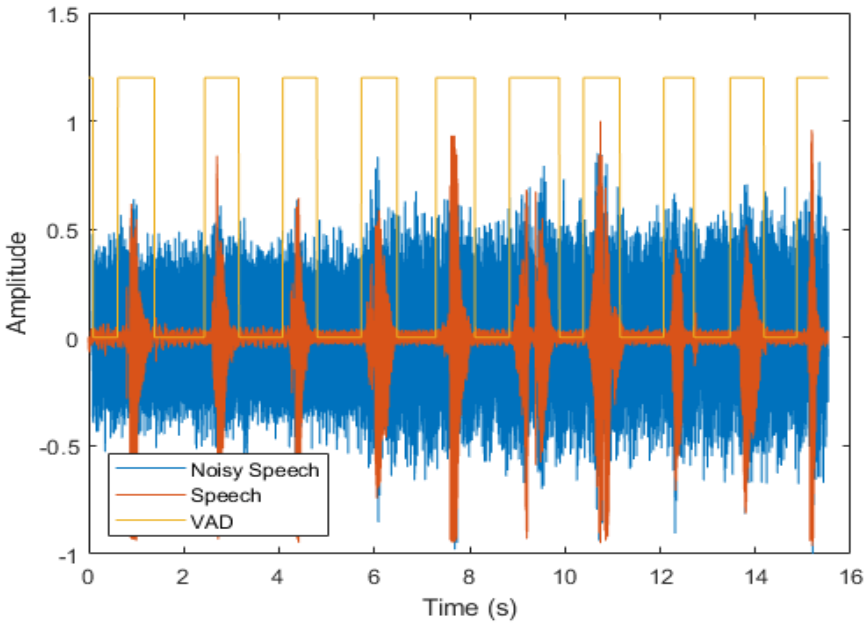


Рис. 1. Пример работы VAD модели

Класс «*Speech*» содержит почти беспрерывную речь, максимально допустимая пауза между словами – 50 мс. Данный шаг направлен на максимальное сокращение несоответствия между названием класса и его содержимым.

Класс «background noise» содержит различные звуки, которые встречаются в аудиоданных помимо речи: помехи, шум окружающей среды, артефакты речи, такие как кашель, чихание, свист и т. д.

Класс «*Silence*» содержит данные из двух других классов, которые были сильно занижены по уровню громкости. Данное решение объясняется тем, что в реальных условиях тишина не бывает идеально тихой, фоновые шумы есть, но не ярко выраженные.

Так как на вход данной модели решено было подавать аудио длительностью 100 мс, то и обучающая выборка также была сформирована из семплов по 100 мс.

По итогу мы получаем отфильтрованный набор данных, состоящий из речи. Следующим шагом для успешного выполнения поставленной задачи является формирование субтитров к этим данным.

Результатом работы *VAD* модели являются выявленные промежутки времени, в которых была обнаружена речь.

4 ASR

Следующим элементом системы является *ASR*. Данный модуль предназначен для распознавания текста в аудиофрагментах, которые мы получили из модуля *VAD*.

Нейроакустическая модель является главным элементом. Без нее невозможно построить систему ASR. К обучению модели стоит подойти основательно, ведь от того, как хорошо обучится модель, будет зависеть результат системы в целом. Для успешного обучения модели придется соблюсти несколько условий.

4.1 Качество данных

Для того чтобы качественно обучить модель, нужно внимательно подойти к данным. Самым важным критерием качественных данных служит полное соответствие текстовой транскрипцией аудиофайла с фактическим текстом, произносимым в аудиофайле. Другим важным фактором является само качество аудиофайла. В лучшем случае это один спикер, который говорит речь, совпадающую с текстовой транскрипцией. В аудиосигнале крайне нежелательно наличие двух и более спикеров, которые говорят одновременно в момент времени, даже с учетом того, что текстовая транскрипция будет совпадать в реальной речью, так как нейроакустическая модель учится предсказывать символ «с» в момент времени P(t).

4.2 Объем данных

Для того, чтобы получить качественную модель потребуется большой объем данных. В одной из работ[1] обращают внимание на важность количества данных, авторы использовали в своей работе 11 940 часов размеченной речи. Собрать такой большой датасет в условиях, когда нет доступа к корпоративным данным, практически невозможно. К этому прибавляется еще и сложность ручной разметки. На 1 час разметки может понадобиться от 2 до 10 часов труда разметчика (влияют специфичность доменов, например медицинский, или наличие / отсутствие инструментов разметки сырых данных, например другая ASR система). Однако в данное время ведутся

научно-исследовательские работы, которые предполагают, что для получения качественной модели можно обойтись 1, 10, 100 часам размеченных данных. В статье про Wav2Vec2.0[2] авторы приводят результаты, демонстрирующие успешность гипотез по использованию малого объема данных.

5 AudioTagging

Данная модель помогает проанализировать качество получившего аудиофрагмента на наличие посторонних шумов.

Пример работы модели представлен на рис. 2.

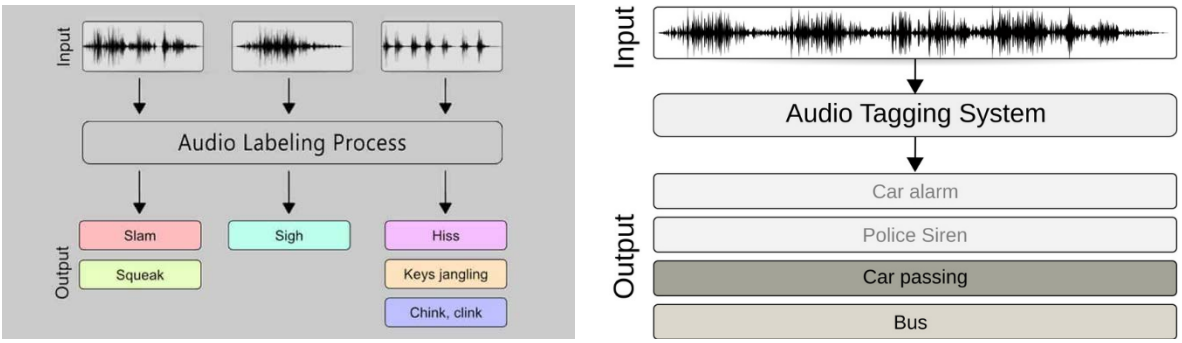


Рис. 2. Пример работы модели AudioTagging

5 Результаты

Благодаря разработанному инструменту нам удалось разметить несколько аудиокниг двух авторов. Для первого автора получилось извлечь 24 часа полезных данных из 50, для второго автора удалось извлечь 42 часа полезных данных из 79.

Используя эти данные нам удалось так же обучить модель синтеза речи. Качество модели мы оценивали с использованиям MOS [3] метрики.

Для первого автора метрика равняется – 3,9.

Для второго створа метрика равняется – 4.2.

6 Заключение

В данной работе было описано, как можно создать работающую систему автоматической разметки аудиоданных. Несмотря на то, что для достижения поставленной задачи необходимо обучить несколько нейронных моделей, описанный метод весьма универсален.

Список используемых источников

1. Dario Amodei, Rishita Anubhai, Eric Battenberg, Carl Case, Jared Casper, Bryan Catanzaro, Jingdong Chen, Mike Chrzanowski, Adam Coates, Greg Diamos, Erich Elsen, Jesse Engel, Linxi Fan, Christopher Fougner, Tony Han,Awni Hannun, Billy Jun, Patrick LeGresley, Libby Lin, Sharan Narang, Andrew Ng, Sherjil Ozair, Ryan Prenger, Jonathan Raiman, Sanjeev Satheesh, David Seetapun, Shubho Sengupta, Yi Wang, Zhiqian Wang, Chong Wang, Bo Xiao,

Dani Yogatama, Jun Zhan, Zhenyao Zhu «Deep Speech 2: End-to-End Speech Recognition in English and Mandarin. URL : https:// arxiv.org/abs/1512.02595

2. Alexei Baevski, Henry Zhou, Abdelrahman Mohamed, Michael Auli «wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations». URL : https://arxiv.org/abs/2006.11477

3. MOS metric. URL : https://en.wikipedia.org/wiki/Mean_opinion_score

Статья представлена
директором НИИ «Технологии связи», доцентом кафедры ИКС СПбГУТ,
кандидатом технических наук, доцентом Елагиным В. С.

УДК 004.4
ГРНТИ 20.53.19

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ВЕРИФИКАЦИИ QR-КОДОВ СЕРТИФИКАТОВ ВАКЦИНАЦИИ

И. А. Залесский, Ю. В. Денисова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В атмосфере продолжающейся пандемии в Российской Федерации принимается ряд постановлений, посвящённых требованиям к созданию пропускного режима в определённые категории общественных мест и транспорта. Пропускной режим предполагает использование двумерных штриховых кодов (QR-кодов) в качестве основной документации для основания наличия права на допуск. Из-за этого возросла потребность в наличии информационной системы, которая могла бы проводить верификацию предъявляемого документа и не допускать возможности представления поддельного удостоверения. В статье представлена реализация демоверсии информационной системы, решающей поставленную проблему. Рассмотрены все возможные варианты данных, которые могут содержаться в QR-коде. Определён наиболее быстрый метод считывания данных существующего сертификата вакцинации. Выявлены преимущества над уже существующими решениями.

QR-код, данные сертификата вакцинации, JSON-объект, скорость загрузки данных.

Информационная система (ИС) должна соответствовать следующим требованиям:

- Наличие системы распознавания QR-кодов в режиме реального времени;
- Проверка содержимого QR-кода на соответствие правильному формату данных;

•Запрос и последующий вывод данных сертификата, если таковой существует;

•Контроль повторного использования одного и того же сертификата в разное время в течение определённого периода;

•Хранение истории сканирования как для подтверждённых сертификатов, так и для некорректных данных, содержащихся в QR-коде.

Средства решения задачи

В качестве платформы для реализации выбрана операционная система (ОС) Android вследствие того, что по данным компании «Statcounter» на момент декабря 2021 года устройства с ОС Android занимали более 70 % мирового рынка мобильных устройств [1]. Также, показатели, размещённые на сайте компании «Statista» позволяют сделать вывод о том, что непосредственно в России пользователи выбирают ОС Android в 80 % случаев [2]. Эта информация подтверждает обоснованность выбора ОС для реализации поставленной задачи.

В качестве технологий для разработки ИС применяется язык программирования Java и интегрированная среда разработки Android Studio.

Принцип работы ИС

ИС обрабатывает получаемое с камеры изображение в режиме реального времени и при появлении в области видимости QR-кода фиксирует изображение и декодирует данные в результате чего мы получаем строку с содержимым QR-кода [3].

Поскольку единственно верный формат данных QR-кода сертификата включает в себя ссылку на портал «Госуслуг» достаточно разделить возможное содержимое на две группы: данные, содержащие ссылку на портал «Госуслуг» и все остальные данные.

Для более гибкого предполагаемого ведения статистики по использованию QR-кодов в ИС добавлена возможность проверки содержимого на факт того, является ли оно ссылкой, чтобы в последующем можно было выделить три формата данных: неправильные данные, неправильные ссылки и ссылки определённого формата, ведущие на портал «Госуслуг».

В процессе выполнения работы было выявлено, что валидные ссылки на сертификаты имеют доменное имя «gosuslugi.ru», причём единый формат обязательно включает в себя также и приставку «www.». Но для подтверждения того, что ссылка ведёт на сертификат, необходимо также проверять и путь, содержащийся в ссылке. Ссылки правильного формата могут иметь один из трёх путей:

– /covid-cert/verify/********** (где * – это цифры номера сертификата);

– /vaccine/cert/verify//********** (где * – это данные некого хэш-кода);

– /covid-cert/status/********** (где * – это данные некого хэш-кода).

Только при факте соответствия доменному имени и одному из путей ссылка считается правильной, и ИС выполняет дальнейшие действия по поиску информации о сертификате.

После проверки декодированной строки, содержавшейся в QR-коде, в том случае, если данные удовлетворяют поставленным условиям, исходная ссылка преобразуется и производится HTTP-запрос методом GET с целью получения данных сертификата человека в формате JSON-объекта.

JSON (JavaScript Object Notation)-объект – это текстовый формат обмена данными между клиентом и сервером [4].

Полученный JSON-объект обрабатывается, и данные сертификата выводятся на экран.

Типы сертификатов, которые могут быть обработаны в ИС:

– сертификаты вакцинации;

– временные сертификаты вакцинации;

– сертификаты переболевших;

– результаты ПЦР-тестов.

Вывод данных упомянутых выше типов сертификатов представлен на рис. 1.

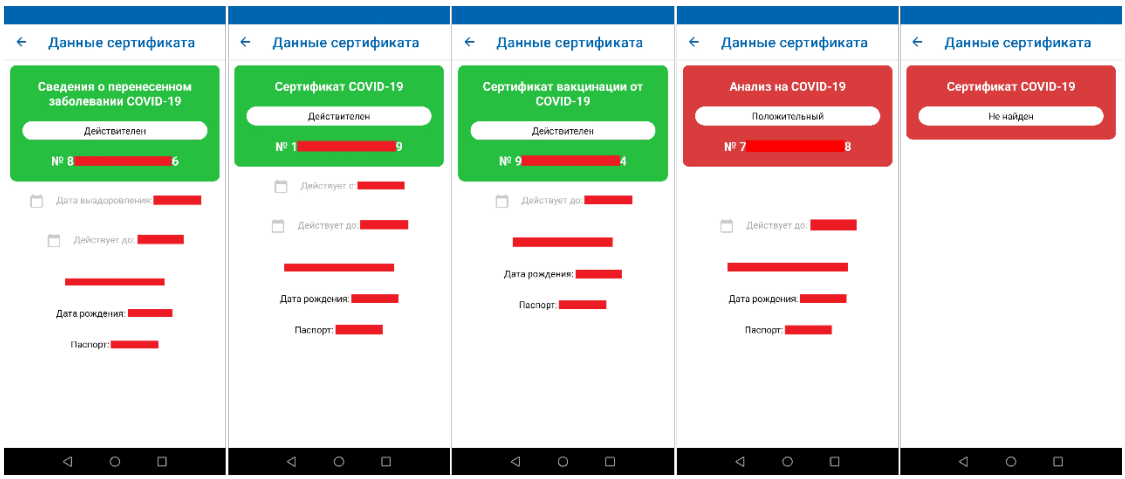


Рис. 1. Вывод данных различных типов сертификатов

Вслед за выводом данных сертификата на экран и перед их сохранением в память производится проверка на повторное использование. Если в течение последних 12 часов использовался действительный сертификат

с таким же номером, то пользователь увидит информирующее об этом сообщение на экране своего устройства с рекомендуемыми действиями (рис. 2).

В самом конце, после проверки повторного использования сертификата или после проверки содержимого на предыдущих этапах, данные сохраняются в память устройства. Для сертификатов хранится информация о них (даже для тех, данные о которых не найдена), а для невалидных данных хранится само содержимое для осуществления возможности ведения статистики в будущем.

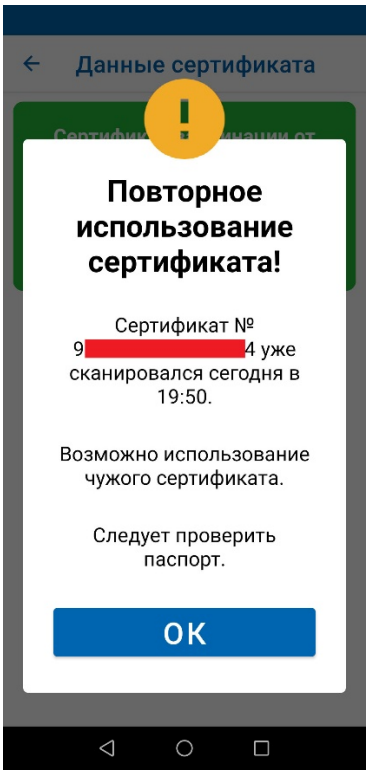


Рис. 2. Уведомление о повторном использовании сертификата

Сравнение скорость загрузки данных

Основным «конкурентом» представленной ИС является мобильное приложение «Госуслуги СТОП Коронавирус», которое также предоставляет возможность сканирования и верификации сертификатов вакцинации, но использует другой метод для вывода данных сертификата на экран.

После проверки содержимого QR-кода приложение «Госуслуги СТОП Коронавирус» осуществляет HTTP-запрос методом GET по полученной ссылке и открывает веб-страницу внутри приложения при помощи компонента интерфейса, называемого WebView в то время, как разработанная ИС производит запрос JSON-объекта и самостоятельно выводит элементы интерфейса на экран [5].

Для сравнения скорости вывода данных сертификатов на экран разными методами было проведено тестирование, в ходе которого внутри представленной ИС был сымитирован способ загрузки данных сертификата из приложения «Госуслуги СТОП Коронавирус».

В сетях с разной скоростью загрузки данных (42,42 Мбит/с и 1,88 Мбит/с) с применением двух методов были выведены данные сертификатов. После каждого из 100 повторений фиксировалась разница между временем начала HTTP-запроса и временем окончательного вывода всех данных на экран. Вслед за окончанием тестирования был произведён расчёт среднего значения времени для каждого из методов при разной скорости загрузки данных. Результаты расчётов представлены в таблице 1.

ТАБЛИЦА 1. Сравнение времени загрузки данных сертификатов с использованием разных методов

Скорость загрузки в сети, Мбит/с	Используемый метод	Среднее время загрузки данных, мс
42,42	JSON	214
	WebView	336
1,88	JSON	316
	WebView	484

Исходя из данных таблицы 1 можно сделать вывод о том, что время загрузки данных сертификатов вакцинации при разной скорости загрузки в сети в 1,5 раза меньше в случае преобразования исходной ссылки и осуществления HTTP-запроса с целью получения данных в формате JSON-объекта. Соответственно, сама по себе скорость загрузки данных сертификатов в разработанной ИС в 1,5 раза больше.

Список используемых источников

1. Mobile Operating System Market Share Worldwide. URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/2021 (дата обращения: 05.02.2022).

2. Market share held by mobile operating systems in Russia from January 2012 to December 2021 [Электронный ресурс]. URL: https://www.statista.com/statistics/262174/market-share-held-by-mobile-operating-systems-in-russia/ (дата обращения: 05.02.2022).

3. Разработка Android-приложения на Java для верификации QR-кодов сертификатов вакцинации. URL: https://habr.com/ru/post/646243/ (дата обращения: 05.02.2022).

4. Что такое JSON. URL: https://habr.com/ru/post/554274/ (дата обращения: 05.02.2022).

5. CC-QR-Scanner. Github. URL: https://github.com/Girrafeec/CC-QR-Scanner (дата обращения: 05.02.2022).

Статья представлена заведующим кафедрой БИС СПБГУТ, кандидатом технических наук, доцентом Бородянским Ю. М.

УДК 629.06
ГРНТИ 28.23.20

РОБОТОЛОГИЯ: УПРАВЛЕНИЕ СОЦИАЛЬНЫМИ СООБЩЕСТВАМИ РОБОТОВ

И. А. Зикратов[1], Т. В. Зикратова[2], В. О. Хамова[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Военный институт (Военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия»

Решение задачи оптимизации действий самоорганизующихся групп роботов приводят к попыткам использования в робототехнике механизмов управления социумами живых организмов. Сформулирована постановка задачи выбора оптимального плана группой (роем) роботов. Показаны тенденции интеллектуального управления роями, основанных на парадигме «интеллекта поведения». Проведена аналогия между социальными группами живых существ и групп роботов, которая позволила ввести новый термин для социумов роботов – роботология.

групповая робототехника; поведенческие модели; доверие; репутация; мнение; управление социумом; дестабилизирующие факторы.

В настоящее время разрабатывается большое количество теоретических моделей организации групп (роев) роботов, и методов, направленных на совершенствование качества группового управления при решении задач совместного движения, агрегации, распределения группы роботов в пространстве, совместной координации движения, коллективного картографирование и т. д. [1–4].

Известно, что управление небольшими группами роботов, состоящих из нескольких единиц, может осуществляться централизованно, с одного пункта управления. Однако такой способ неприменим, когда рой состоит из десятков, сотен или тысяч роботов (агентов). Такие рои построены в парадигме «умной пыли» (англ. smartdust) [5], когда группы состоят из самоорганизующихся агентов, обменивающиеся беспроводными сигналами и работающие как единая система.

Самоорганизующаяся мультиагентная робототехническая система (МРТС) должна быть способной вырабатывать оптимальное решение в условиях непредсказуемой (и даже враждебной) динамики внешней среды и/или недостоверной информации, поступающей от других агентов. Причины появления недостоверной информации, циркулирующей в МРТС, могут быть вызваны как естественными, так и искусственными дестабилизирующими факторами (ДФ).

К естественным ДФ относятся погодные и климатические условия, естественные препятствия и помехи, сбои и/или отказы узлов и систем робота [6].

К искусственным ДФ относятся меры противодействия рою со стороны противоборствующей стороны [7, 8].

Таким образом, в рое должна существовать некая экспертная система, которая будет выявлять влияние ДФ на поведение системы и определять тех агентов, способность которых эффективно выполнить задачу в текущих условиях обстановки вызывает сомнения [6]. Авторами предложена математическая формулировка задачи выработки оптимизационного плана в условиях ДФ в следующей нотации.

Пусть рой состоит из группы агентов $\mathbf{R}(t)$, которые в дискретные моменты времени $t = t_0, t_0 + 1, \dots, T - 1$ на основе анализа текущего состояния внешней среды $\mathbf{E}(t)$, состояния $\mathbf{S}(t)$ агентов роя вырабатывают действия $\mathbf{A}(t)$, направленные на выполнения поставленной задачи. Очевидно, что в этом случае $\mathbf{A}(t)$, вырабатываемое роботом R_i зависит от оценки этим роботом внешней среды $\hat{\mathbf{E}}(t)$. своего состояния $\hat{\mathbf{S}}(t)$ и заложенных в него критериев. Причем вырабатываемое действие может зависеть от воздействия ДФ ($\mathbf{A}(t) \simeq f(\mathbf{g}(t))$ в случае, если R_i находится в зоне воздействия ДФ, и не может способствовать приращению целевого функционала.

Следовательно, алгоритм управления роем в условиях воздействия ДФ должен выявить множество агентов $\mathbf{r}'(t)$ в наименьшей степени подверженных влиянию ДФ. Тогда совокупность генерируемых этими агентами действий $\mathbf{A}'(t)$ позволит выработать коллективное решение такое, что для всего дискретного интервала времени $t = \overline{t_0, T-1}$ значение функционала $\mathbf{Y}$ будет стремиться к экстремальным значениям:

$$\mathbf{Y} = \sum_{t=t_0}^{T-1} \mathbf{F}(\mathbf{r}'(t), \mathbf{E}(t), \mathbf{A}'(t), \mathbf{g}(t))\,\Delta t \to \mathbf{Y}^{\max(min)}, \quad (1)$$

при ограничении:

$$\mathbf{r}'(t) \in \mathbf{R}(t). \quad (2)$$

Здесь $\mathbf{g}(t)$ – вектор-функция помехи, обусловленная воздействием ДФ.
Как известно, традиционные механизмы фильтрации адресов и трафика в условиях открытой и масштабируемой МРТС не эффективны. В связи с этим наибольший интерес у исследователей вызывает концепция изучения социального взаимодействия роботов-агентов друг с другом и с окружающей средой [9, 10]. В этой концепции полагается, что «интеллект» системы формируется эмерджентно как результат индивидуального поведения и взаимодействия множества распределенных сущностей (роботов, программных агентов и т. п.) между собой и с внешней средой [11].

Для иллюстрации интеллектуальное поведение роя с использованием разработанного авторами механизма социального поведения агентов приведем простейший пример.

Пусть группа из четырех агентов R_1, R_2, R_3 и R_4 должна принять совместное решение в отношении свойств (например - цвета) объектов А и Б (рис.). При этом агенты R_1, R_2 и R_3 наблюдают объект А, агенты R_2, R_3 и R_4 наблюдают объект Б. Все агенты находятся в зоне радиосвязи друг с другом и обмениваются результатами наблюдений за объектами и агентами роя для выработки совместного решения. Пусть агент R_3 попал в зону влияния ДФ, и не может верно оценить свойства объектов А и Б, т. е. передает ошибочную информацию о цветах наблюдаемых им объектов.

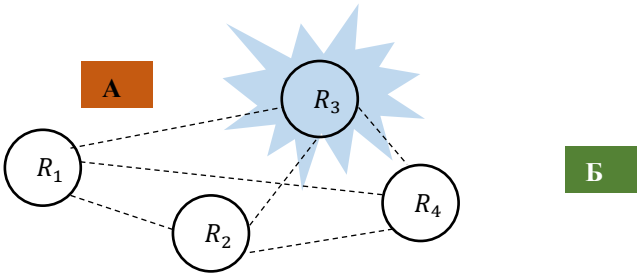


Рисунок. Группа из четырех роботов-агентов, зона ДФ и исследуемые объекты А и Б

Тогда получим следующие результаты.

1. Агенты R_1 и R_2 одинаково оценили свойства объекта А ($\hat{\mathbf{E}}_1^{\text{А}}(t) = \hat{\mathbf{E}}_2^{\text{А}}(t) = \mathbf{E}^{A}(t)$). В этом случае можно полагать, что у R_1 и R_2 возникает готовность к положительному взаимодействию друг с другом , основанная на уверенности в конструктивности такого взаимодействия. Описание подобных взаимоотношений в психологии называют *доверием*. И наоборот, если из-за влияния ДФ оценка $\hat{\mathbf{E}}_3^{\text{А}}(t)$ такая, что $\hat{\mathbf{E}}_1^{\text{А}}(t) = \hat{\mathbf{E}}_2^{\text{А}}(t) \neq \hat{\mathbf{E}}_3^{\text{А}}(t)$, то к агенту R_3 со стороны R_1 и R_2 доверия не возникает.

2. Агенты R_2 и R_4 одинаково оценили ситуацию в отношении объекта Б ($\hat{\mathbf{E}}_2^{\text{Б}}(t) = \hat{\mathbf{E}}_4^{\text{Б}}(t) = \mathbf{E}^{\text{Б}}(t)$).), и не согласны с оценкой $\hat{\mathbf{E}}_3^{\text{Б}}(t)$. Тогда результаты оценки доверия агентов друг к другу можно представить в табличном виде.

ТАБЛИЦА 1. Величины доверия агентов по результатам анализа объектов А и Б

	R_1	R_2	R_3	R_4
R_1		1	0	0
R_2	1		0	1
R_3	0	0		0
R_4	0	1	0	

Если в качестве обобщенной оценки доверия w_i i-го робота принять взвешенную сумму оценок всех агентов роя, то получим следующие результаты: $w_1^{\text{д}} = w_4^{\text{д}} = 0{,}33$, $w_2^{\text{д}} = 0{,}67$ и $w_3^{\text{д}} = 0$. Отсюда следует, что несмотря на то, что агенты R_1 и R_4 находятся вне зоны ДФ, величина доверия к ним невысока относительно доверия к агенту R_2.

3. Из таблицы 1 следует, что оценки доверия двух агентов в отношении третьего агента могут совпадать или не совпадать. Например у R_1 и R_2 одинаковое отношение к R_3 ($\hat{\mathbf{S}}_1^3(t) = \hat{\mathbf{S}}_2^3(t)$). Учитывая, что R_2 уже имеет доверие со стороны R_1, можно утверждать, что он подтвердил отношение к себе как члену коллектива, передающему достоверную информацию - выставил оценку агенту R_3 , совпадающую с оценкой от R_1. По аналогии с психологией в этом случае можно говорить о *репутации* агентов, т.е. закреплении уверенности в готовности к взаимодействию. Исходя из такого определения R_1 поставит R_2 оценку репутации 1.

4. Кроме того, принимая во внимание, что R_1 имеет доверие к R_2, можно допустить, что агент R_1 доверяет *мнению* R_2 в отношении тех объектов или агентов, которые не доступны для наблюдения самому агенту R_1. Например, R_1 не видит объект Б и поэтому не может оценить достоверность сведений об этом объекте, переданные агентом R_4, но принимая во внимание высокий уровень доверия к R_4 со стороны R_2, агент R_1 также может поставить определенную оценку агенту R_4. Учитывая, что эта оценка основана только на *мнении* соседнего агента, она может иметь меньшее количественное значение, чем оценка, основанная на данных своих сенсоров. Аналогичную оценку получит агент R_1 от R_4. Исходя из этих соображений таблица репутации примет следующий вид.

ТАБЛИЦА 2. Оценка репутации агентов
по результатам анализа таблицы доверия и мнения «доверительных» агентов

	R_1	R_2	R_3	R_4
R_1		1	0	0,5
R_2	1		0	1
R_3	0	0		0
R_4	0,5	1	0	

Тогда $w_1^{\text{Р}} = w_4^{\text{Р}} = 0{,}5, w_2^{\text{Р}} = 0{,}67, w_3^{\text{Р}} = 0$. Эти показатели с большей уверенностью позволяют выделить агентов, не находящихся под влиянием ДФ, т. к. СКО$\left(w^{\text{Р}}\right)$ < СКО$(w^{\text{Д}})$ и качество кластеризации объектов под влиянием ДФ и вне этого влияние будет выше. Учитывая что $\hat{\mathbf{E}}_1^{\text{А}}(t) = \hat{\mathbf{E}}_2^{\text{А}}(t)$ и $\hat{\mathbf{E}}_2^{\text{Б}}(t) = \hat{\mathbf{E}}_4^{\text{Б}}(t)$ можно полагать, что коллективное решение задачи агентами с высоким уровнем доверия и репутации с учетом критерия (1) и ограничений (2) найдено.

Таким образом, в работе показано, что оперируя заимствованными из социальных наук категориями *доверия, мнения и репутации* можно решать задачи коллективного управления роботами в условиях негативного воздействия внешней среды. Анализ подобных решений, опубликованных в других работах показал, что сочетание терминов «робот» и «социум» в применительно к социальной робототехнике все чаще употребляется не для описания человеко-машинного взаимодействия, а для исследования социумов роботов [10,11].

Группу роботов можно назвать социумом тогда, когда в ней появится устойчивое взаимодействие между объектов собой [11].

Очевидно, что для исключения путаницы в терминах целесообразно различать предметы исследования социальной робототехники. С этой целью для исследований, направленных на изучение социумов роботов авторами предложен новый термин – *роботология*, под которым будет пониматься отрасль знаний о совместной деятельности сообществ роботов. На наш взгляд термин отражает современные тенденции в исследовании групповой робототехники и будет способствовать интеграции методов социальных наук в мультиагентные самоорганизующиеся технические системы.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0014).

Список используемых источников

1. Trianni V., Campo A. Fundamental collective behaviors in swarm robotics // Springer Handbook of Computational Intelligence. Springer Berlin Heidelberg, 2015. С. 1377–139

2. Navarro I., Matia F. An Introduction to Swarm Robotics // ISRN Robot. Artic. ID 608164. 2013. С. 10.

3. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective // Swarm Intelligence. 2013. Vol. 7. pp. 1–41. DOI:10.1007/s11721-012-0075-2 3.

4. Зикратов И. А., Викснин И. И., Зикратова Т. В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. No 5. С. 839–849. DOI:10.17586/2226-1494-2016-16-5-839-849.

5. Michael J. Sailor and Jamie R. Link, Smart dust: nanostructured devices in a grain of sand // Chemical Communications, vol. 11, p. 1375, 2005.

6. Зикратова Т. В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021;7(3):92-100. DOI: 10.31854/1813-324X-2021-7-3-92-100.

7. Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics // International Journal on Advances in Security, Vol. 2, No. 2&3, 2009, pp. 288–297.

8. Zikratov I. A., Lebedev I. S., Kuzmich E. V., Gurtov A. V. Securing swarm intellect robots with a police office model // В сборнике: 8th IEEE International Conference on Application of Information and Communication Technologies, AICT 2014 – Conference Proceedings. 2014. С. 7035906.

9. Yogeswaran M., Ponnambalam S.G. Swarm Robotics: An Extensive Research Review // Advanced Knowledge Application in Practice, InTech, 2010. pp. 259–278.

10. Городецкий В. И. Поведенческие модели кибер-физических систем и групповое управление: основные понятия // Известия ЮФУ. Технические науки. 2019. No 1 (203). С. 144–162. DOI: 10.23683/2311-3103-2019-1-144-162 2.

11. Карпов В.Э. Социальные сообщества роботов: от реактивных к когнитивным агентам. // Мягкие измерения и вычисления. 2019. № 2 (15). С. 61–78.

УДК 004.4
ГРНТИ 81.96

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВИРТУАЛЬНОГО ПУНКТА УПРАВЛЕНИЯ

В. Г. Иванов, П. П. Корчевной, В. Е. Пестерев

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В данной статье рассказывается про виртуальный пункт управления. Описываются самый популярный метод организации безопасности сети.

метавселенная, виртуальная реальность, структура ВирПУ, система IPS, кибербезопасность, сетевое соединение.

В настоящее время IT индустрия достигла уровня, позволяющего использовать виртуальную реальность для организации цифрового рабочего места должностного лица пункта управления, который уже становится виртуальным [1], тем самым в систему управления войск уже сегодня можно ввести новый ее элемент как виртуальный пункт управления (ВирПУ).

Технологическую основу ВирПУ будет составлять высокотехнологичное оборудование, построенное на современных технологиях, можно смело говорить о возможности создании искусственного технологического виртуального пространства в целях управления войсками и оружием, которое позволяет объединить в единую платформу (среду) множество должностных лиц (персонала) и средств управления. Следовательно, система управления войсками с виртуальными элементами должна обеспечить надежное и эффективное управления подразделениями, частями, соединениями при подготовке и в ходе боя размещенных в реальном мире. При этом ВирПУ должны обладать высокой готовностью к работе, живучестью, способностью сохранять или быстро восстанавливать свою боеспособность в условиях деструктивных воздействий противника и обеспечивать возможность как централизованного, так и децентрализованного управления войсками [2]. Также позволять в виртуальном месте согласовывать все действия войск на различных уровнях управления и вести операции одновременно на суше, море, в воздухе, космосе и в киберпространстве, при этом значительно повышая скрытность и безопасность проводимых мероприятий в ходе операции. Функционирование виртуального пункта управления должно обеспечивать работу должностных лиц в соответствии с реальным пунктом управления исходя из его звена управления.

Структура должна соответствовать реальному пункту управления, его размещению на местности и оборудованию. Для обеспечения пространственного и функционального сходства необходимо создать типовую виртуальную структуру пункта управления на единой виртуальной территориальной платформе (рис.).

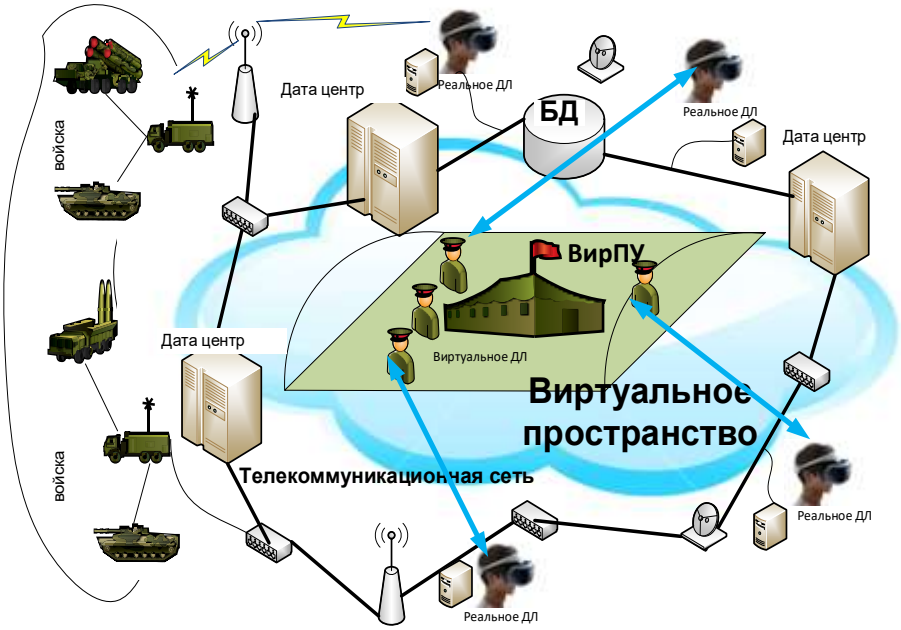


Рисунок. Структура виртуального пункта управления

Для реализации виртуального пункта управления предлагается создать следующую структуру:

1. Персональные средства виртуальной реальности, предназначенные для индивидуального использования пользователями (должностными лицами).

2. Серверы виртуальных должностных лиц, предназначенные для создания виртуальных пользователей (аватаров) и их регистрации, формирования алгоритма их действий согласно функциональных (специальных) обязанностей.

3. Полигональные и технологические серверы, предназначенные для создания виртуальных объектов (элементов) виртуального пункта управления, и обеспечения технологического взаимодействия.

4. Центр виртуальной реальности (дата центр) предназначен для формирования единого виртуального объекта (помещения), и организации взаимодействия с серверами виртуальных должностных лиц, полигональными и технологическими серверами.

5. Средства связи, каналы связи и телекоммуникационного оборудования, предназначенного для формирования единого телекоммуникационного

пространства обеспечивающее высокоскоростной обмен данными между сервером виртуального пользователя, центром и сервером виртуальной реальности с высокой степенью живучести.

Одним из важных вопросов при использовании виртуального пункта управления является обеспечение безопасности его функционирования в рамках использование ресурса телекоммуникационной сети, то есть кибервоздействия противника на Вир ПУ и его инфраструктуру [3].

По мнению авторов основной проблемой нарушения безопасности на ВирПУ будет компрометации данных. Злоумышленник получивший не санкционированный доступ к системе, получит доступ к аватару должностного лица, что обеспечит возможность кражи персональных данных пользователя (должностного лица пункта управления), позволяя ему выдать себя за ДЛ, что является угрозой шпионажа и кражи данных по средствам социальной инженерии. Так же не исключена угроза появления новых видов атак, например невидимых аватаров, делающих присутствие злоумышленника незаметным, что в свою очередь приводит к нарушению безопасности и, следовательно, к функционированию ВипПУ.

Чтобы предотвратить не санкционированный доступ противника к системе и не допустить нарушения безопасности необходимо использование системы IPS (Intrusion Prevention System) – системы предотвращения вторжений, производящей анализ трафика на основе:

сигнатур – сопоставление активности с сигнатурами уже известных угроз;

аномалий – определение подозрительной активности путем сравнения поведения отдельных элементов трафика с эталонными параметрами;

политик – мониторинг с одновременным использованием метода сигнатур и аномалий.

Не маловажную роль играет проектирование системы, от этого зависит не только уровень защищенности, но и ресурсозатратность системы, влияющая на скорость обмена данными. Так по месту размещения IPS разделяют на:

NIPS (Network Intrusion Prevention System) – устанавливается на стратегически важных элементах ВирПУ и телекоммуникационной сети, глубоко анализируя весь входящий и исходящий трафик. Но настолько тщательный анализ является крайне ресурсозатратным. В случае большой нагрузки на систему может привести систему к пропуску некоторых пакетов, что способно создать угрозу безопасности системы.

HIPS (Host-based Intrusion Prevention System) – устанавливается на отдельный хост в сети и обеспечивает только его безопасность.

NBA (Network Behavior Analysis) – занимается анализом сетевого трафика для обнаружения подозрительного трафика, отклоняющегося от уже существующей модели поведения трафика в сети.

Таким образом правильно построенная система IPS способна организовать защиту ВирПУ, как на стороне серверов, так и на стороне пользователей (должностных лиц), от большинства кибератак противника, оповещая при этом администратора сети обо всем подозрительном и откровенно опасном трафике, немедленно блокируя это трафик, согласно правилам установленным администратором пункта управления.

Принимая во внимание что, обеспечение безопасности ВирПУ будет краеугольным фактором его функционирования, то исследования и решения данных задач является уже сегодня актуальной задачей.

Список используемых источников

1. Иванова А. В. Технологии виртуальной и дополненной реальности: возможности и препятствия применения // Стратегические решения и риск-менеджмент. 2018. № 3. URL: https://doi.org/10.17747/2078-8886-2018-3-88-107

2. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи. Монография/ СПбПУ. СПб., 2018. 214 с.

3. Иванов В. Г., Филин А. В., Сарафанников В. С., Баранова А. В. Обеспечение безопасности и устойчивости управления на основе развертывания виртуальных пунктов управления // Сб. ст. II Всероссийской научно-технической конференции. ФГАУ "Военный инновационный технополис "ЭРА". Анапа, 2020. С. 263–269.

УДК 004.946
ГРНТИ 28.17.33

МЕТОДЫ АВТОМАТИЧЕСКОЙ РАССТАНОВКИ ОБЪЕКТОВ

Р. С. Иванов, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время появляется множество проектов с виртуальными мирами с целью организации социального взаимодействия и бизнес-процессов. В предложенных проектах имеется перечень проблем, усложняющих организацию рабочего виртуального пространства, что влияет на качество оптимизации. Для этого предлагается метод, позволяющий осуществить автоматическую расстановку физических объектов в пределах помещения, который позволит частично решить указанные проблемы.

автоматическая расстановка объектов, методы расстановки объектов.

В последние годы появилось множество программ для автоматического моделирования экстерьеров и фасадов зданий, автоматическая генерация реалистичных внутренних конфигураций еще не получила должного внимания. В современном мире она может использоваться как для предварительного просмотра интерьеров в помещениях, без необходимости делать специальную расстановку объектов, так и в создании внутренней среды для социальных виртуальных миров и многопользовательских онлайн-игр, которые содержат большое количество реалистичного контента окружающей среды. С ростом популярности которых всё больше необходимы автоматизированные методы для синтеза внутренней среды, так как сложно и непрактично моделировать стандартным ручным методом внутреннюю обстановку помещения. В связи с этим, автоматическая генерация моделирования обстановки окружающей среды позволяет осуществить быструю визуализацию (рендеринг) и оптимальный выбор из множества полученных вариантов обстановки будущего интерьера [1].

Важен вопрос эргономики, связанный с правильной организации пространства помещения, которое может содержать разные виды физических объектов, относящихся к интерьерам мебели. Рассмотрим критерии позволяющие оптимизировать данный процесс:

- Доступность объекта;
- Размещение предметов относительно друг друга;
- Дизайн совокупности объектов и помещения;
- Размер пространства;
- Ограничение количества объектов, относительно размеров пространства.

Например, помещение может содержать разные виды физических объектов, относящихся к интерьерам мебели. Экран телевизора или компьютера не должны загораживаться, так как эти предметы должны быть в зоне видимости. Кроме того, большинство объектов должны быть доступны для технического обслуживания человеком. Так же, одни объекты часто помещается поверх других, например, вазы на столе или навесные конструкции, поэтому между объектами может существовать связь, как родительский и дочерний объект или кухонный фурнитур.

Для автоматической расстановки предметов необходима подготовка данных конфигураций по каждому предмету. Для различных типов предметов используются шаблоны, учитывающие специфику их применений, такое как, например, свободное пространство вокруг предмета, возможные сочетания с другими предметами или применение с объектами окружения.

Для улучшения размещения необходимо выбрать тип помещения, например, кухню или гостиную. Далее добавляется необходимый набор мебели. Затем применяется метод размещения с конкретизированным подбором объектов.

Рассмотрим несколько методов организации пространства помещения и расположения предметов. В первом методе осуществляется расстановка предметов по сетке (XY). При применении данного метода конфигурации предметов ограничиваются настройками параметров, таких как зона взаимодействия с предметом и зоной с возможной постановкой объекта в фиксированных единицах. С добавлением параметра (Z) сетки можно осуществить упрощённую автоматическую расстановку мебели с объектами взаимодействия и декором. Такой метод поможет в быстром просмотре вариантов и удобен в примерном подсчёте занимаемой и свободной площади (рис.).

Второй метод размещения зависит от расположения соседних объектов и их настроек различных зон. В таком методе учитывается гораздо больше параметров и имеется больше вариантов размещения. Но увеличивается сложность используемых технологий и время работы программы. Для упрощения можно размещать не только отдельные объекты, но и готовые шаблоны фурнитура с различными вариациями.

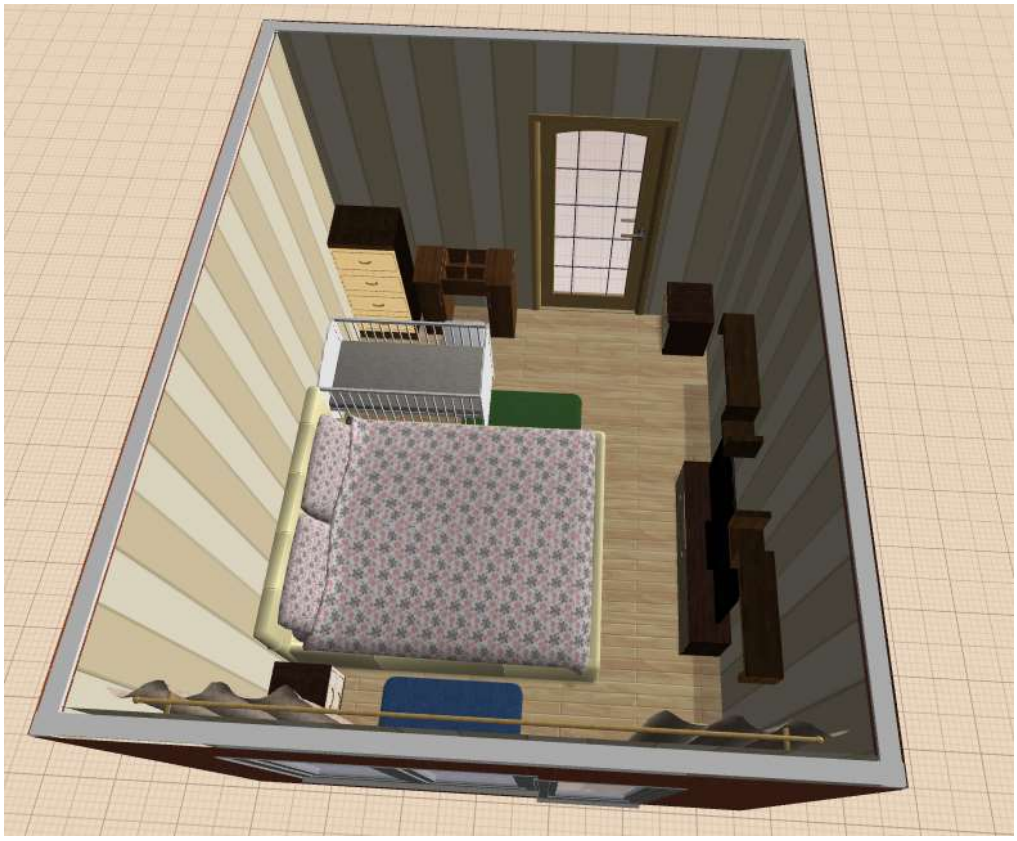


Рисунок. Пример размещения объектов по сетке

Третий метод требует обучения модели на большом объёме данных. Модель может выдавать быстрые результаты, но не учитывать многих пара-

метров из-за которых на выходе с увеличением числа размещаемых объектов увеличивается ошибка расстановки. Также предварительно требуется большая работа людей для создания обучающих данных [2].

ТАБЛИЦА 1. Таблица методов и параметров

Метод	Простота реализации	Скорость расстановки	Качество расстановки	Количество объектов
Расстановка по сетке	средняя	средняя	средняя	низкое
Размещения от соседних объектов	сложная	низкая	средняя	среднее
Обученная модель	сложная	высокая	высокая	высокое

Методы автоматического размещения объектов, зачастую специально делаться под конкретные задачи. Они могут помочь в быстром распределении и предварительном просмотре интерьеров, а также обратить внимание на интерактивные зоны.

Предлагается метод комбинации размещения объектов по сетке и относительно соседних предметов. В данном методе к размещённым на сетке (XYZ) физическим объектам автоматически добавляются соседние объекты с учётом рассмотренных критериев, что позволяет решить поставленную задачу.

Список используемых источников

1. Lap-Fai Yu, Sai-Kit Yeung, Chi-Keung Tang, Demetri Terzopoulos, Tony F. Chan, Stanley J. Osher. “Make it Home: Automatic Optimization of Furniture Arrangement” // July 2011ACM Transactions on Graphics 30(4):86. DOI:10.1145/2010324.1964981.

2. Henderson Paul, Subr Kartic, Ferrari Vittorio. “Automatic Generation of Constrained Furniture Layouts” // arXiv:1711.10939v3 [cs.CV] 24 Jan 2019.

3. Создание системы расстановки объектов по уровню при помощи редактора blueprint. 2016. URL: https://habr.com/ru/post/277515/?ysclid=l8vc4nsd2w594637645.

УДК 004.491
ГРНТИ 81.93.29

СИСТЕМА ИДЕНТИФИКАЦИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПРИЗНАКИ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ, СРЕДСТВАМИ ПРОГРАММНО-УПРАВЛЯЕМОГО БРАУЗЕРА

Н. В. Изотов, С. М. Макеев, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье приводится описание автоматизированной системы сбора и идентификации информационных материалов, содержащих признаки экстремистских материалов. Представлено описание подсистемы сбора, основанной на применении программно-управляемых браузеров, а также подсистема классификации информационных материалов на основе статистических мер TF-IDF.

сбор информации, классификация, экстремизм, программно-управляемый браузер, TF-IDF.

Одной из серьезных угроз безопасности Российской Федерации является распространение запрещенной информации, перечень которой определен статьей 10 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технология и о защите информации". К одному из классов законодательно запрещенной информации относятся материалы с экстремистской направленностью. Ответственность за ряд направлений деятельности, связанной с экстремистскими материалами, предусмотрена статьями 13.37, 20.29 Кодекса РФ об административных правонарушениях, статьей 280 Уголовного кодекса РФ.

Проблема противодействия распространению запрещенной информации заключается в необходимости решения ряда сложных задач, сложность которых связана с постоянно растущим количеством источников информации, средств распространения, средств доступа, средств обхода ограничений.

В работе рассмотрен в универсальный подход по реализации технологий доступа и сбора информации из общедоступных источников на примере социальной сети «Вконтакте», основанный на применении программно-управляемых браузеров, который интегрирован в автоматизированную систему выявления признаков экстремистских материалов.

Вопросами изучения распространения информации в социальных сетях, их мониторингом, выявлением деструктивной информации активно занимаются и в России, и за рубежом. В частности, в работах [1, 2] рассмотрены вопросы моделирования распространения информации в социальных сетях. Авторы трудов [3, 4] исследовали вопросы распространения деструктивного контента для географически ограниченной местности. Подходы по определению параметров деструктивного контента рассмотрены в работах [5, 6]. Вопросы автоматизации идентификации источников деструктивного контента исследовались авторами [7].

Также известны ряд коммерческих сервисов автоматического мониторинга общедоступной информации, таких как *Brand Analytics, YouScan*, Медиа логия, Крибрум, которые частично способны решать рассматриваемые задачи, но не обеспечивают полного цикла подготовки аналитического материала.

Проблема доступа и сбора исходных данных состоит в многообразии источников информации, протоколов доступа, форм представления материалов. В связи с чем под каждый отдельный источник информации необходима индивидуальная настройка средств сбора.

Сбор информации, публикуемой в социальной сети «Вконтакте», возможно с помощью использования стандартных протоколов доступа к веб-сайтам *http(s)* либо *API*-интерфейса. Первый способ требует реализации сложной системы обработки большого количество интерфейсов, второй – использует систему доступа к данным, в которой осуществляется фильтрация и контроль доступа, а также контроль осуществления автоматических действий (защита от ботов), поэтому оба способа обладают серьезными недостатками.

Вместе с тем, технологии автоматизированного тестирования веб-приложений дают возможность использовать в качестве средства доступа к ресурсам веб-сайта программно-управляемые браузеры. Для управления браузером используется драйверы (*Selenium, Puppeter*) и *Python*-сценарии, позволяющие задавать последовательность действий (операций) и данных, передаваемы удаленному ресурсу. Схема извлечения информации при реализации такого подхода показана на рис. 1.

Задача разработчика системы извлечения информации заключается в разработке отвечающего требованиям сценария и интерфейса к нему.

Функциональное представление процесса мониторинга социальной сети на предмет источника распространения запрещенной информации, представлено на рис. 2.

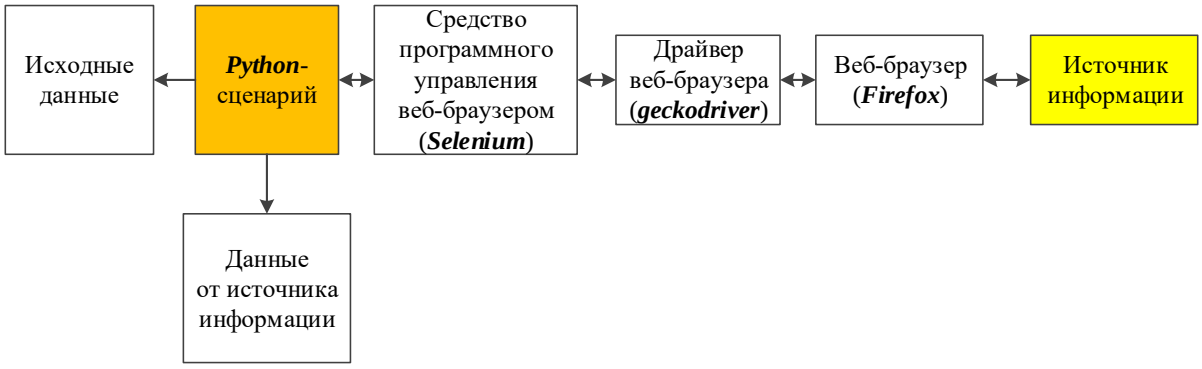


Рис. 1. Структурная схема извлечения данных из источника информации средствами программно-управляемого браузера

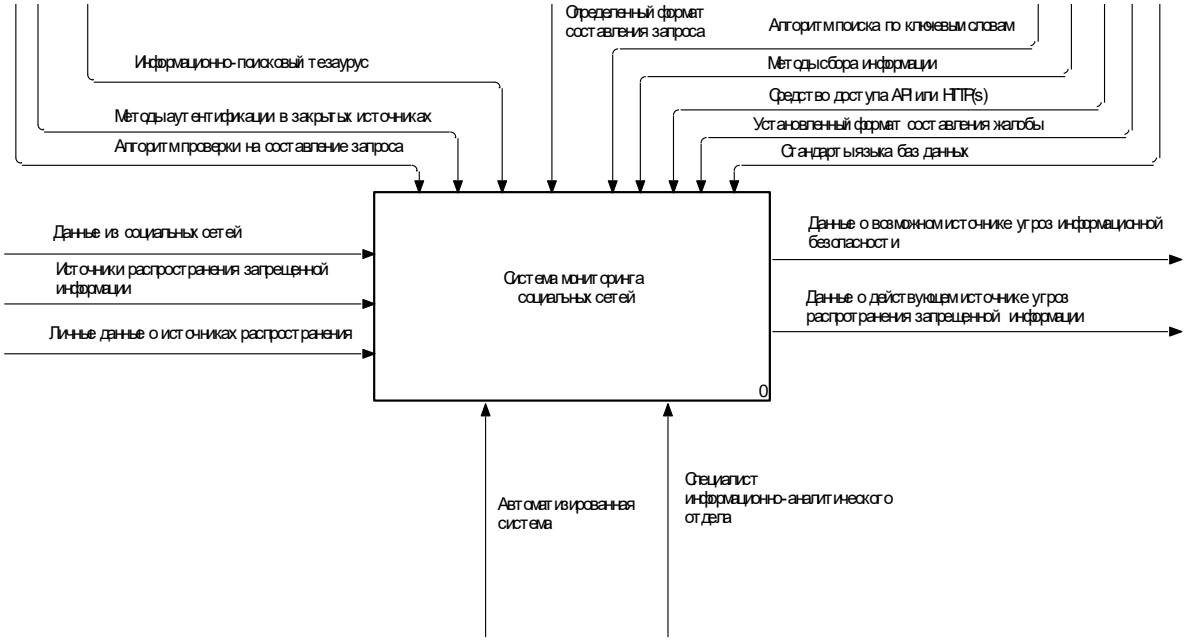


Рис. 2. Функциональное представление процесса мониторинга

Из схемы видно, что рассматриваемая система мониторинга должна учитывать большое количество исходных данных. При чем некоторые исходные данные подвержены изменениям во времени.

Полнофункциональная структурная схема системы мониторинга (свидетельство о государственной регистрации программы для ЭВМ № 2017618056) [8] показана на рис. 3.

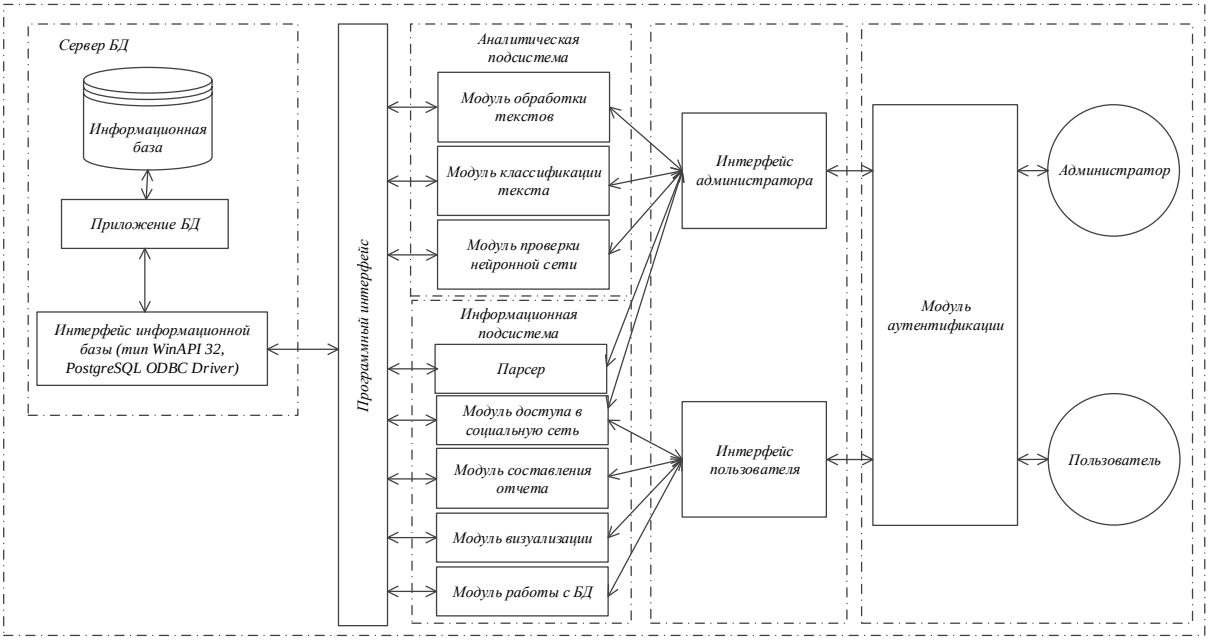


Рис. 3. Структура автоматизированной системы мониторинга

В состав автоматизированной системы мониторинга входят:

1) модули, отвечающие за реализацию функций безопасности (идентификация и аутентификация, контроль доступа, аудит событий безопасности);

2) модули, реализующие информационную подсистему (основные функции):

– доступ к источнику информации;
– синтаксический анализ (парсинг);
– подготовка отчета;
– визуализация (графический интерфейс);
– взаимодействие с системной управления базы данных;
– классификация данных;

3) модули, реализующие аналитические функции:

– обработка текста (функции компьютерной лингвистики);
– обучение сверточной нейронной сети (в разработке);
– аналитическая обработка;

4) система управления базами данных и модули, отвечающие за взаимодействие с ней.

5) подсистема управления параметрами (интерфейс администратора).

Функции аналитической обработки наиболее доступно реализовывать на базе математического аппарата статистических мер *TF-IDF* [9] при наличии тезауруса по заданной тематике.

Мера *TF* (частота слова) определяется как $tf(t,d)=\frac{n_t}{\sum_k n_k}$, где n_t – число вхождений слова *t* в документ, а в знаменателе – общее число слов в документе. Мера *IDF* (обратная частота документа) – инверсия частоты, с которой некоторое слово встречается в документах коллекции – рассчитывается как $itf(t,D)=\log\frac{|D|}{|\{d_i\in D\,|\,t_i\in d_i\}|}$, где $|D|$ – число документов в коллекции, $|\{d_i\in D\,|\,t_i\in d_i\}|$ – число документов из коллекции *D*, в которых встречается *t*, когда $n_t\neq 0$. Мера *IDF* позволяет уменьшить вес слов, которые встречаются наиболее часто. Таким образом мера *TF-IDF* определяется выражением $tf-idf(t,d,D)=tf(t,d)\times tf(t,D)$.

На основе рассчитанной меры *TF-IDF* для слов из тезауруса может быть рассчитана степень принадлежности анализируемого материала к экстремистскому, которую можно вычислить с помощью выражения аддитивной свертки, отражающий важность каждого слова и частоту его встречаемости, рассчитанную на основе меры *TF-IDF* – $F(a_{ij})=\sum_{j=1}^{n}\lambda_j\cdot a_{ij},\sum_{j=1}^{m}\lambda_j=1$, где a_{ij} – значение меры *TF-IDF* для *j*-го ключевого слова из тезауруса, а λ_j – его вес (важность).

Очевидно, что как состав тезауруса, так и веса (важность) ключевых слов, входящих в него, определяет специалист в рассматриваемой предметной области.

Результаты функционирования описываемой системы на данном этапе показывают достаточно высокий уровень ошибок 1-го рода («ложное срабатывание») – свыше 30 %, что требует высокой вовлеченности эксперта в процесс отбора материалов и совершенствования модели экстремистского материала. В связи с этим перспективным направлением рассматривается использование классификатора на основе сверточной нейронной сети. Сверточная нейронная сеть для эффективной работы требует большого объема обучающей выборки, которую планируются составить на основе работы системы, построенной на классификаторе на базе меры *tf-idf*.

Вместе с тем, представленная система мониторинга показала хорошие результаты по эффективности извлечения информационных материалов из социальной сети на базе программно-управляемого браузера, а также возможность масштабирования, тем самым задача получения достаточно надежного средства доступа и извлечения информационных материалов решена успешно.

Список используемых источников

1. Семенов И. В., Савинов Д. А., Москалева Е. А. и др. Моделирование эпидемических процессов в социальной сети медиа-контентом // Информационная безопасность. 2018. Т. 21. № 1. С. 104–109.

2. Потемкин А. В. Мониторинг информационных потоков распространения сообщений в глобальных информационных сетях Интернет // Вестник компьютерных и информационных технологий. 2015. № 10. С. 44–50.

3. Ещенко А. В., Шварцкопф Е. А., Остапенко А. Г., Степанов М. Н. Модель ареала распространения деструктивного контента в сети Facebook для интернет-пользователей Воронежской области // Информационная безопасность. 2018. Т. 21. № 2. С. 245–260.

4. Сафронова В. В., Сибирко К. В., Йири В., Белоножкин В. И., Паринова Л. И. Риск-анализ и прогнозирование ареала распространения деструктивного контента в сообществе "МДК" // Информационная безопасность. 2018. Т. 21. № 3. С. 400–407.

5. Остапенко А. Г., Кунавин В. Е., Сидельникова В. С., Остапенко О. А. Метрики деструктивного контента на видеохостинге Youtube // Информационная безопасность. 2018. Т. 21. № 3. С. 284–289.

6. Остапенко А. Г., Паринов А. В., Калашников А. О., Щербаков В. Б., Остапенко А. А. Социальные сети и деструктивный контент. Серия 3. Теория сетевых войн : монография / Воронежский государственный технический университет. Москва : Научно-техническое издательство "Горячая линия-Телеком", 2018. 276 с.

7. Ишков Д. А., Нежельский Е. Р., Степанов М. Н. Автоматизация поиска распространителей деструктивного контента в социальных сетях // Информационная безопасность. 2019. Т. 22. № 2. С. 256–259.

8. Маркин Д. О., Макеев С. М., Изотов Н. В., Андросов А. Ю. Система идентификации информационных угроз на основе открытых данных сети Интернет // Известия Тульского государственного университета. Технические науки. 2020. Выпуск 9. С. 86–94.

9. Jones, K. S. A statistical interpretation of term specificity and its application in retrival // Journal of Documentation. MCB University : MCB University Press, 2004. Vol. 60. No. 5. pp. 493–502.

УДК 004.056
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ РЕВЕРС-ИНЖИНИРИНГА МАШИННОГО КОДА

К. Е. Израилов[1, 2], **Н. Е. Романов**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Данная работа посвящена изучению возможности применения генетического алгоритма, являющегося эвристическим методом поиска, для решения задачи декомпиляции. В исследовании рассматривается общая схема работы, так называемой, генетической декомпиляции машинного кода в псевдоисходный для последующего статического анализа с целью поиска уязвимостей. Помимо этого, значительная часть работы затрагивает разбор потенциальных преимуществ и недостатков использования такого подхода в реверс-инжиниринге. В результате проделанного исследования авторами так же был сделан вывод о том, что использование предлагаемой концепции обосновано и может значительно повлиять не только на развитие реверс-инжиниринга, но и на информационную безопасность в целом.

информационная безопасность, машинный код, реверс-инжиниринг, декомпиляция, генетический алгоритм.

Введение

В настоящее время все чаще компании используют в своих системах сторонние программные обеспечения, которые в ряде случаев предоставляются без исходного кода. При таких условиях аудит с точки зрения информационной безопасности использования таких приложений усложнен (даже при их изначально безопасной разработке [1]) и приходится использовать реверс-инжиниринг, включающий в себя различного рода технологии, такие как декомпиляторы, дизассемблеры, распаковщики и отладчики.

Применение такого подхода к обеспечению безопасности используется уже давно и, как следствие, на уже имеющихся принципах оно достигло некоторого предела в развитии. Все новые решения незначительно повышают результат, и не дают качественного скачка в росте эффективности, так как не используют принципиально новых идей, а лишь улучшают имеющиеся. Тогда очевидно, что поиск новых подходов для реализации реверс-инжиниринга является безусловно актуальной задачей.

Одним из таких подходов может быть использование генетического алгоритма для декомпиляции программного обеспечения. Данный подход яв-

ляется воссозданием процессов, происходящих в живой природе: наследования, мутации, отбора и кроссинговера - в рамках восстановления исходного текста программы из ее машинного кода [2]. Применение в технических устройствах и программировании принципов живой природы уже давно существует и вносит огромный вклад в развитие науки. В качестве примера можно привести нейронные сети, которые основаны на биологической аналогии с мозгом человека. В таком случае, возможность использовать генетический алгоритм для процесса декомпиляции заслуживает дополнительных исследований, так как потенциально может значительно повлиять на развитие реверс-инжиниринга и информационную безопасность в целом.

Принцип работы

Суть алгоритма заключается в поиске такого исходного кода, который в результате компиляции будет максимально близок к заданному машинному коду, чью работу требуется проанализировать [3, 4]. Это отличает данный алгоритм от уже имеющихся, в которых машинный код преобразуется в исходный, а не наоборот [5]. Данную задачу нельзя решить перебором, особенно если исходный код очень большой, поэтому необходимы методы оптимизации, для чего и используется генетический алгоритм.

Опишем более детально процесс реализации декомпиляции, основанной на генетическом алгоритме и представленной на рисунке.

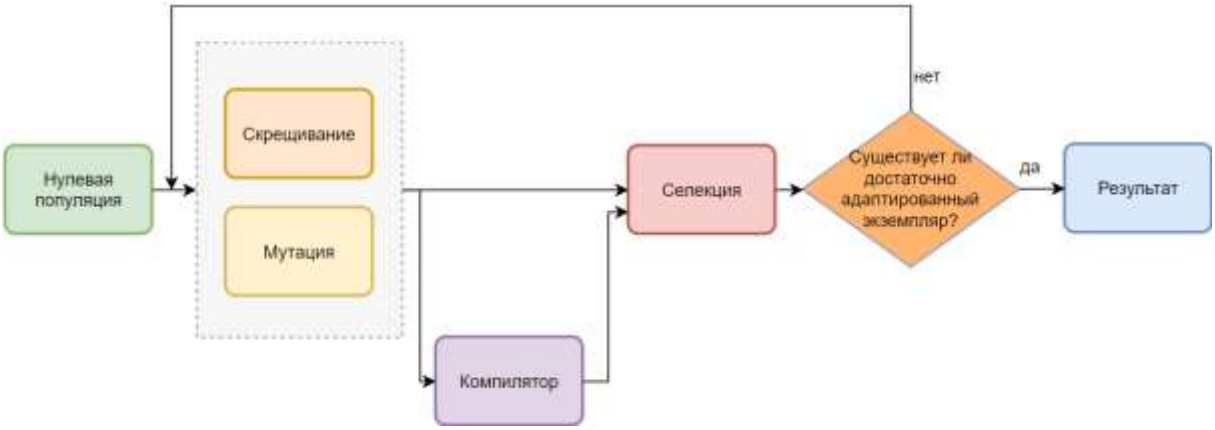


Рисунок. Структурная схема генетической декомпиляции

При запуске такого алгоритма создается первоначальная (нулевая) популяция особей, в данном случае, это определённое количество сгенерированных предполагаемых исходных кодов программ. Каждый такой исходный код будет представлять собой элемент пространства решений задачи. В качестве хромосомы особи мы считаем текст программы, написанной на высокоуровневом языке.

Далее итеративно генерируются новые поколения путем скрещивания, под которым подразумевается получение нового высокоуровневого кода из двух уже имеющихся. При этом в процессе эволюции с определённой частотой в экземплярах происходят мутации в генах – случайные изменения одной или нескольких конструкций кода, например символов. Процесс создания новых поколений будет происходить до тех пор, пока не будет найдена подходящая особь или не выполнится число заранее заданных итераций.

Затем вычисляется приспосабливаемость каждой из особей к условиям окружающей среды. В рамках задачи декомпиляции это означает определение того, насколько машинный код, скомпилированный из экземпляра популяции близок к заданному коду. Для этого используют так называемую фитнесс-функцию. Экземпляры с наилучшей приспосабливаемостью отбираются для следующего поколения (селекция).

Важно правильно разработать функцию приспосабливаемости, так как от нее во многом зависит эффективность данного алгоритма. Она может быть основана на определении подобия двух ассемблерных кодов, например, учитывать совпадение количества, состава, содержимого и порядка расположения строк. Ассемблерный код в этом случае получается практически тождественными преобразованиями из машинного.

Развитие популяции происходит за счет селекции более приспособленных особей, мутации генов и кроссинговера (перераспределения родительских генов новой особи).

Преимущества и недостатки

Одним из преимуществ такого подхода является отсутствие явной привязки к языку программирования и типу процессорных инструкций. Компилятор является внешним модулем, что также позволяет не быть зависимым от него. Так же важно отметить, что данная технология может позволить уйти от ошибок, возникающих из-за человеческого фактора при декомпиляции, проявляющегося на этапах разработки алгоритмов или постобработки результатов.

Из недостатков подхода можно выделить потребность алгоритма в мощных вычислительных ресурсах [6], так как для каждой популяции необходимо не только посчитать функцию приспосабливаемости, но и скомпилировать исходные коды в машинные. В том случае, если в популяции большое количество особей с объемными хромосомами, может потребоваться много времени для того, чтобы скомпилировать каждый исходный код в машинный, а затем посчитать фитнесс-функцию, чтобы произвести селекцию. Более того, технологии, основанные на генетических алгоритмах плохо масштабируемы. Размер области поиска решений очень велик, так как существует огромное количество комбинаций конструкций кода. В качестве решения этой проблемы можно предложить декомпозицию задач, что

уменьшит количество элементов пространства решений. К тому же генетический алгоритм имеет свойство находить не глобальный максимум, а локальный. Для решения этой проблемы есть множество способов, например, увеличение количества мутаций, использование более продуманного метода отбора для поддержания популяционного разнообразия, повторное воспроизведение алгоритма с другой начальной популяцией или другими параметрами.

Заключение

В статье был описан подход к реализации декомпиляции на основе генетического алгоритма. Исходя из анализа преимуществ и недостатков можно сделать вывод о том, что использование предлагаемой концепции обосновано и может внести большой вклад в развитие информационной безопасности, в частности реверс-инжиниринга [7–15]. Несмотря на наличие ряда недостатков, которые ограничивают реализацию генетической декомпиляции, были предложены идеи по противодействию им. Продолжением исследования должна стать детальная проработка слабых звенья для того, чтобы можно было разработать полноценное программное обеспечение по декомпиляции машинного года в исходный.

Список используемых источников

1. Романов Н. Е., Израилов К. Е., Покусов В. В. Система поддержки интеллектуального программирования: машинное обучение feat. быстрая разработка безопасных программ // Информатизация и связь. 2021. № 5. С. 7–17. DOI: 10.34219/2078-8320-2021-12-5-7-16.

2. Бочаров В. С., Отбоева С. Д. Генетические алгоритмы // Современные технологии в мировом научном пространстве. Сборник статей Международной научно-практической конференции, Уфа, 11 мая 2019. Уфа: ООО "ОМЕГА САЙНС", 2019. С. 21–26.

3. Израилов К. Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021;7(4):95-109.

4. Израилов К. Е. Применение генетических алгоритмов для декомпиляции МК // Защита информации. Инсайд. 2020. No 3(93). С. 24–30.

5. Бугеря А. Б., Ефимов В. Ю., Кулагин И. И., Падарян В. А., Соловьев М. А., Тихонов А. Ю. Программный комплекс для выявления недекларированных возможностей в условиях отсутствия исходного кода // Труды Института системного программирования РАН. 2019. Т. 31. No 6. С. 33–64.

6. Яндукова М. А., Жолондиевский Э. Р. Генетические алгоритмы и сферы их применения // Перспективы развития цифровой экономики в России и за рубежом. Сборник статей международной научно-практической конференции, Тольятти, 20 мая 2021. Тольятти: Тольяттинская академия управления, 2021. С. 130–133.

7. Буйневич М. В., Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 115–130.

8. Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 86–104.

9. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

10. Buinevich M., Izrailov K., Vladyko A. The life cycle of vulnerabilities in the representations of software for telecommunication devices // The proceedings of 18th International Conference On Advanced Communications Technology (Pyeongchang, South Korea, 2016). IEEE, 2016. PP. 430–435.

11. Buinevich M., Izrailov K., Vladyko A. Method and prototype of utility for partial recovering source code for low-level and medium-level vulnerability search // The proceedings of 18th International Conference on Advanced Communication Technology (Pyeongchang, South Korea, 2016). IEEE, 2016. pp. 700–707.

12. Buinevich M., Izrailov K., Vladyko A. Method for partial recovering source code of telecommunication devices for vulnerability search // The proceedings of 17th International Conference On Advanced Communications Technology (PyeonhChang, South Korea, 2015). IEEE, 2015. pp. 76–80.

13. Buinevich M., Izrailov K. Method and utility for recovering code algorithms of telecommunication devices for vulnerability search // The proceedings of 16th International Conference on Advanced Communication Technology (PyeonhChang, South Korea, 2014). IEEE, 2014. pp. 172–176.

14. Buinevich M., Izrailov K., Vladyko A. Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices // The proceedings of 19th International Conference on Advanced Communication Technology (Pyeongchang, South Korea, 2017). IEEE, 2017. pp. 408–414.

15. Buinevich M., Izrailov K., Vladyko A. Metric of vulnerability at the base of the life cycle of software representations // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. pp. 1–8.

УДК 621.004
ГРНТИ 49.33.29

К ВОПРОСУ О КОНТРОЛЕ ЦЕЛОСТНОСТИ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Для решения задачи контроля целостности инструментарий операционной системы Astra Linux SE расширен комплексом средств защиты, который реализует функции управления целостностью данных. Этот комплекс позволяет контролировать как

целостность данных, так и содержимое исполняемых файлов, что позволяет с высокой вероятностью установить факт отсутствия в ОС данных и функций, обладающих недекларируемыми возможностями, и является подтверждением целостности и подлинности передаваемых и хранимых данных.

операционная система, информационная безопасность, комплекс средств защиты, контроль целостности, контрольная сумма, замкнутая программная среда, регламентный контроль целостности.

Совершенствование информационных технологий, повышение их роли и значимости требуют постоянного внимания к вопросам обеспечения безопасности информации.

Проблема обеспечения информационной безопасности может быть успешно решена только тогда, когда создана и функционирует комплексная система защиты информации. Для реализации комплексного подхода к обеспечению защиты информации необходимо использовать не только базовые [1] и дополнительные средства защиты информации [2, 3], а также использовать механизмы, предотвращающие попытки несанкционированного доступа.

Функциональные возможности операционной системы (ОС) Astra Linux SE расширены комплексом средств защиты (КСЗ), реализующим дополнительные функции администрирования системы.

Современная операционная система специального назначения (ОС СН) должна обеспечивать функции аудита доступа к объектам файловой системы (ФС) и контроля целостности, как данных, так и исполняемых файлов. Корректная и полная настройка системы аудита ОС СН обеспечивает контроль за изменениями в объектах ФС, а контроль целостности позволяет с большей долей вероятности установить отсутствие в ОС Astra Linux SE данных и функций, обладающих недекларируемыми возможностями.

В ОС СН Astra Linux SE в состав средств защиты включен комплекс программ для решения задачи контроля целостности. Данный комплекс реализует функции управления целостностью данных и состоит из следующих средств [3]:

- подсчета контрольных сумм файлов и оптических дисков;
- контроля соответствия дистрибутиву;
- регламентного контроля целостности;
- создания замкнутой программной среды.

Самым распространенным методом проверки целостности объектов ФС является контроль изменения файлов с помощью подсчета контрольной суммы.

Контрольная сумма – это значение, которое рассчитывается по набору данных с помощью определённого алгоритма и используется для проверки целостности данных при их передаче или хранении. Отличающиеся наборы

данных при их сравнении с большой долей вероятности будут иметь разные контрольные суммы.

Алгоритмы вычисления контрольной суммы [4] представлены в таблице 1.

ТАБЛИЦА 1 Алгоритмы вычисления контрольной суммы

Алгоритм	Область применения	Примеры
Общего назначения	Для проверки целостности цифровых данных при их передаче по каналам связи	CRC8, CRC16, CRC32
Криптографические	Подтверждение целостности и подлинности передаваемых и хранимых данных	Семейства алгоритмов MD (Message Digest Algorithm, MD2 – MD6), SHA (Secure Hash Algorithm, SHA1), ГОСТ Р 34.11-2012 («Стрибог»)

Для подсчета контрольных сумм файлов и оптических дисков в ОС Astra Linux SE используются команды:

md5sum, по умолчанию использует алгоритм MD5. Контрольные суммы с помощью этой команды подсчитываются только для файлов, а для директорий выводится сообщение об ошибке. Для проведения последующей оценки целостности хранимых данных, вывод команды можно перенаправить в контрольный файл.

shasum, реализуется семейством алгоритмов SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 и SHA-512/256.

В ОС Astra Linux SE задача контроля целостности хранимых данных решается с помощью библиотеки libgost. Библиотека используется в следующих программных средствах:

- подсчета контрольных сумм файлов и оптических дисков;
- контроля соответствия дистрибутиву;
- регламентного контроля целостности:
- модулях аутентификации.

Для подсчета контрольных сумм файлов и оптических дисков по стандартам ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 в ОС Astra Linux SE на базе библиотеки libgost включена утилита командной строки gostsum (аналог команды md5sum).

Для контроля соответствия объектов ФС ОС Astra Linux SE ее дистрибутиву разработана графическая утилита «Проверка целостности системы», которую можно запустить с помощью команды fly-admin-int-check.

В состав дистрибутива ОС СН Astra Linux SE (поставляется на оптическом диске) для обеспечения контроля целостности объектов ФС входит файл gostsums.txt, который создается командой gostsum и содержит список контрольных сумм всех файлов из пакета программ дистрибутива.

С помощью графической утилиты «Проверка целостности системы» можно вычислить контрольные суммы файлов и проверить соответствие эталонных контрольных сумм из файла gostsums.txt полученным контрольным суммам файлов.

Указанные команды и утилиты реализуют статический контроль целостности объектов ФС ОС СН.

Для выполнения расширенного контроля целостности файлов в ОС СН разработана система AFICK (Another File Integrity Checker). AFICK обеспечивает проверку следующих атрибутов файла: метки времени, дискреционных атрибутов, мандатных меток безопасности.

В ОС Astra Linux SE используется модифицированный вариант системы AFICK, основанный на алгоритме подсчета контрольных сумм ГОСТ Р 34.11-94 и контроле атрибутов файлов подсистемы безопасности PARSEC (мандатные атрибуты и атрибуты подсистемы аудита безопасности). Система AFICK базируется на библиотеке libgost, как и графическая утилита «Проверка целостности системы».

В AFICK некоторые правила заданы по умолчанию, но можно создавать и свои правила. Файл /etc/afick.conf является базовым конфигурационным файлом системы AFICK и состоит из нескольких секций.

Например, правило MyRule = p+d+i+n+u+g+s+b+md5+m означает слежение за всеми стандартными атрибутами файла и использование хэш-функции MD5 для слежения за целостностью содержимого файлов.

Секция alias содержит правила проверки объектов ФС. Она дополнена тремя действиями:

– контроля целостности мандатных меток безопасности объектов ФС;

– контроля целостности данных системы аудита безопасности ОС;

– слежения за целостностью содержимого объектов ФС с использованием криптографического алгоритма ГОСТ Р 34.11-94.

Секция action содержит типовые правила для каталогов, файлов конфигурации системы и журналов системы аудита. Она дополнена правилами для системы безопасности PARSEC – PARSEConly, PARCEC и GOST.

В секции files to scan по умолчанию определены пути к каталогам и файлам, для которых выполняется регламентный контроль целостности, и применяемые к ним правила контроля, а также представлен ряд дополнительных путей с правилами, которые закомментированы символом «#» и могут быть активированы при удалении символа комментария.

Например,

```
#/etc/security   PARSEC
#/etc/pam.d      PARSEC
```

С помощью этой секции создается база данных системы AFICK (файл с расширением ndbm), в ней хранятся эталонные значения контрольных

сумм и атрибутов объектов ФС. База данных защищена с помощью системы разграничения доступа.

Строка database:=/var/lib/afick/afick в файле afick.conf определяет путь к файлу базы данных системы AFICK.

В системе AFICK существует возможность выполнения регламентного контроля целостности объектов ФС. Для этого AFICK объединяется с сервисом запуска программ по расписанию CRON. При запуске AFICK автоматически устанавливает ежедневное задание для демона crond.

Результатом контроля целостности системы AFICK является выводимый на экран отчет, в котором отображаются начальные и текущие контрольные суммы объектов ФС, а также выводится сообщение об изменении их размеров.

Для мониторинга объектов ФС на наличие изменений используется графическая утилита системы AFICK в которой настройка секций файла afick.conf осуществляется выбором элементов меню Настройка. При этом для элементов секций выводится соответствующее диалоговое окно. Все изменения отображаются в разделах отображения изменений и предупреждений.

Система AFICK фиксирует изменения в файлах и каталогах, сравнивая их атрибуты с атрибутами, которые были сохранены при последнем запуске ОС, а также может настроить правила проверки целостности директорий.

Средства создания замкнутой программной среды в ОС Astra Linux SE разрешают ввести электронную цифровую подпись (ЭЦП) в исполняемые файлы формата ELF (Executable and Linkable Format) устанавливаемого программного обеспечения (ПО). Средства реализованы в виде невыгружаемого модуля ядра ОС СН digsig_verif и представляют механизм контроля целостности загружаемых исполняемых файлов и разделяемых библиотек формата. Они функционируют в 3 режимах:

– штатном, в котором исполняемым объектам ФС формата ELF и разделяемым библиотекам без ЭЦП или с ложной ЭЦП, исполнение запрещается;

– для проверки ЭЦП в ПО, в котором исполняемым объектам ФС формата ELF и разделяемым библиотекам без ЭЦП или с ложной ЭЦП, исполнение разрешается. Выводится сообщение об ошибке проверки ЭЦП;

– отладочном для тестирования ПО (по умолчанию), в котором ЭЦП при загрузке исполняемых объектов ФС формата ELF и разделяемых библиотек не проверяется.

Файл /etc/digsig/digsig_initramfs.conf является конфигурационным для выбора режима функционирования модуля digsig_verif, управление которым осуществляется через интерфейс ФС sysfs.

Команды и утилиты, реализующие статический контроль целостности объектов ФС, функционируют в режимах вычисления и проверки контрольной суммы объектов ФС ОС СН. Такая проверка является неэффективной для файлов, которые постоянно меняются в процессе работы ОС СН. Контроль целостности на основе контрольной суммы файла не учитывает следующие атрибуты файла: метки времени, дискреционные атрибуты и мандатные метки безопасности.

Система AFICK сочетает функции контроля целостности файлов и их атрибутов с использованием криптографических алгоритмов подсчета контрольных сумм с интеграцией с сервисом запуска программ по расписанию CRON. Такое сочетание позволяет выполнять периодический контроль целостности ключевых файлов ОС СН Astra Linux SE с целью защиты от внесения в них случайных или преднамеренных изменений.

Список используемых источников

1. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О дополнительных задачах администрирования средств защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. С. 318–323.

4. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие / под редакцией доктора технических наук П. Н. Девянина. Москва: Горячая линия – Телеком, 2018. 311 с.

УДК 621.391
ГРНТИ 81.93.29

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ В СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ СУБД

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Проведен анализ методов резервного копирования и восстановления информации в защищенной СУБД PostgreSQL из состава операционной системы специального назначения «Astra Linux SE». Рассмотрены преимущества и ограничения для каждого метода. Даны рекомендации по составлению расписания резервного копирования и восстановления информации в базе данных.

операционная система специального назначения, система управления базами данных, база данных, защита информации, резервное копирование и восстановление информации, архивирование.

Современная защищенная система управления базами данных (СУБД) PostgreSQL 9.6 в операционной системе специального назначения (ОС СН) «Astra Linux Special Edition», релиз Смоленск, версия 1.6 с встроенными средствами защиты информации предназначена для разработки информационных систем и систем управления для работы с конфиденциальной информацией и с информацией, содержащей сведения, составляющие государственную тайну.

Применение СУБД для создания баз данных (БД) в интересах должностных лиц, позволяет решать задачи быстрого поиска информации, необходимой для работы должностных лиц, реализовать многоуровневую защиту информации, обеспечить разграничение доступа пользователей к защищаемым ресурсам БД и управление информационными потоками [1, 2].

Для защиты информации в БД, для надежного и быстрого восстановления работы БД в состав ОС СН «Astra Linux Special Edition» и СУБД PostgreSQL 9.6 входят средства резервного копирования и восстановления информации (РКВИ).

Для осуществления РКВИ в СУБД PostgreSQL 9.6 существуют три метода, которые имеют разные алгоритмы реализации:

1. Выгрузка в SQL;
2. Копирование на уровне файлов;

3. Непрерывное архивирование.

Выгрузка в SQL.

В основе этого метода – генерация текстового файла, который содержит команды SQL (SQL-дамп). Эти команды SQL при выполнении на сервере создают новую БД, копию той, что была на момент выгрузки (исходное состояние БД). Для создания новой БД в PostgreSQL применяется вспомогательная программа pg_dump.

Программа pg_dump может создать файлы в различных форматах, отличных от исходного формата файлов БД. Так же утилита предоставляет возможность параллельной обработки данных и удобное управление восстановлением данных.

Процедуру резервного копирования можно выполнять с любого удалённого компьютера, с которого есть доступ к БД.

Утилита pg_dump не использует для своей работы специальные привилегии. Для ее работы, в первую очередь, необходимо задать дискреционные права доступа на чтение всех таблиц БД [3], которые необходимо выгрузить. Поэтому для копирования всей базы данных её необходимо запускать с правами суперпользователя СУБД.

Важное преимущество pg_dump по сравнению с другими методами резервного копирования и восстановления в том, что вывод утилиты можно загрузить в любые новые версии PostgreSQL, в то время как резервная копия на уровне файловой системы и непрерывное архивирование (два других метода РКВИ) строго зависят от версии сервера.

Метод с применением pg_dump так же будет работать при переносе БД на другую машинную архитектуру, например, при переносе с 32-битной на 64-битную версию сервера.

Текстовые файлы, созданные pg_dump, предназначаются для последующего чтения программой psql, которая восстанавливает БД. Перед восстановлением SQL-дампа все пользователи, которые владели объектами БД или имели права на объекты в БД, должны существовать. Если их нет, то при восстановлении БД будут возникать ошибки.

РКВИ средствами PostgreSQL 9.6 (метод SQL-дамп) рекомендуется для применения в случае работы с БД большого количества пользователей с различными правами доступа. При выполнении РКВИ утилита pg_dump не препятствует доступу для чтения или для записи других пользователей в БД.

Копирование на уровне файлов.

Вторым методом резервного копирования является непосредственное копирование тех файлов, в которых PostgreSQL хранит содержимое БД.

В состав ОС СН «Astra Linux SE» входит множество средств РКВИ.

Утилиты tar, rsync являются традиционными инструментами для создания резервных копий и архивирования файловой системы (ФС).

Утилита tar предназначена для удалённого резервного копирования, может работать с различными дисковыми накопителями. Утилита позволяет создать только полную копию файлов, в которых хранится БД.

Утилита rsync предназначена для резервного копирования или синхронизации файлов и каталогов с минимальными затратами трафика. Все действия утилиты выполняются от имени администратора с помощью механизма sudo.

При использовании утилиты rsync для резервного копирования на уровне ФС необходимо в первый раз осуществить запуск rsync при работающем сервере, а затем, на время второго запуска rsync, остановить сервер БД. Второй раз выполнение rsync потребует меньше времени, т.к. необходимо передать относительно небольшой объем данных. Результат копирования будет целостным т. к. сервер был остановлен на время работы утилиты. Этот подход позволяет минимизировать время простоя сервера.

Резервная копия в ФС не обязательно будет иметь меньший объем, чем SQL-дамп. Она может занять даже больше места, т.к. утилите pg_dump не требуется включать в SQL-дамп содержимое индексов, достаточно только включить команды для их воссоздания.

Однако есть следующие ограничения для данного метода:

Для получения копии, сервер БД должен быть остановлен. Перед восстановлением данных сервер БД должен быть остановлен.

Нельзя сохранить или восстановить только некоторые отдельные таблицы или БД из соответствующих файлов и каталогов. Это не возможно, т.к. в этих файлах содержится лишь часть необходимой информации. Остальная часть информации находится в файлах журнала записи выполнения транзакций. Файл с таблицей можно использовать только вместе с этой информацией. Поэтому невозможно восстановить одну только таблицу и соответствующие ей данные, т. к. это нарушит все остальные таблицы БД.

Таким образом, резервное копирование на уровне ФС работает только в случае полного копирования и восстановления всей БД.

Непрерывное архивирование.

Всё время в процессе работы СУБД PostgreSQL ведёт журнал предзаписи (WAL), который расположен в подкаталоге pg_xlog/ каталога с данными БД. В этот журнал записываются все изменения, которые происходят в файлах данных.

Этот журнал необходим для безопасного восстановления БД после сбоя сервера. Если происходит сбой, целостность БД может быть восстановлена в результате «воспроизведения» тех записей, которые сохранились после последней контрольной точки.

Журнал дает возможность использовать сочетание двух методов РКВИ (резервного копирования на уровне ФС и копирования файлов WAL).

При необходимости восстановления данных, можно сначала восстановить копию файлов, а затем выполнить «воспроизведение» журнала из скопированных файлов WAL. Работа БД будет восстановлена.

Такой подход более сложен для администрирования, но имеет ряд преимуществ.

В качестве начальной точки для восстановления необязательно иметь полностью согласованную копию на уровне файлов. Несогласованность копии будет исправлена при воспроизведении журнала.

При воспроизведении можно обрабатывать неограниченную последовательность файлов WAL, непрерывную резервную копию БД можно получить, продолжая архивировать файлы WAL. Это особенно важно для больших БД, полные резервные копии которых очень объемные, а РКВИ занимает много времени.

Воспроизводить все записи WAL до конца не обязательно. Процесс можно остановить в любой точке. Эта технология поддерживает восстановление БД на любой момент времени.

Как и резервное копирование на уровне ФС, этот метод позволяет восстанавливать только всю БД целиком, а не ее части. Для архивов требуется большой объем памяти, базовая резервная копия может быть объёмной, а системы будут генерировать много мегабайт трафика WAL, который необходимо архивировать.

Этот метод резервного копирования рекомендуется использовать в тех ситуациях, где необходима высокая надёжность РКВИ.

Таким образом, расписание РКВИ в СУБД PostgreSQL рекомендуется составлять с учетом преимуществ и ограничений для каждого метода РКВИ. Применение различных алгоритмов РКВИ позволит восстановить работу БД в кратчайшие сроки.

Список используемых источников

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Механизмы разграничения доступа к данным в СУБД в среде операционной системы специального назначения Astra Linux SE // Региональная информатика: материалы XVII Санкт-Петербургской международной конференции, СПб., 28–30 октября 2020 г. СПб.: СПОИСУ, 2020. Т. 1. С 79–81.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Разграничение доступа к данным в СУБД из состава операционной системы специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 259–263.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

УДК 004.056.57
ГРНТИ 81.93.29

ОПИСАНИЕ МЕТОДОВ АНАЛИЗА И ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

А. О. Казанцев, В. О. Малюков, Р. С. Скакунов

Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Сетевая и системная безопасность сейчас невероятно важны. Из-за быстрого распространения вредоносного ПО традиционные методы анализа не справляются с огромными выборками.

реверсивная разработка, системная безопасность, шифрование, обфускация.

Введение

Безопасность сетей и систем - невероятно важные вопросы в настоящее время. По данным *Kaspersky Security Network* [1], в 2021 году ежедневно блокировалось 14 миллионов угроз. Кроме того, постоянно появляются новые типы вредоносного ПО, которые становятся все более агрессивными. Например, использование вредоносных скриптов Power-Shell в том же году увеличилось на 1000%. Что еще хуже, антивирусные методы, используемые злоумышленниками, также неуклонно совершенствуются. Использование полиморфных движков позволяет разработчикам вредоносных программ мутировать существующий код, сохраняя неизменными исходные функции. Это достигается, например, с помощью обфускации и шифрования. Это привело к быстрому распространению вредоносного ПО, с которым традиционные методы анализа справляются с трудом, поскольку они полагаются на сопоставление сигнатур и эвристические правила.

Обфускация и шифрование кода.

Поскольку исполняемые файлы могут быть проанализированы путем дизассемблирования, были изобретены новые методы, называемые антиреверсивной разработкой, чтобы затруднить этот процесс. Их используют не только разработчики вредоносных программ, но и компании-разработчики программного обеспечения, чтобы защитить коммерческие программы от взлома или пиратства. Обфускация кода и шифрование — два широко используемых метода.

Обфускация кода использует ненужные выражения и данные, чтобы сделать исходный или машинный код сложным для понимания человеком (рис. 1).

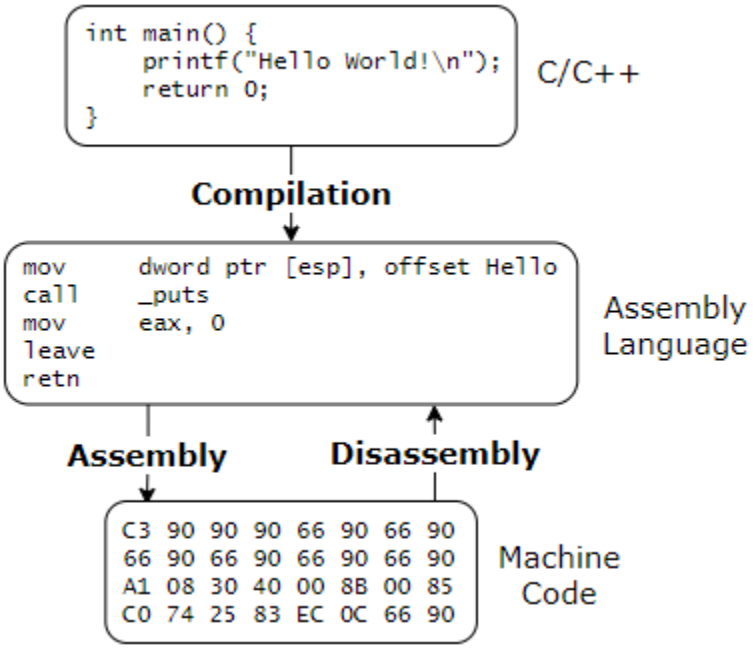


Рис. 1. Компиляция, сборка и разборка

В отличие от обфускации, шифрование кода упаковывает и шифрует исполняемые файлы на диске. Они расшифруются во время исполнения. Это означает, что их почти невозможно проанализировать с помощью статического дизассемблирования, полагаясь вместо этого на выполнение и просмотр системных журналов. *IDA Pro* не смог разобрать зашифрованные инструкции и отображает только шестнадцатеричный машинный код (рис. 2).

```
dd 0AE2C543Fh, 2F10C7A2h, 8059DFA5h, 1108E115h, 0CE3D9038h
dd 2007DFBBh, 77DA9179h, 904F0AD2h, 0DBD3E36Dh, 0D0BCF948h
dd 0DB7695C0h, 0B9B72C77h, 849CAA3Ah, 5AC7847Dh, 0BAA2BFBFh
dd 9D6EE0FAh, 0E275F58Ch, 0E172C2F0h, 0D3BCB558h, 27A93062h
dd 319BB966h, 320907F5h, 0C42A8F80h, 6A86F551h, 37EC06DAh
dd 4EB946Bh, 162FBB98h, 73A6A2DEh, 0CFE5D957h, 6DC5B790h
```

Рис. 2. *IDA Pro* не удалось дизассемблировать зашифрованные инструкции

Формат Portable Executable

Формат *Portable Executable (PE)* – формат исполняемых файлов в системах Windows [2], состоящий из нескольких заголовков и секций (рис. 3). Заголовки можно рассматривать как метаданные, расположенные в начале исполняемого файла. Они инкапсулируют системную информацию, такую

как таблицы экспорта и импорта API, ресурсы (значки, изображения и аудио и т. д.), а также распределение данных и кода. Эта информация имеет решающее значение для анализа вредоносных программ. Данные и исполняемый код хранятся в разных разделах за заголовками, в зависимости от их функций.

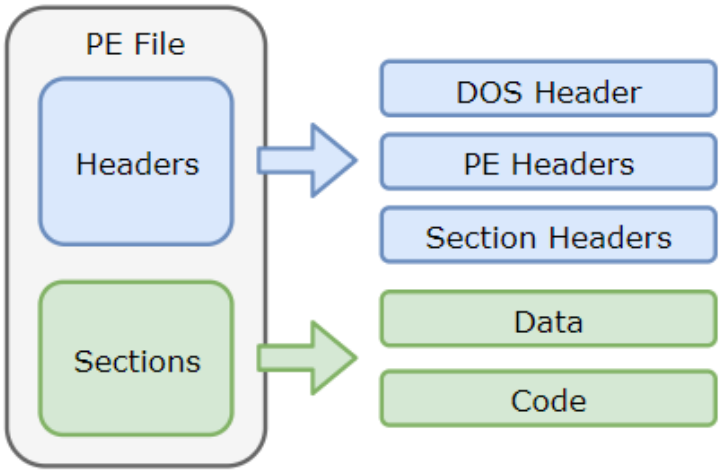


Рис. 3. Формат *Windows PE*

Для анализа формата PE не нужны инструменты дизассемблирования, и злоумышленники не могут полностью стереть эти данные. Таким образом, даже если вредоносное ПО зашифровано, большинство структур по-прежнему доступны, но могут быть не очень точными.

Традиционный анализ вредоносных программ

Традиционные методы включают статический анализ дизассемблирования и динамический анализ поведения. Как упоминалось ранее, они в значительной степени полагаются на экспертов.

Статический анализ должен сначала дизассемблировать машинный код с помощью профессиональных инструментов, таких как *IDA Pro*. Аналитики изучают потоки управления и инструкции, чтобы понять вредоносное поведение. Теоретически он обеспечивает полное покрытие кода, но требует много времени и уязвим для обфускации или шифрования кода.

Напротив, динамический анализ может эффективно решать проблему обфускации кода. Потому что он фокусируется только на системных событиях и не заботится о подробных инструкциях. Кроме того, он не подвержен шифрованию, поскольку зашифрованные файлы должны расшифровываться перед выполнением. Однако динамический анализ стоит дорого и требует виртуальных сред для запуска вредоносных программ. Кроме того, некоторые вредоносные действия не будут зарегистрированы, поскольку среда не соответствует условиям выполнения. Вредоносное ПО также может обнаруживать виртуальные среды и скрываться.

Заключение

В 1949 г. американский ученый венгерского происхождения Джон фон Науманн разработал математическую теорию создания самовоспроизводящихся программ. Это была первая теория создания компьютерных вирусов

Проблема вредоносных программ заслуживает повышенного внимания как одна из самых главных неприятностей, с которыми ежедневно сталкиваются современные пользователи компьютеров. Их пагубное воздействие проявляется в том, что они подрывают принцип надёжности компьютера и нарушают неприкосновенность личной жизни, нарушают конфиденциальность и разрывают отношения между защищёнными механизмами работы компьютера, посредством некоторых комбинаций шпионских действий.

Список используемых источников

1. Развитие информационных угроз во втором квартале 2021 года. Статистика по ПК // Лаборатория Касперского. 2021. URL: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/

2. Microsoft Corporation, “PE format”. 2021. URL: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format

Статья представлена старшим научным сотрудником НИО-3 НИЦ ВАС, кандидатом технических наук, доцентом В. А. Мешалкиным.

УДК 004.056.5
ГРНТИ 81.93.29

МОДЕЛЬ ПРОЦЕССА РЕАГИРОВАНИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА НАРУШЕНИЯ ЗАЩИЩЕННОСТИ СЕТИ

О. Э. Калашников, В. А. Липатников, М. А. Синдеев, А. А. Шевченко

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Известные методы управления защитой сетей VoIP-телефонии с применением специальных мер в современных условиях недостаточно эффективны, так как не рассматривают способы поддержки принятия решений и прогнозирования угроз вторжений. Целью работы является разработка предложения по обеспечению защиты сети VoIP- телефонии путем прогнозирования и поддержки принятия решений в условиях

угроз вторжений. В статье предложена модель действий администратора ИБ ИТКС при возникновении события нарушения ИБ.

информационная безопасность, информационные технологии; информационные сети, когнитивные карты, VoIP, информационно-телекоммуникационная сеть (ИТКС).

В связи с быстрым развитием информационных технологий, в том числе сети Интернет, объединяющей разнородные сети, и переходом к информационному обществу, проблема обеспечения ИБ и построения распределенных сетей VoIP телефонии стала одной из наиболее актуальных [1]. К средствам защиты в настоящее время предъявляются более жесткие требования [2, 3]. Известны методы обеспечения необходимого уровня защищенности различных систем, например, способ управления ИБ информационно-вычислительной сети (ИВС) путем реализации ложной сети на основе выделенного сервера с контейнерной виртуализацией [4, 5]. Однако в этом случае при управлении ИВС не используются данные анализа динамики действий нарушителя

Основным требованием, предъявляемым системам обеспечения безопасности сейчас, является способность находить аномалии и соответственно, вторжения в реальном времени. Возникает противоречие между новыми эффективными средствами кибернетического вторжения и существующими способами защиты ИТКС.

Модель сети

В связи с большим количеством факторов необходимости внедрения интеллектуальных средств защиты в сетях нового поколения целесообразно разработать новую модель информационной сети в условиях динамики угроз вторжения с использованием интеллектуальных технологий аналитики, прогнозирования и реагирования на инциденты. Для этого построим схему исследуемой сети (рис. 1).

На схеме изображены три офиса предприятия – «Центральный офис», «Офис 1» и «Офис 2». Каждый сегмент сети выходит в WAN через межсетевой экран, обеспечивающий защиту периметра от атак. Для обеспечения конфиденциальности и целостности данных передача производится посредством построения VPN-туннелей, которые конфигурируются на VPN-серверах. Чтобы обеспечить работу сети (маршрутизацию ip-пакетов), в инфраструктуру добавлены маршрутизаторы. А чтобы увеличить количество подключенных устройств и разбиение сети на сегменты подсети используются коммутаторы. Для обеспечения функционирования VoIP-телефонии автоматические VoIP-станции присутствуют в каждом офисе. Чтобы собирать и обрабатывать информацию о безопасности сети, в каждом сегменте ИТКС разворачиваются агенты нейтрализации и контроля угроз. Для обес-

печения возможности интеллектуальной автоматизации, удобства управления, мониторинга и проактивной защиты от вторжения нарушителя необходимо внедрить сервер безопасности, который будет находиться в центральном офисе и обеспечивать вышеперечисленные функции во всей сети, в том числе собирать и обрабатывать актуальную информацию с агентов.

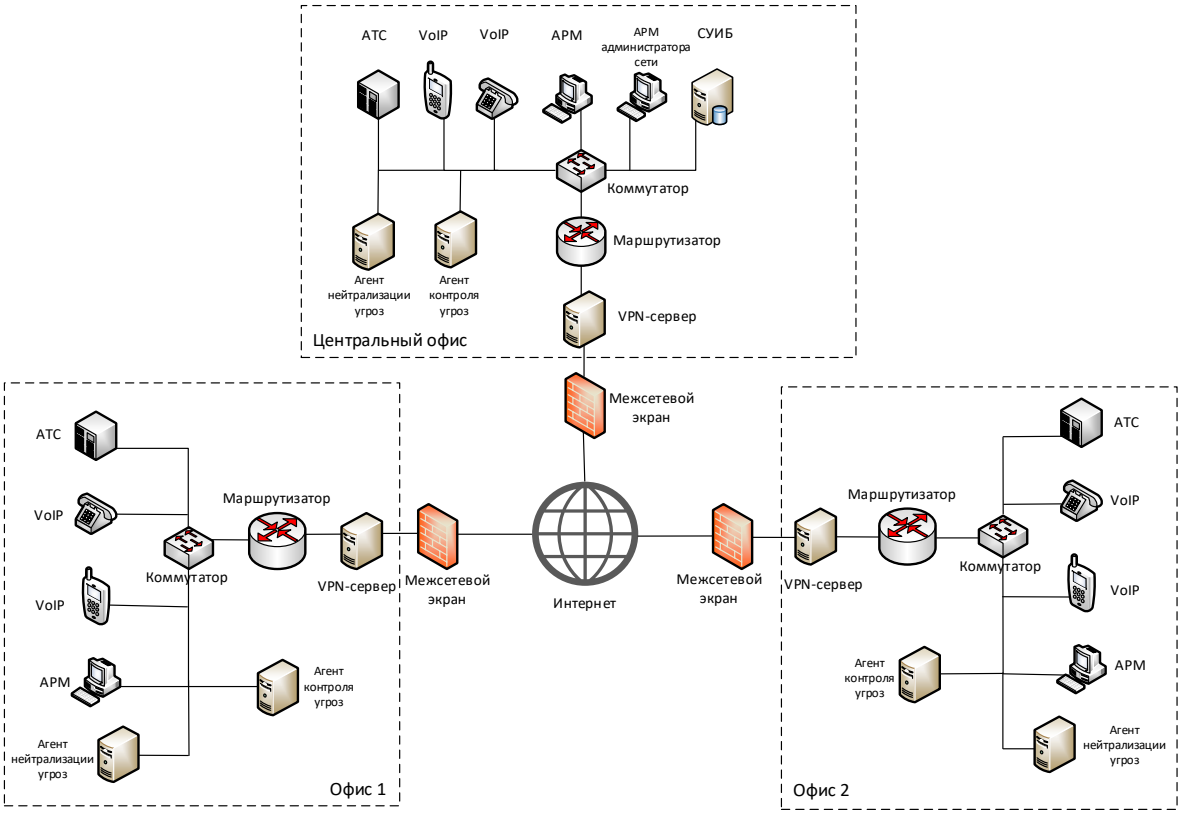


Рис. 1. Исследуемая схема информационно-телекоммуникационной сети с VoIP-телефонией

Алгоритм действий администратора при возникновении события ИБ

Управление инцидентами и обработка событий ИБ весьма трудоемкий процесс. Поэтому администратору или автоматизированной системе управления безопасностью необходимо иметь четкое представление о том, как производить обработку событий с наибольшей эффективностью и скоростью.

Исходя из вышеперечисленных особенностей был предложен алгоритм действий администратора ИБ при возникновении события безопасности (рис. 2, см. ниже).

Алгоритм подразумевает обеспечение цикличной системы рассмотрения, классификации и нейтрализации угрозы администратором или автоматической системой на основе интеллектуальных технологий.

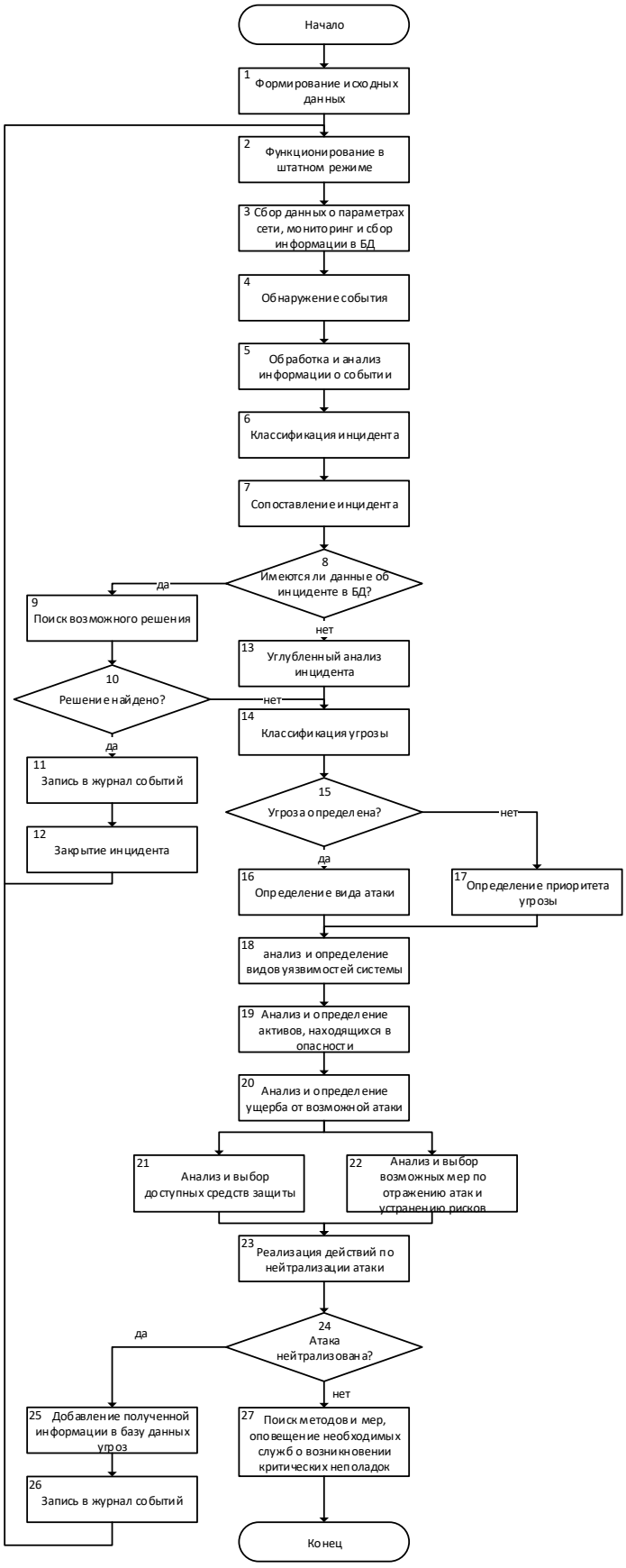


Рис. 2. Алгоритм действий администратора ИБ ИТКС при возникновении события нарушения ИБ

Разработанный алгоритм в полной мере отражает шаги, которые необходимо предпринять администратору или автоматизированной системе ИБ, чтобы обработать событие.

В соответствии с анализом предложенного алгоритма действий администратора в условиях угроз вторжений предложена модель процесса реагирования администратора ИБ на нарушения защищенности сети и описан граф последовательности обработки событий от возникновения до результата оценки рисков (рис. 3).

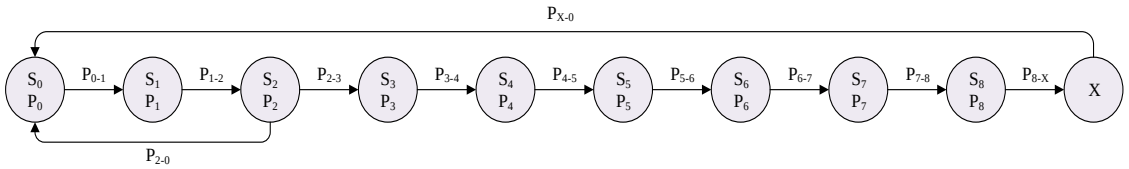


Рис. 3. Граф состояний системы поддержки принятия решений администратора при возникновении события нарушения ИБ

В таблице 1 описаны состояния графа, обозначающие шаги обработки события от возникновения до предложения оценки рисков и вариантов его обработки системой или администратором.

ТАБЛИЦА 1. Состояния графа последовательности обработки событий от возникновения до результата оценки рисков

Событие	Описание
S_0	Исходное состояние. Защищенное состояние ИТКС (без аномальных воздействий)
S_1	Возникновение события ИБ
S_2	Квалификация системой события в инцидент
S_3	Определение системой инцидента в угрозу
S_4	Анализ системой уязвимостей, исходя из определенной ранее угрозы
S_5	Анализ системой подверженных атаке (угрозе) активов организации
S_6	Анализ негативных последствий воздействия угрозы на активы организации, исходя из базы угроз
S_7	Анализ средств защиты, доступных для закрытия уязвимостей системы от обнаруженной угрозы
S_8	Предложение методов и мер по отражению атак и обработке рисков
X	Противодействие угрозе согласно решению администратора и системы

Разработанная модель позволит повысить эффективность обеспечения кибернетической безопасности и работы системы управления и администратора ИБ, за счет уменьшения времени необходимого на анализ и обработку рисков, а также за счет повышения точности прогнозов и обработки событий.

Список используемых источников

1. Лукацкий А. Обнаружение атак. СПб.: Изд-во БХВ-Петербург, 2008. 304 с.
2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». URL: http://protect.gost.ru/default.aspx, (дата обращения: 17.12.2018).
3. Кузнецов А. В., Муравьева Д. С. Создание систем управления событиями и инцидентами ИБ (SIEM) // Information Security. 2012. № 3. С. 28–29.
4. Gu Y., McCallum A., Towsley D. Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation // Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. 2005. pp. 32–32.
5. Липатников В. А., Шевченко А. А., Яцкин А. Д. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. № 4 (102). С. 116–126.

УДК 004.7
ГРНТИ 81.93.29

ПРЕДЛОЖЕНИЕ ПО КЛАССИФИКАЦИИ КОМПЬЮТЕРНЫХ АТАК НА РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

О. Э. Калашников, В. А. Липатников, М. А. Синдеев, А. А. Шевченко

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Традиционно атаки делят на категории в зависимости от эффекта, который они производят: нарушение конфиденциальности информации, нарушение целостности информации и отказ в обслуживании. Основным недостатком такого деления является его слабая информативность, так как по информации о классе атаки практически ничего невозможно сказать о ее особенностях.

классификация, атаки, сети, систематизация, компьютерные атаки.

Существующие классификации сетевых атак не имеют классификационных признаков систематизации данных, мало информативны и не являются строгой классификацией компьютерных атак (КА). В предложенной классификации КА установлено соответствие между основными характеристиками элементов информационно-телекоммуникационной сети (ИТКС), спецификой их применения и особенностями реализации атак по принятым классификационным признакам.

Разработка классификации КА основана на материалах «Методики оценки угроз безопасности информации» ФСТЭК России [1]. При разработке классификатора КА использованы общие подходы к классификации объектов в области информационных технологий и существующие научные методы классификации угроз информационной безопасности (ИБ). Процесс выявления нарушителя ИБ представляет собой сложную задачу, основной проблемой которой является достоверность входных данных. Анализ рассмотренных методик показал, что технические причины являются главным препятствием для простого определения источника КА. Перспективно выглядит применение методов машинного обучения и искусственного интеллекта совместно с инструментами цифровой криминалистики. Благодаря анализу информационных материалов по известным инцидентам создана классификация КА [2, 3]. Обобщение представлено в виде таблицы 1.

ТАБЛИЦА 1. Классификация КА на ИТКС

№ п/п	Признак классификации КА	Содержание и индекс классификатора (Yij)
1.	По источнику атаки	Внешние ($Y_{1;1}$) Внутренние ($Y_{1;2}$)
2.	По цели воздействия	Нарушение целостности ($Y_{2;1}$) Нарушение доступности ($Y_{2;2}$) Нарушение штатного режима функционирования ($Y_{2;3}$)
3.	По принципу воздействия	Использование существующих (штатных) каналов доступа ($Y_{3;1}$) Использование скрытых каналов доступа ($Y_{3;2}$) Формирование новых каналов доступа ($Y_{3;3}$)
4.	По способам воздействия	Нарушение структур данных ($Y_{4;1}$) Нарушение текстовых файлов, объектных и загрузочных кодов программ ($Y_{4;2}$) Нарушение функций общего ПО ИТКС (операционной системы, системы управления базами данных и других программ) ($Y_{4;3}$) Нарушение функций специального ПО ИТКС ($Y_{4;4}$) Нарушение сети (протоколов) передачи данных ($Y_{4;5}$) Искажение программ и информации в цифровом коммуникационном оборудовании ($Y_{4;6}$)
5.	По характеру воздействия	Активное воздействие (нарушение, разрушение, искажение) ($Y_{5;1}$) Пассивное воздействие (сбор информации, наблюдение, анализ) ($Y_{5;2}$) Интерактивный режим нарушителя с объектом (субъектом) доступа ($Y_{5;3}$) Воздействие при выполнении ТЦУ (осуществлении информационно-вычислительного процесса обработки данных) ($Y_{5;4}$)

№ п/п	Признак классификации КА	Содержание и индекс классификатора (Yij)
6.	По объектам и субъектам воздействия	Пункты управления ($Y_{6;1}$) Мобильные пункты управления ($Y_{6;2}$) Центры управления ($Y_{6;3}$) Операторы ($Y_{6;4}$) Лица, принимающие решения ($Y_{6;5}$)
7.	По средствам воздействия	«Ложная информация» ($Y_{7;1}$) Искажения информации ($Y_{7;11}$) Введение дезинформации ($Y_{7;12}$) «Функциональное поражение» ($Y_{7;2}$) Нарушение режимов функционирования ($Y_{7;21}$) Блокирование информации ($Y_{7;22}$) Разрушение (стирание информации) ($Y_{7;23}$) Перехват информации ($Y_{7;24}$) Разглашение (утечка) информации ($Y_{7;24}$) Хищение информации ($Y_{7;25}$) «Разрыв соединения» ($Y_{7;26}$) Логическое отключение абонентов ($Y_{7;3}$) Перенаправление пакетов данных (искажение порядка маршрутизации) ($Y_{7;31}$) «Спам» ($Y_{7;32}$)
8.	По используемой ошибке	Ошибки в работе администратора локальной вычислительной сети и администратора безопасности информации ($Y_{8;1}$)
9.	По состоянию нарушаемых технологических операций	Сбор, прием, передача данных, обмен информацией ($Y_{9;1}$) Осуществление информационно-вычислительного процесса ($Y_{9;2}$) Запись, считывание, хранение информации в базе данных ($Y_{9;3}$)
10.	По уровню эталонной модели взаимодействия открытых систем (ЭМВОС)	Физический ($Y_{10;1}$) Канальный ($Y_{10;2}$) Сетевой ($Y_{10;3}$) Транспортный ($Y_{10;4}$) Сеансовый ($Y_{10;5}$) Представительский ($Y_{10;6}$) Прикладной ($Y_{10;7}$)
11.	По типу воздействия	Программное ($Y_{11;1}$) Программно-техническое ($Y_{11;2}$)
12.	По потенциальному ущербу	Низкий ущерб ($Y_{12;1}$) Средний ущерб ($Y_{12;2}$) Высокий ущерб ($Y_{12;3}$) Катастрофический ущерб ($Y_{12;4}$)
13.	По соответствию требованиям к средствам защиты информации	Класс защищенности для АС ($Y_{13;1}$) Класс защищенности для СВТ ($Y_{13;2}$) Класс защищенности для межсетевых экранов ($Y_{13;3}$)

№ п/п	Признак классификации КА	Содержание и индекс классификатора (Yij)
		Класс защищенности для антивирусных средств ($Y_{13;4}$) Класс по контролю отсутствия не декларированных возможностей ($Y_{13;5}$)
14.	По сценариям воздействия субъекта доступа	Внешний злоумышленник (вероятный противник) ($Y_{14;1}$) Санкционированный оператор ($Y_{14;2}$) Санкционированный абонент удаленного доступа ($Y_{14;3}$) Зарегистрированный оператор внешней системы ($Y_{14;4}$) Администратор ИТКС ($Y_{14;5}$) Администратор безопасности информации ($Y_{14;6}$) Программист – разработчик ($Y_{14;7}$)
15.	По этапам жизненного цикла системы	Технологические воздействия ($Y_{15;1}$) Эксплуатационные воздействия ($Y_{15;2}$)
16.	По характеру возникновения	Преднамеренные воздействия ($Y_{16;1}$) Непреднамеренные воздействия ($Y_{16;2}$)
17.	По виду совершенного компьютерного преступления	Неправомерный доступ к компьютерной информации ($Y_{17;1}$) Создание, использование и распространение вредоносных программ ($Y_{17;2}$) Нарушение правил эксплуатации средств вычислительной техники и программного обеспечения ($Y_{17;3}$)

Классификация КА позволяет анализировать действия нарушителя и распознавать атаки на раннем этапе их реализации, а также определить происхождение и источник атаки благодаря интеграции цифровой криминалистики с уликами из реального мира для установления злоумышленника или группы злоумышленников [4]. Также появляется возможность разрабатывать проактивные системы ИБ, способных обеспечивать высокий уровень защиты от угроз [5]. Рассмотренных подход нивелирует недостатки других подходов к классификации и позволяет улучшить качество обработки данных [6]. Полученные таким образом данные могут использоваться для проектирования систем защиты ИТКС с функцией прогнозирования поведения нарушителя, что является главным достоинством предложенного подхода для повышения ИБ сетей.

ТАБЛИЦА 2. Распределение классификационных признаков по типам атак

Тип атаки	Классификационный признак компьютерной атаки																
Ранняя десинхронизация	$Y_{1;1}$	$Y_{2;3}$	$Y_{3;1}$	$Y_{4;3}$	$Y_{5;3}$	$Y_{6;6}$	$Y_{7;21}$	-	$Y_{9;3}$	$Y_{10;1}$	$Y_{11;2}$	$Y_{12;2}$	$Y_{13;1}$	$Y_{14;1}$	$Y_{15;2}$	$Y_{16;1}$	$Y_{17;3}$
Ложные ARP-ответы	$Y_{1;1}$	$Y_{2;2}$	$Y_{3;1}$	$Y_{4;5}$	$Y_{5;1}$	$Y_{6;6}$	$Y_{7;12}$	-	$Y_{9;3}$	$Y_{10;1}$	$Y_{11;1}$	$Y_{12;3}$	$Y_{13;1}$	$Y_{14;1}$	$Y_{15;1}$	$Y_{16;1}$	$Y_{17;1}$
Имперсонация TCP-соединения без обратной связи	$Y_{1;1}$	$Y_{2;3}$	$Y_{3;1}$	$Y_{4;6}$	$Y_{5;3}$	$Y_{6;6}$	$Y_{7;32}$	-	$Y_{9;1}$	$Y_{10;3}$	$Y_{11;1}$	$Y_{12;1}$	$Y_{13;2}$	$Y_{14;1}$	$Y_{15;1}$	$Y_{16;1}$	$Y_{17;1}$
Атака SYN flood (Neptune)	$Y_{1;1}$	$Y_{2;2}$	$Y_{3;1}$	$Y_{4;5}$	$Y_{5;1}$	$Y_{6;6}$	$Y_{7;12}$	-	$Y_{9;1}$	$Y_{10;3}$	$Y_{11;1}$	$Y_{12;1}$	$Y_{13;3}$	$Y_{14;1}$	$Y_{15;1}$	$Y_{16;1}$	$Y_{17;1}$
Атака на дерево STP	$Y_{1;1}$	$Y_{2;3}$	$Y_{3;2}$	$Y_{4;3}$	$Y_{5;4}$	$Y_{6;6}$	$Y_{7;21}$	-	$Y_{9;1}$	$Y_{10;2}$	$Y_{11;1}$	$Y_{12;1}$	$Y_{13;3}$	$Y_{14;1}$	$Y_{15;2}$	$Y_{16;1}$	$Y_{17;3}$
Подмена DHCP сервера	$Y_{1;1}$	$Y_{2;2}$	$Y_{3;1}$	$Y_{4;3}$	$Y_{5;1}$	$Y_{6;6}$	$Y_{7;2}$	-	$Y_{9;1}$	$Y_{10;2}$	$Y_{11;1}$	$Y_{12;4}$	$Y_{13;3}$	$Y_{14;1}$	$Y_{15;2}$	$Y_{16;1}$	$Y_{17;3}$
Атака на VLAN	$Y_{1;1}$	$Y_{2;3}$	$Y_{3;1}$	$Y_{4;6}$	$Y_{5;1}$	$Y_{6;6}$	$Y_{7;1}$	-	$Y_{9;1}$	$Y_{10;3}$	$Y_{11;1}$	$Y_{12;2}$	$Y_{13;3}$	$Y_{14;1}$	$Y_{15;1}$	$Y_{16;1}$	$Y_{17;1}$

Список используемых источников

1. ФСТЭК 5 февраля 2021. Методика оценки угроз безопасности. URL: https://fstec.ru.

2. Липатников, В. А., Коршунов Г. И., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4 (95). С. 61–72. DOI 10.31799/1684-8853-2018-4-61-72.

3. Петренко С. А., Ступин Д. Д.Национальная система раннего предупреждения о компьютерном нападении / Университет Иннополис. Санкт-Петербург: Издательский Дом "Афина", 2017. 440 с.

4. Christian R. Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. 2019, Springer, Cham, 2019. 424 p.

5. Липатников В. А., Косолапов В. С., Шевченко А. А., Сокол Д. С. Модель оценки процесса подготовки и реализации вторжений в сетях IP-телефонии // Информация и космос. 2021. № 4. С. 55–69.

6. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем: Материалы всероссийской научно-практической конференции с международным участием, Санкт-Петербург, 28–29 мая 2019 года. Санкт-Петербург: Институт проблем транспорта им. Н.С. Соломенко РАН, 2019. С. 207–214.

УДК 004.492.3:004.056.57
ГРНТИ 81.93.29

МОДЕЛЬ ТРОЯНСКОЙ ПРОГРАММЫ PEGASUS НА ОСНОВЕ ЭВРИСТИЧЕСКИХ ПРИЗНАКОВ

Д. В. Караев, Д. О. Маркин, Д. В. Пинин

Академия Федеральной службы охраны Российской Федерации

В статье приводится модель вредоносного программного обеспечения средства Pegasus (троянская программа, осуществляющая несанкционированный доступ и сбор данных), алгоритм ее выявления, а также программная реализация алгоритма, функционирующая под управлением операционной системы Android. Модель основана на эвристических признаках троянской программы – подмножестве используемых системных привилегий и потенциально опасных API-вызовов. Представлена оценка эффективности разработанного подхода при анализе резервных копий данных (дампов) с нескольких устройств.

статический анализ, сигнатура, троянская программа, Android, Pegasus.

В условиях развития информационных технологий и острого повышения напряженности международной обстановки резко возросло количество компьютерных атак. Особую роль в данных атаках занимает распространение троянских программ (согласно определению по ГОСТ Р 57429–2017), способных воздействовать не только на персональные ЭВМ, но и на смартфоны, планшетные компьютеры и другие вычислительные средства. В большинстве таких случаев атаки достигают цели даже при наличии установленных средств защиты – антивирусов и межсетевых экранов. Данные обстоятельства требуют постоянного совершенствования моделей вредоносного программного обеспечения (ВПО), а также методов и алгоритмов его обнаружения, учитывающих современные особенности защиты ВПО от обнаружения, такие как. например, шифрование и обфускация [1].

Известны методы для детектирования ВПО на основе машинного обучения, которые позволяют анализировать большие наборы исполняемых файлов и выявлять аномалии на основе мер сходства характеристик, описано в работе [2], определение характеристик использования *API*-вызовов для *APK*-приложений ОС *Android* с различными уровнями разрешений, а именно: пакеты, классы, функции и *API* рассмотрено в работе [3], использование алгоритмов электронной подписи для фильтрации программ рассмотрено в работе [4].

Модель объекта анализа

Прикладное ПО для ПО для ОС *Android* как правило поставляется в форме *APK*-пакета (*Android Package Kit*), структура которого показана на рисунке 1. Пакетный набор представляет собой *zip*-файл, но он имеет другой формат и другое расширение.

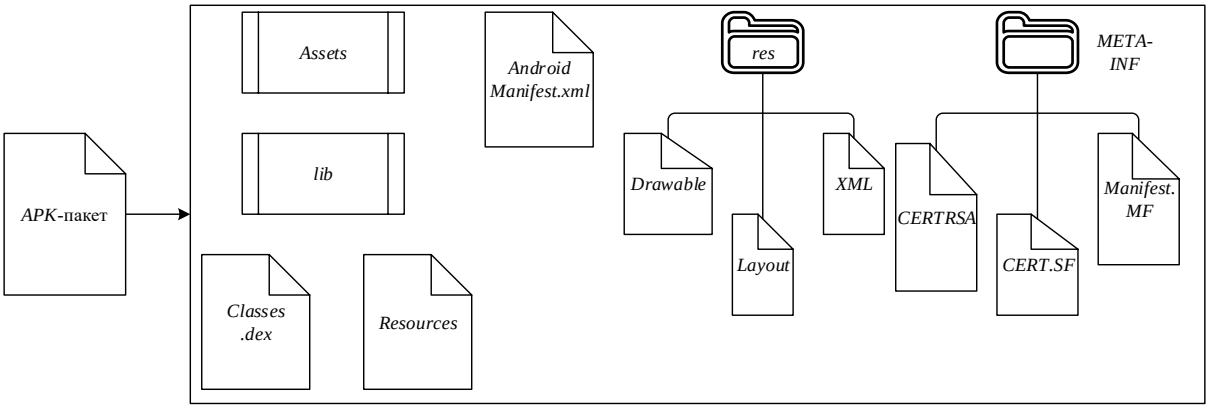


Рис. 1. Состав *APK*-файла

Файл *APK* содержит несколько файлов и папок, описанных ниже:

1. *Assets* – дополнительный каталог, в котором находятся все активы приложения.

2. Каталог *lib*, в котором находятся все скомпилированные нативные библиотеки, такие как библиотеки объектов.

3. Каталог *META-INF* содержит все файлы, связанные с информацией о безопасности и сертификатами приложения. Ниже перечислены наиболее важные файлы в этом каталоге:

– файл *Manifest.MF* содержит дайджест *SHA1* всех ресурсов, используемых приложением;

– файл *CERT.RSA* содержит стандарты криптографии с открытым ключом (PKCS), имена различных криптографических алгоритмов и синтаксис криптографических сообщений;

– в файле *CERT.SF* сохраняется файл дайджеста в форме *SHA1* для *Manifest.MF*.

4. Файл *AndroidManifest.xml* содержит важную информацию о приложении, такую как имя пакета, необходимые разрешения и все компоненты, определенные в приложении.

5. Исполняемый файл *Classes.dex*, содержащий байткод *Dalvik*, преобразованный из исходного кода *Java*.

6. В каталоге *Res* находятся все ресурсы, используемые приложением (например, изображения, иконки, и строки), которые не скомпилированы в файл *resources.arse*, содержащий все предварительно скомпилированные ресурсы.

Чтобы проанализировать *APK*-файл, его необходимо распаковать в подходящий формат. Одним из инструментов, который позволяет это сделать, является средство *APKtool*. Данный инструмент имеет открытый исходный код, и предназначен для обратной разработке прикладного ПО для ОС *Android* путем декодирования *APK*-файла. Декодирование *APK*-файла заключается в преобразовании его в каталог, содержащий приведенную известную файловую структуру.

Модель троянской программы Pegasus

Задача, рассматриваемая в данной работе, заключается в идентификации троянской программы *Pegasus,* в данных резервной копии ОС *Android*. Соответственно, требуется разработать алгоритм анализа, способный распознать вредоносное ПО известного образца троянской программы.

Анализ открытых источников и публикаций, описывающих особенности рассматриваемой троянской программы, позволил сделать вывод, что для ее идентификации целесообразно использовать эвристический подход на основе выделения подмножества разрешений объектов анализа. Вывод основан на специфическом наборе разрешений, требуемых для средства *Pegasus*, который является объективно избыточным для большинства известных легитимных программ. Дополнительно могут использоваться признаки используемых исследуемой программой *API*-вызовов.

Примеры опасных разрешений, которые могут использоваться в легальных случаях и наоборот, выглядят следующим образом:

```
android.permission.CALL_PHONE
android.permission.CAMERA
android.permission.DUMP
android.permission.WRITE_SMS
android.permission.READ_SMS
```

Задачей алгоритма обнаружения при такой постановке задачи заключается в идентификации запрашиваемых приложением привилегий, на основе чего делаются выводы о функционале предоставленного *APK*-файла, вызываемые инструкции, представленные в виде *Java*-кода, полученного из байт-кода программы. В результате анализа пакета программы полученные показатели передаются на блок принятия решения, который классифицирует программу как троянскую либо как безопасную.

В пакете программы выделяются признаки используемых разрешений, а также используемые *API*-вызовы, посредством которых осуществляется вредоносный функционал. Данные признаки могут быть формально представлены в виде множеств $\{P_1, \ldots, P_8\}$ – разрешения, и $\{K_1, \ldots, K_8\}$ – *API*-вызовы. Элементы первого множества представляют собой запрашиваемые привилегии, причём каждый из них может иметь весовой коэффициент ω_p, варьирующийся от 1..2 в зависимости от степени возможных последствий применения этих привилегий. Выбор весового коэффициента в большинстве случаев равен 1, однако наиболее характерные привилегии, при необходимости, отмечаются коэффициентом 2. Элементы второго множества являются сигнатурами, каждая из которых также имеет весовой коэффициент ω_s, варьирующийся от 1..4 в зависимости от степени возможных последствий.

Самый высокий коэффициент имеют сигнатуры, напрямую реализующую логику поведения трояна, минимальный коэффициент присваивается элементам множества, типичным для других семейств и, возможно, реализующих нетипичный функционал для данного вида ВПО.

Обоснование применения признаков основывается на анализе особенностей выявленных экземпляров троянских программ.

База данных сигнатур включает в себя объединение основных конструкций *Java*-приложений для ОС *Android* [5], например:

– запрос информации об устройстве: *getActiveNetworkInfo*;

– выполнение кода: *Landroid/util/Base64;->decode;exec*("*chmod* 777 */data/data/com.lenovo.safecenter/cache*");

– доступ к каталогам: */sys/devices/system/cpu/cpu0/cpufreq/*;

– *BroadcastReceiver:android.intent.action.PACKAGE_REMOVED*.

Алгоритм и средство распознавания троянской программы Pegasus

Структурная схема средства, реализующего описанный алгоритм выявления троянской программы *Pegasus*, представлена на рис. 2.

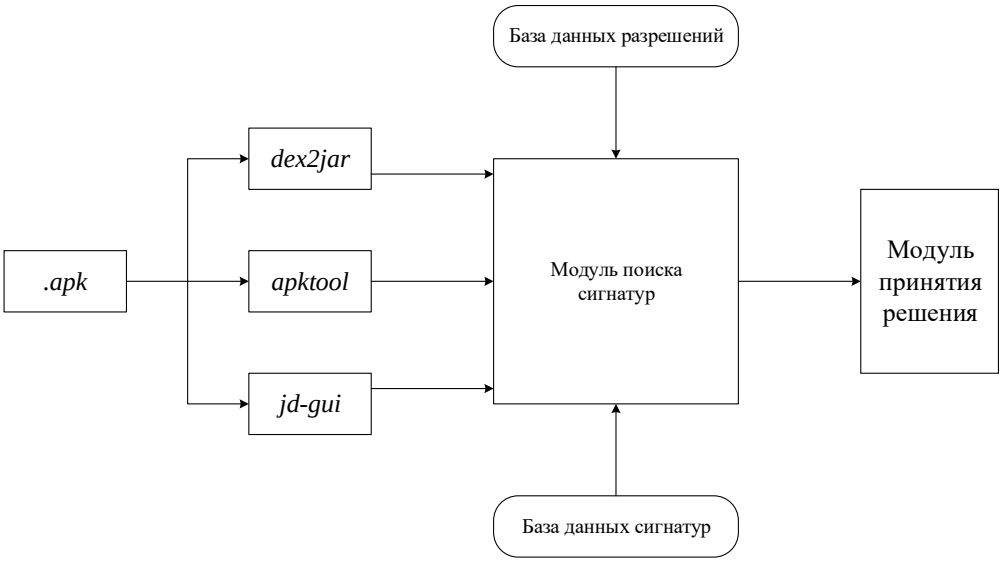


Рис. 2. Схема программного средства анализа

Состав используемых программных средств, с помощью которых выполняется дизассемблирование, декомпилирование приложения под *Android*:

1. *Dex2jar* — транслятор байт-кода *Dalvik* в байт-код *JVM*, на основе которого имеется возможность получить код на языке *Java*.

2. *Jd-gui* —декомпилятор, позволяющий получить из байт-кода *JVM* читаемый код *Java*.

3. *Apktool* - декомпиляция и компиляция установочных пакетов *Android* (**.apk*), в том числе и системных приложений, который необходим для восстановления манифеста приложения.

Порядок использования разработанного средства предполагает создание резервной копии данных с устройства (бэкапа) и передачу его программе, после чего производится анализ находящихся в ней *APK*-приложений.

Сначала с использованием приведённых выше программ восстанавливается структура приложения, после чего с использованием содержимого баз данных проводится анализ манифеста и непосредственно самого кода приложения.

Принятие решения реализована на основе решения системы уравнений:

$$\begin{cases} \left(\omega_p \cdot P_x \geq 90\right) \cap \left(\omega_s \cdot K_x \geq 105\right) = a \\ \left(\omega_p \cdot P_x \geq 40\right) \cap \left(\omega_s \cdot K_x \geq 95\right) = b \\ \left(\omega_p \cdot P_x \leq 40\right) \cap \left(\omega_s \cdot K_x \geq 105\right) = c \end{cases},$$

где $P_x \in P$, $K_x \in K$

При a=1 приложение относится к семейству троянского программного обеспечения. При b=1 алгоритм отметит приложение, как опасное. При c=1 или других случаях, не относящихся к данной системе уравнений, приложение будет являться безопасным.

Выводы

Выборка *APK*-файлов для анализа работы алгоритма обеспечила вероятность ошибки первого рода (20 %), что привело к необходимости отнесения приложения к потенциально опасным. Причина высокой вероятности ошибки первого рода вызвана высоким запросом привилегий такими приложениями, как Яндекс.*Go*, *Skype* и прочими популярными приложениями, обращающимися к геолокации пользователя, списку контактов в системе и прочими системными привилегиями, которые могут компрометировать пользователя и пересекаться с привилегиями, запрашиваемыми троянской программой, однако отслеживание данного коэффициента важно для получения информации о намерениях приложения в системе.

Список используемых источников

1. Маркин Д. О., Рыков Д. А. Методы и средства обфускации и деобфускации исходных текстов веб-приложений на языке Javascript // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. Санкт-Петербург: СПбГУТ, 2020. Т. 2. 748 с. С. 520–524.

2. Latifur Khan Latifur Khan A Machine Learning Approach to Android MalwareDetection // European Intelligence and Security Informatics Conference, 2012, pp. 141–147.

3. Qi Li Xiaoyu Li Android Malware Detection Based on Static Analysis of Characteristic Tree // International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, October 2015, pp. 84–91

4. Quentin Jérôme Kevin Allix Using opcode-sequences to detect malicious Android applications // IEEE International Conference on Communications (ICC), August 2014, pp. 914–919.

5. Применение методов машинного обучения для анализа безопасности приложений Android. URL: https://www.ruscrypto.ru/resource/archive/rc2016/files/14_pavlenko.pdf (дата обращения: 12.01.2022).

УДК 004.75
ГРНТИ 20.15.05

АНАЛИЗ ИДЕНТИФИЦИРУЮЩИХ ПРИЗНАКОВ КОНФИДЕНЦИАЛЬНОГО ТРАФИКА

А. В. Кирьянов, А. Ю. Торопцев

Академия Федеральной службы охраны Российской Федерации

Взаимодействие между распределенными сетями организаций в настоящее время преимущественно организуется при помощи сетей с коммутацией пакетов (СКП), с применением сетевого протокола взаимодействия IP. При организации связи с использованием арендованных сетей оператора, для сохранения приватности организуются различного рода туннели, в частности виртуальные частные сети (Virtual Private Network – VPN). VPN – территориально распределенная логическая сеть, организованная на базе уже существующих сетей, которая имеет сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных с помощью криптографического оборудования. С помощью данной технологии возможна передача конфиденциальной информации.

конфиденциальный трафик, MPLS L2 VPN, идентифицирующие признаки.

Под конфиденциальностью информации понимают – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [1]. Данное свойство информации защищается по средствам изолирования и шифрования трафика, проходящего по туннелям, организованным при помощи таких технологий как:

- Point-to-Point Tunneling Protocol VPN [2];
- Layer 2 Tunneling Protocol (L2TP) VPN [3];
- Site-to-Site VPN;
- IPSec [4];
- Multiprotocol Label Switching (MPLS) VPN;
- Hybrid VPN;
- MPLS L2 VPN.

Но несмотря на сокрытие передаваемой информации, возможно использование служебных данных для верификации определенного вида трафика, источника и получателя данных, а также данных, которые можно использовать для дальнейшей реализации угроз безопасности информационной системы. Подобной информацией может обладать внеш-

ний нарушитель, который при помощи различных программных и аппаратных закладок в аппаратуре оператора связи способен собирать данные о проходящем трафике.

К идентифицирующим признакам в L2 VPN MPLS туннелях можно отнести следующие параметры:

– MAC-адреса источника и получателя;
– IP-адреса источника и получателя;
– Метки MPLS сетей;
– Метки dot1q;
– Размер пакетов;
– Интенсивность трафика;
– Объем трафика.

Самым простым для инициализации трафика является *MAC* и *IP*-адреса. При рассмотрении пакета данных можно легко обнаружить адреса оборудования, которое передает этот трафик, рис. 1 и 2.

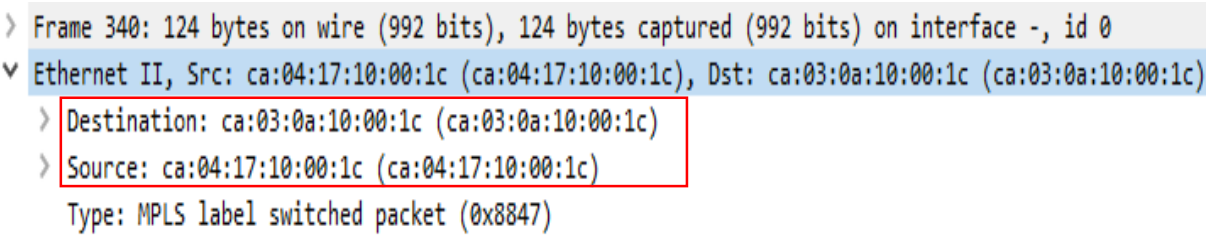


Рис. 1. MAC-адреса источника и получателя в сети с применением MPLS L2 VPN

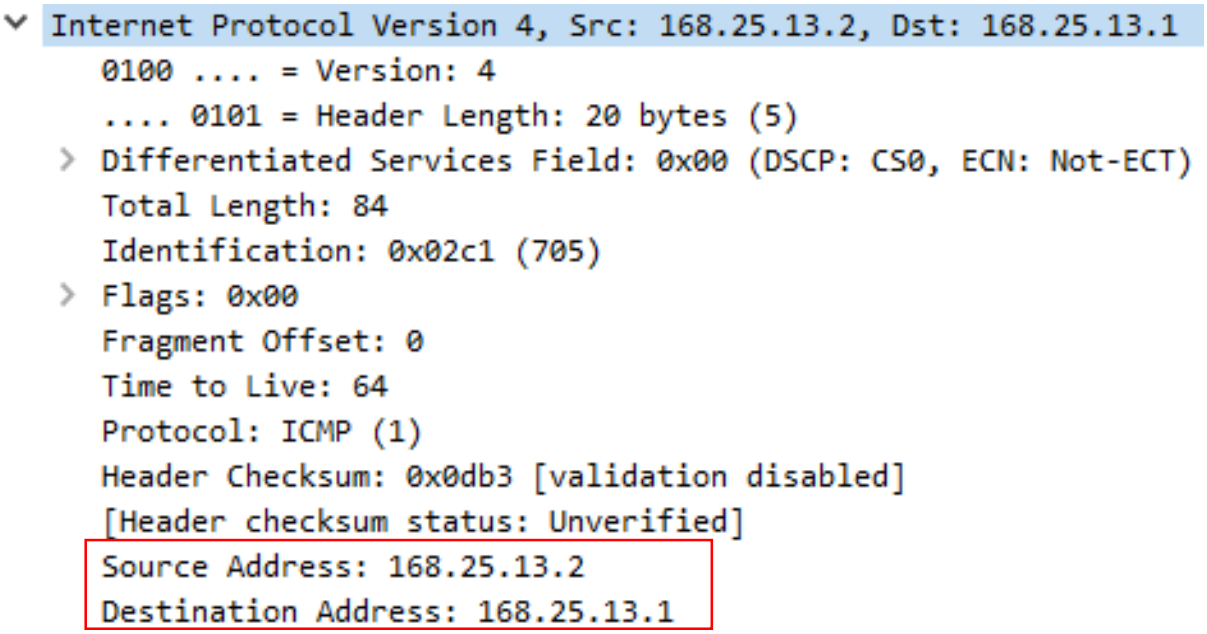


Рис. 2. IP-адреса источника и получателя в сети с применением MPLS L2 VPN

При маршрутизации с использованием MPLS меток, конфиденциальный трафик может быть идентифицирован по ним. Каждая метка по умолчанию присваивается определенной сети туннеля L2 VPN MPLS (рисунок 3) и больше сама собой не изменяется. Поэтому нарушители могут использовать данную особенность при наблюдении за трафиком.

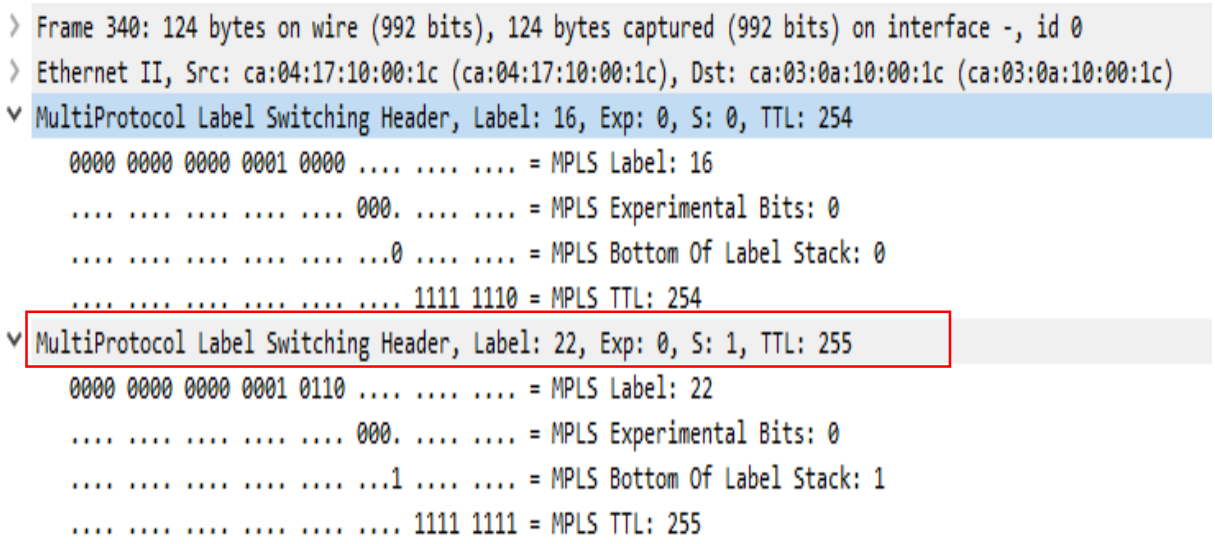


Рис. 3. Метки MPLS в сети с применением MPLS L2 VPN

В сетях с Virtual Local Area Network (VLAN – виртуальная локальная сеть) [5] разграничение и разделение трафика происходит по меткам dot1q, рисунок 4. Аналогично меткам MPLS, после присваивания им значений, сами по себе метки dot1q при прохождении по туннелю L2 VPN MPLS измениться не могут.

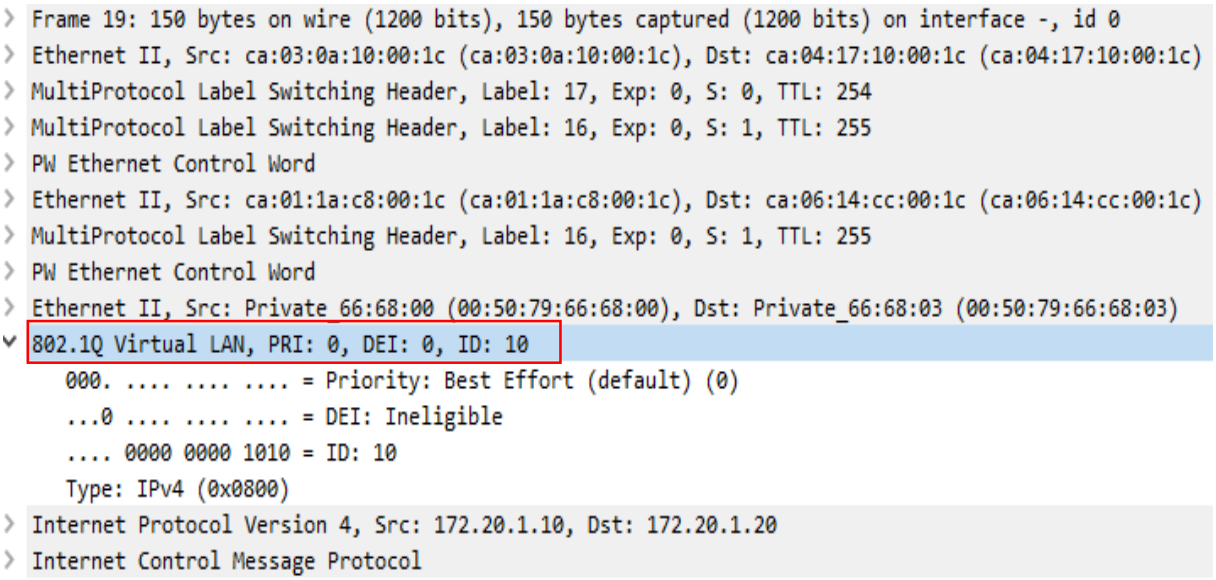


Рис. 4. Метки dot1q в сети с применением MPLS L2 VPN и настройкой VLAN

Ещё одним верификационным признаком может быть размер пакета *Ethernet*. Для многих протоколов передачи данных характерен свой собственный объем байт в каждом пакете, и именно по этой особенности можно определить какой протокол передачи используется, а, следовательно, и тип трафика, передаваемый в сети.

Распознавание трафика также может производиться по его интенсивности. В определенное время разные сервисы могут подавать различную нагрузку, которая чаще всего будет повторяться из раза в раз по определенному графику. Поэтому злоумышленник может использовать данную особенность для реализации угроз безопасности информационной системы.

При функционировании сервисов, таких как обмен мгновенными сообщениями, почтовый сервис, видеоконференцсвязь, Web-сервис, IP-телефония осуществляется передача различного объема трафика, что может быть использовано для обнаружения необходимого вида информации и нарушения одного или нескольких из свойств информации: конфиденциальность, доступность, целостность. Так, например, во время сеанса видеоконференцсвязи, при обнаружении канала его передачи, возможна угроза проведения DDoS атаки, что приведет к потере пакетов, следовательно, к ухудшению качества изображения передаваемой картинки или полному прекращению сеанса связи.

Многие из этих верификационных признаков уже активно маскируют, используя технологии преобразования сетевых адресов (Network Address Translation – NAT), трансляции порт-адреса (Port Address Translation – PAT), нормализации длин пакетов, нормализация неиспользуемых полей пакетов трафика. Целью дальнейших исследований является устранение такого идентифицирующего признака как метки MPLS в L2 VPN MPLS туннелях при помощи разработки алгоритма и создания программного средства по подмене меток в L2 VPN MPLS туннелях.

Список используемых источников

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации"

2. RFC RFC 2637 // IETF Documents. URL: https://datatracker.ietf.org/doc/rfc2637/ (дата обращения: 15.03.2022).

3. RFC RFC 2661 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc2661 (дата обращения: 15.03.2022).

4. RFC RFC 6071 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc6071 (дата обращения: 15.03.2022).

5. RFC RFC 4675 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc4675 (дата обращения: 15.03.2022).

УДК 004.056
ГРНТИ 81.93.29

СОВРЕМЕННЫЕ УЯЗВИМОСТИ В БЕЗОПАСНОСТИ РАБОТЫ *WEB*-ПРИЛОЖЕНИЙ

Е. И. Князев, А. А. Колесников

Академия Федеральной службы охраны Российской Федерации

Огромное количество web-приложений оперируют большим количеством персональных данных. Эти данные находятся между двумя противоборствующими сторонами. С одной стороны, это компании и учреждения, стремящиеся сохранить конфиденциальность данных, а также обезопасить свои информационные системы. С другой же стороны, все более опытные злоумышленники, привлеченные приманкой наживы от похищенных ими данных.

web-приложение, уязвимость, информационная безопасность, угроза.

Web-приложения, являясь общедоступными, имеют большую поверхность для атак и, возможно, различные функции со своими индивидуальными уязвимостями. Даже рассматривая защищенные *web*-сервера, работающие на безопасной операционной системе, можно обнаружить недостатки в безопасности, связанные в основном с программными ошибками в самом приложении или ошибками конфигурации сервера, на котором размещено *web*-приложение [1].

При работе с *web*-приложениями следует знать все критические уязвимости в их структуре. Для ознакомления с актуальными и наиболее серьезными угрозами *web*-приложений стоит обратиться к рейтингу *OWASP Top-10.*

OWASP (Open Web Application Security Project) – некоммерческая организация, занимающаяся вопросами безопасности *web*-приложений [2]. Данное сообщество включает в себя экспертов в области информационной безопасности со всего мира и работает надо созданием статей, рекомендаций, учебных пособий и документации, которые находятся в свободном доступе. Их проекты также включают в себя множество программ и наборов инструментов для разработки программного обеспечения с открытым исходным кодом. Уязвимости, представленные в списке *OWASP Top-10*, оценивают каждый класс недостатков на основе проведенных исследований, которые выявили, что 68 % всех *web*-приложений имеют уязвимости в системе безопасности из этого списка.

Итак, рассмотрим список угроз согласно *OWASP Top-10*, все они представлены в рейтинговой системе:

1. Нарушение контроля доступа.
2. Криптографические сбои.
3. Инъекции.
4. Небезопасный дизайн.
5. Неправильная конфигурация безопасности.
6. Использование уязвимых и устаревших компонентов.
7. Ошибки аутентификации и идентификации.
8. Ошибка целостности программного обеспечения данных.
9. Регистрация безопасности и мониторинг сбоев.
10. Подделка запросов на стороне сервера.

•Нарушение контроля доступа является самой серьезной угрозой безопасности *web*-приложений. Контроль доступа обеспечивает соблюдение политики безопасности, запрещающей пользователям системы и посторонним лицам действовать за пределами их полномочий. Из-за дефектов управления доступом неавторизированные пользователи могут проникнуть в систему и получить доступ к конфиденциальным файлам и системам и, возможно, к настойкам привилегий пользователей.

•Основными нарушениями криптографической защиты данных является сбои в работе или совсем ее отсутствие, вследствие чего происходит раскрытие конфиденциальных данных. *API*-интерфейсы, которые позволяют разработчикам подключать свои *web*-приложения к сторонним службам значительно экономят время. Однако некоторые *API* полагаются на небезопасные методы передачи данных, которые злоумышленники могут использовать для получения доступа к именам пользователей, паролям и другой конфиденциальной информации.

•В процессе инъекционной атаки злоумышленник использует недопустимые данные для внедрения их в *web*-приложение с целью осуществления недекларированных возможностей. Поскольку приложение само не может отделить код, вставленный таким образом, от своего собственного, то злоумышленники могут осуществлять различные атаки с внедрением для доступа к защищаемым данным. По статистике, самой используемой уязвимостью в безопасности *web*-приложений является SQL-запрос. К основной причине уязвимости в ходе *SQL*-запросов можно отнести отсутствие проверки и отчистки данных, используемых *web*-приложением. Можно сказать, что данная уязвимость присуще практически в любом типе технологий.

•Одной из новых уязвимостей, попавшей в рейтинг *OWASP Top-10* только в 2021 году, является небезопасный дизайн [3]. Данная категория посвящена рискам, связанным с ошибками проектирования и архитектуры. Небезопасный дизайн – это широкая категория, представляющая различные недостатки, выраженные как «отсутствующий или неэффективный дизайн элемента управления». Также, существует разница между небезопасным ди-

зайном и небезопасной реализацией. Различаются недостатки дизайна и дефекты реализации по той причине, что у них разные первопричины и методы исправления. Безопасный дизайн все еще может иметь дефекты реализации, приводящие к уязвимостям, которые могут быть использованы. Он не может быть исправлен идеальной реализацией, поскольку по определению необходимые средства безопасности никогда не создавались для защиты от конкретных атак.

•Неправильно настроенные средства контроля доступа, более общие ошибки конфигурации безопасности представляют собой огромный риск, который дает злоумышленникам быстрый и легкий доступ к конфиденциальным данным и областям сайта. Использую технику перебора, злоумышленник может увеличить успех своих противозаконных действий. Наиболее появляющимися ошибками, которые увеличивают риск атаки на *web*-приложения, являются:

– конфигурация по умолчанию;
– незащищенные файлы и каталоги;
– присутствие неиспользуемых страниц;
– неисправленные ранее выявленные ошибки.

Одной из частых ошибок *web*-мастеров – сохранение настроек *CMS* по умолчанию, на что и рассчитано большинство хаккерских атак. *CMS* – система управления контентом, являющаяся программным обеспечением, предназначенным для помощи в создании и редактировании *web*-приложений.

•Преобладание уязвимых и устаревших компонентов делают эту категорию особо опасной. Независимо от того, насколько безопасен ваш собственный код, но почти все современные приложения используют пакеты с открытым исходным кодом, и информация об уязвимостях, связанных с этими пакетами в общем доступе, а также злоумышленники могут использовать *API*, зависимости и другие сторонние компоненты, если они сами не защищены. Хотя в теории может показаться что обновление и управление уязвимыми и устаревшими компонентами простая задача, но на практике множество компаний испытывают с эти трудности. Также, фактором, усложняющим ситуацию является использование сторонних пакетов с открытым исходным кодом.

•Неправильно реализованные вызовы аутентификации и управления сеансом могут представлять огромную угрозу безопасности. Если злоумышленники заметят эти уязвимости, они смогут легко выдать себя за законных пользователей. Подтверждение личности пользователя имеет решающее значение для защиты от связанных с аутентификацией атак. Возможны недостатки аутентификации если *web*-приложение:

– разрешает использование подбора имен пользователя или паролей, а также других автоматизированных атак;

– разрешает использование пользователю стандартных или слабых паролей;

– использует слабую или неэффективную систему восстановления учетных данных и забытых паролей;

– использует простые текстовые, зашифрованные или слабо хешированные хранилища данных паролей;

– имеет неэффективную многофакторную аутентификацию, или же она совсем отсутствует;

– предоставляет идентификатор сеанса в *URL*-адресе;

– повторно использует идентификатор сеанса после успешного входа в систему;

– неправильно аннулирует идентификатор сеанса.

•Нарушение целостности программного обеспечения связано с использованием плагинов, библиотек и модулей из сомнительных источников. Если критически важные данные, используемые *web*-приложением, не проверены, злоумышленники могут подделать их, что может привести к достаточно серьезным проблемам, таким как внедрение вредоносного кода в программное обеспечение. Многие приложения теперь включают функцию автоматического обновления, где обновления загружаются без достаточной проверки целостности и применяется к ранее доверенному приложению. Вследствие чего злоумышленники потенциально могут загружать свои собственные обновления для их масштабного распространения и возможного доступа к различным приложениям.

•Полноценной уязвимостью данный пункт назвать нельзя, но в целом ведение журнала о мониторинге сбоев весьма важно, и его отсутствие или ошибки могут напрямую повлиять на видимость, оповещение об инцидентах и криминалистику. Таким образом, очень важно иметь функциональную систему ведения мониторинга для сбора данных в журнал, а также для оповещения о любых сбоях или ошибках, иначе они могут оставаться незамеченными в течение длительного времени и нанести гораздо больший ущерб. Наиболее возможные пункты, которые включены в данную уязвимость:

– вход или неудачные попытки регистрации;

– отсутствие резервирования журнала в случае сбоя сервера *web*-приложения, хранящего журналы локально;

– неправильно построенные журналы, которые не предоставляют никакой информации;

– системы мониторинга не могут обнаруживать подозрительную активность или оповещать в режиме реального времени;

– отсутствие систем мониторинга и оповещения;

– ненадежная защита журналов на предмет целостности или вообще её отсутствие.

•Подделка запросов на стороне сервера (также известная как *SSRF*) – это уязвимость *web*-безопасности, которая позволяет злоумышленнику заставить приложение на стороне сервера выполнять *HTTP*-запросы к произвольному домену по выбору злоумышленника. В типичной атаке *SSRF* злоумышленник может заставить сервер установить соединение с внутренними службами в инфраструктуре организации. В других случаях они могут заставить сервер подключаться к произвольным внешним системам, что может привести к утечке конфиденциальных данных, таких как учетные данные авторизации. Успешная атака *SSRF* часто может привести к несанкционированным действиям или доступу к данным внутри организации либо в самом уязвимом приложении, либо в других внутренних системах, с которыми приложение может взаимодействовать. В некоторых ситуациях уязвимость *SSRF* может позволить злоумышленнику выполнить произвольную команду.

Список используемых источников

1. Информационная безопасность. URL: https://2sharp.pro/infosec/ (дата обращения: 27.02.2022)

2. Что такое OWASP Top-10 и как использовать указанные риски и уязвимости. URL: https://blog.themarfa.name/chto-takoie-owasp-top-10-i-kak-ispolzovat-ukazannyie-riski-i-uiazvimosti/ (дата обращения: 26.02.2022)

3. OWASP TOP-10. URL: https://owasp.org/Top10/ (дата обращения: 25.02.2022)

Статья представлена
профессором кафедры Безопасности сетевых технологий Академии ФСО России, кандидатом технических наук, доцентом А. А. Полковым/

УДК 621.395
ГРНТИ 49.33.35

МЕТОДЫ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ СООБЩЕНИЙ

Ю. Ф. Кожанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются общие принципы симметричного шифрования с закрытыми ключами. Предложены способы повышения криптостойкости системы.

шифрование, дешифрование, криптостойкость.

Классическая модель криптосистемы приведена на рис. 1. В модели присутствуют три участника: два легальных пользователя и злоумышленник.

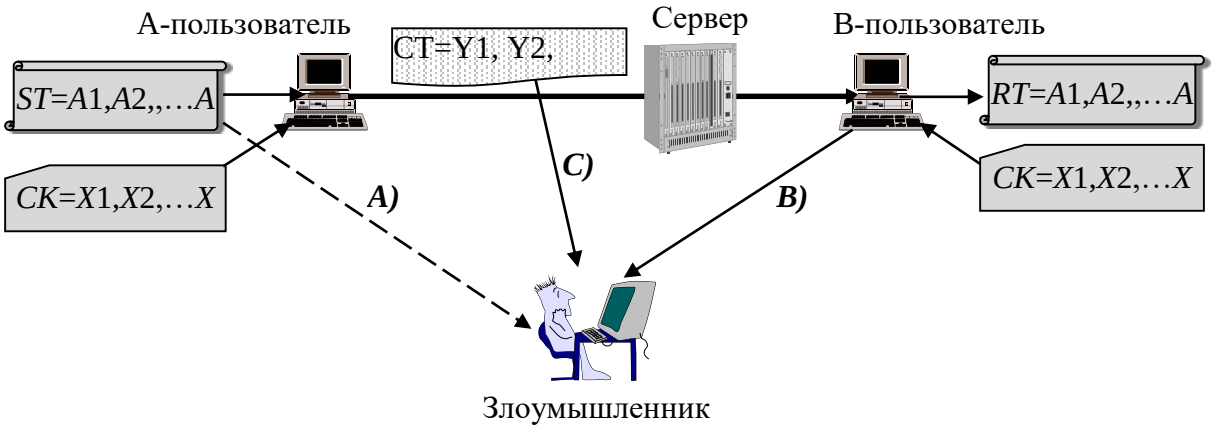


Рис. 1. Классическая модель криптосистемы

Легальные пользователи обмениваются между собой конфиденциальной информацией. Для того чтобы она была недоступна посторонним лицам, сообщение на передаче преобразуется в нечитаемый (зашифрованный) текст, который получается перемешиванием открытого текста с элементами ключа шифрования по определенному алгоритму (программе).

На приеме легальный пользователь, используя ключ дешифрования, восстанавливает исходный текст. Ключи шифрования и дешифрования могут совпадать или отличаться.

Задача злоумышленника заключается в перехвате и чтении всех передаваемых сообщений. При этом предполагается, что злоумышленник имеет возможность подключения к каналу связи и ему доступны

A) Некоторые открытые тексты.

B) Алгоритм шифрования\дешифрования передаваемых сообщений.

C) Зашифрованный текст.

Первое предположение основано на том, что злоумышленник может быть знаком с ***некоторыми*** открытыми текстами, которые могут быть похищены, подсмотрены или скопированы его соучастником.

Алгоритм шифрования\дешифрования во многих случаях не является секретом.

Зашифрованный текст легко перехватывается при использовании незащищенного канала связи.

Поэтому единственным секретом является только ключ дешифрования, который при его дискредитации и позволяет злоумышленнику читать ***все*** передаваемые зашифрованные сообщения.

Легальный А-пользователь передает открытый текст $ST = A1, A2,…An$, который шифруется секретным ключом $CK = X1, X2,…Xm$ с использованием некоторой математической или логической функции F.

На приеме легальный В-пользователь с помощью обратных преобразований (функции F^{-1}) и того же ключа *CK* восстанавливает из принятого зашифрованного текста *CT* исходный открытый текст *RT* = *ST*.

Цель злоумышленника, которому доступны только зашифрованный текст (все *Yi*) и алгоритмы шифрования/дешифрования (F и F^{-1}), заключается в подборе такого значения *CK* (всех *Xi*), чтобы при их использовании получить осмысленный текст *ST*.

Процесс шифрования можно представить в виде системы из *n* уравнений вида

$$\begin{aligned} &Y1 = F(A1, X1, X2, \ldots Xm) \\ &Y2 = F(A2, X1, X2, \ldots Xm) \\ &\ldots \\ &Yn = F(An, X1, X2, \ldots Xm), \end{aligned}$$

в которой в шифровании каждого символа участвуют все символы ключа.

Процесс дешифрования можно представить в виде системы из *n* уравнений вида

$$\begin{aligned} &A1 = F^{-1}(Y1, X1, X2, \ldots Xm) \\ &A2 = F^{-1}(Y2, X1, X2, \ldots Xm) \\ &\ldots \\ &An = F^{-1}(Yn, X1, X2, \ldots Xm), \end{aligned} \qquad (1)$$

в которой имеем (n + m) неизвестных.

При известных *CK* = (*X*1,*X*2,…*Xm*) и *CT* = (*Y*1,*Y*2,…*Yn*) с помощью функции F^{-1} из (1) нормально вычисляются все *Ai*, что и является целью дешифрования текста.

Задача дешифрации решается, если злоумышленнику известен открытый текст *ST*, который может быть похищен, подсмотрен или скопирован его соучастником. В этом случае появляется целевая функция и при известных *Ai*, *Yi* и F^{-1} путем подбора определяются все *Xi*, т.е. вскрывается значение секретного ключа.

Система (1) при случайных значениях *Ai*, *Yi* и известных и F^{-1} принципиально не решается относительно *Xi*, поскольку отсутствует целевая функция (осмысленный или известный текст).

Чтобы затруднить подбор ключа используется несколько способов, некоторые из которых приведены ниже.

1. Использование секретных ключей большой длины (m), включающие в себя буквы, цифры и некоторые символы.

При вводе ключа короткой длины производится его искусственное расширение за счет использования уже введенных символов. Например, пусть секретный ключ *СК* состоит из 3-х символов D, E, F (коды 68, 69,70) и его нужно расширить до 8 с использованием функции a·bmod251, где a и b – предпоследняя и последняя цифры текущего ключа. Тогда четвертый код ключа равен 69·70mod251 = 61, пятый – 70·61mod251 = 3, шестой – 61·3mod251=183, седьмой – 3·183mod251=47, восьмой – 183·47mod251=67. Коды расширенного ключа D, E, F, =, ETX, I, /, C.

2. Использование одноразовых ключей при каждом сеансе связи.

В этом случае даже наличие у злоумышленника текущего секретного ключа не дает ему возможность читать все последующие сообщения. Для реализации этого способа используется отдельный канал связи для передачи нового значения ключа. Например, А-пользователь по ISDN-сети сообщает очередной ключ шифрования в виде фразы «Давай поговорим сегодня». Эта фраза, точнее кодовое значение символов, и будут использованы в качестве ключа при сеансе связи, но уже через Интернет.

3. Сокрытие источника передачи информации.

Способ предусматривает назначение временного идентификатора источнику (псевдонима) при каждом новом сеансе связи. В сетях связи мобильных абонентов соответствие временного идентификатора TMSI истинному значению IMSI хранится в узле коммутации (MSC). Это позволяет маскировать источник информации, ключ которого возможно скомпрометирован. В IP-сетях следует использовать динамический IP-адрес.

4. Передача провокационных сообщений.

Суть метода состоит в передаче бессмысленных сообщений в случайные промежутки времени. Легальный пользователь после дешифрации просто отбросит это сообщение. То же самое сделает и злоумышленник, отбросив как неверный, даже правильно подобранный ключ.

Список используемых источников

1. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 600 с.

УДК 004.052.42 + 004.932.2
ГРНТИ 50.07.07

О НЕКОТОРЫХ ВАРИАНТАХ АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А. В. Козачок, С. А. Копылов, А. А. Полехин

Академия Федеральной службы охраны Российской Федерации

Дефекты и ошибки в компьютерных программах являются одной из составных частей процессов проектирования, реализации и функционирования программного обеспечения. Для повышения защищенности программного обеспечения применяются методы анализа программного обеспечения. Применение методов анализа позволяет выявить недостатки этапа разработки и отладки, а полученные результаты могут быть использованы в процессе устранения обнаруженных дефектов и корректировки исходного кода программы. В статье приведено описание средств обнаружения ошибок разработки и функционирования в процессе анализа программного кода. В процессе анализа существующих решений в области разработки безопасного программного обеспечения дано определение верификации программ, представлена классификация существующих методов верификации, описаны их основные достоинства и недостатки. Обоснован выбор символьного выполнения программ для повышения безопасности программного кода. Определены направления дальнейших исследований.

анализ программного обеспечения, безопасное программное обеспечение, символьное выполнение программ.

Широкое внедрение информационных технологий во все сферы общества привело к увеличению числа прикладного и системного программного обеспечения, позволяющего осуществлять доступ пользователей к информационным ресурсам. Помимо доступа к сервисам и услугам в процессе информационного взаимодействия может осуществляться передача персональных данных и конфиденциальной информации. Наличие указанной информации накладывает дополнительные требования на процесс разработки безопасного программного обеспечения.

Под безопасным программным обеспечением понимается программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранения мер уязвимостей программы [1]. К уязвимостям программного обеспечения (программы) относятся недостатки, обусловленные ошибками, допущенными на этапах жизненного цикла. При разработке безопасного программного обеспечения на различных этапах могут применяться методы анализа и верификации,

позволяющие обнаружить дефекты, аномалии, ошибки, а также недекларированные возможности в процессе выполнения программного обеспечения (программ).

Под анализом программного обеспечения понимается проверка соответствия создаваемых в ходе разработки и сопровождения программного обеспечения артефактов (исходный код, описание архитектуры, модель предметной области и др.) другим, ранее созданным или используемым в качестве исходных данных, а также соответствие этих артефактов и процессов их разработки правилам и стандартам [2, 3]. Частным случаем анализа является верификация, которая проверяет соответствие между нормами стандартов, описанием требований (техническим заданием) к программному обеспечению, проектными решениями, исходным кодом, пользовательской документацией и функционированием самого программного обеспечения.

К методам анализа программного обеспечения относятся [4–7]:

– экспертиза (общая и специальная);

– формальные методы (дедуктивный анализ, проверка моделей и проверка согласованности);

– статический анализ (проверка правил корректности и поиск дефектов по шаблонам);

– динамический анализ (мониторинг и тестирование);

– синтетические (гибридные) методы.

Под экспертизой программного обеспечения выступает систематическая оценка программного продукта командой квалифицированных специалистов, направленная на проверку пригодности предполагаемого использования программного продукта и выявление несоответствия со спецификациями и стандартами [8]. К общим методам экспертизы программного обеспечения относятся техническая экспертиза, сквозной контроль, инспекция и аудит. Специальные методы разделяются на следующие: организационная экспертиза, экспертиза удобства использования, экспертиза защищенности и анализ свойств архитектуры. К достоинствам методов данной группы относятся возможность обнаружения практически любых видов ошибок в программном обеспечении на любом из этапов его жизненного цикла, что позволяет сократить время существования недостатка (дефекта), а также последствий, которые он может нанести. Недостатками являются невозможность автоматизации проводимых действий, а также необходимость активной деятельности экспертов и их высокого уровня подготовленности.

Ко второй группе методов анализа программного обеспечения относятся формальные методы, основанные на использовании формальных моделей требований, поведения программного обеспечения или его окружения, в процессе анализа [9, 10]. Формальные методы могут быть применимы

только к тем объектам, которые могут быть описаны математически или иметь спецификацию, соответствующую языку верификатора. Разработка модели исследуемого объекта является недостатком присущем всем методам указанной группы и обусловлена высокой степенью трудозатрат по описанию формальной модели программного продукта. Кроме того, формальные методы, как и методы экспертизы не могут быть автоматизированы и требуют наличия специалиста, способного осуществлять верификацию.

Методы статического анализа программного обеспечения представляют собой вид работ по инструментальному исследованию программы, основанный на анализе исходного кода программы с использованием специальных инструментальных средств (статических анализаторов) в режиме, не предусматривающем реального выполнения кода [11, 12]. Все методы статического анализа исходного кода можно разделить на два вида: контроль того, что все формализованные правила корректности построения выполнены, и поиск типичных ошибок и дефектов основе некоторых шаблонов, а также комбинация указанных методов. К достоинствам методов статического анализа относится высокая степень автоматизации и простота реализации. Недостатками являются: возможность обнаружения нескольких классов ошибок (дефектов), высокие значения ложных срабатываний статического анализатора и применимость методов статического анализа только для верификации исходного кода программы.

В отличие от статических методов анализа динамические методы направлены на осуществление анализа кода программы, работы отдельных компонентов или прототипа в режиме непосредственного выполнения (функционирования) [13]. Отличительной особенностью методов данной группы является необходимость наличия полноценно функционирующей системы или ее прототипа в процессе осуществления верификации, что не позволяет использовать динамические методы на этапе проектирования и разработки программного обеспечения. Кроме того, для проведения верификации вводится этап предварительной подготовки, направленный на создания, конфигурирование системы в которой будет выполняться тестирование и набора тестов, позволяющих осуществлять анализ программного обеспечения. При этом достоинством является возможность контролировать характеристики выполнения программного кода и работы всей системы в реальном времени, что, в свою очередь, позволяет выявить дефекты (ошибки), которые не могут быть обнаружены средствами всех ранее перечисленных методов верификации.

С целью устранения существующих недостатков как статических, так и динамических методов, а также формальных методов и экспертизы широкое распространение получили синтетические (гибридные) методы анализа, представляющие собой композицию из методов анализа (верификации) разных групп [14, 15]. Так, например, в процессе анализа (верификации) может

выполняться тестирование на основе моделей или мониторинг формальных свойств и т. д. Использование гибридных методов позволяет осуществить наиболее полный анализ программного обеспечения и позволяет обнаружить дефекты (ошибки), которые не могут быть выявлены методами одной группы. К одним из таких методов верификации относятся методы символьного выполнения программ, позволяющие анализировать программный код, как в статическом режиме, так и режиме выполнения программ (программного кода).

Символьное выполнение представляет собой расширенное нормальное выполнение, обеспечивающее нормальные вычисления в особом виде представления [16]. Для этого происходит расширение вычислительных определений для базовых операций, позволяющих принимать в качестве входных данных символы и на выходе формировать символьные формулы. Для символьного выполнения изменяется семантика выполнения, но синтаксис языка и индивидуальные особенности программ, написанных на данном языке, остаются неизменными. Единственной возможность по вводу символьных объектов данных (символов, представляющих целые числа) является использование входных значений программы. Входные данные программы присваиваются как значения программных переменных. Таким образом, для осуществления обработки символьных входных данных значения переменных могут принимать значения так же, как и знаковые целочисленные константы.

Рассмотренные особенности символьного выполнения программ позволяют использовать методы данного класса в процессе как динамического, так и статического анализа программного обеспечения (программ), которые, в свою очередь, позволяют обнаруживать дефекты, аномалии и ошибок программирования на различных этапах жизненного цикла программного обеспечения. Для практической реализации методов символьного выполнения программ в процессе анализа программного обеспечения необходимо осуществить сравнительный анализ существующих подходов к символьному выполнению программ, определить их достоинства и недостатки, обосновать выбор конкретного подхода. Реализация указанных задач в процессе практической реализации символьного выполнения программ является направлением дальнейших исследований.

Список используемых источников

1. ГОСТ Р 56939–2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. М. : Изд-во стандартов, 2016. 24 с. : ил.

2. Кулямин В. В. Методы верификации программного обеспечения. URL: http://https://www.ispras.ru/publications/methods_of_software_verification. pdf. (дата обращения: 31.01.2022).

3. ISO/IEC TR 19759:2015. Software Engineering. Guide to the software engineering body of knowledge (SWEBOK). Женева : IEEE Computer society. 2015. 335 с. : ил.

4. Sanchez C. A survey of challenges for runtime verification from advanced application domains (beyond software) // Formal Methods in System Design. 2018. N 54. pp. 279–335.

5. Beyer D. Software Verification with Validation of Results // Tools and Algorithms for the Construction and Analysis of Systems. 2017. N 1. pp. 331–349.

6. Kumar R., Mullen E., Tatlock Z., Myreen M. O. Software Verification with ITPs Should Use Binary Code Extraction to Reduce the TCB // Lecture Notes in Computer Science. 2018. N 10895. pp. 362–369.

7. Родригес М., Пьяттини М., Эберт К. Верификация и валидация по: технологии и инструменты // Открытые системы. СУБД. 2019. N 2. pp. 17–24.

8. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации. М. : Радио и Связь. 2012. 192 с.

9. Hamada I. A., Sherif K., Khaled E., Amr B. A formal methods-based Rule Verification Framework for end-user programming in campus Building Automation Systems / [и др.] // Building and Environment. 2020. Vol 181. pp. 1–13.

10. Harrison M. D., Masci P., Campos J. C., Curzon P. Verification of User Interface Software: The Example of Use-Related Safety Requirements and Programmable Medical Devices // IEEE Transactions on Human-Machine Systems. 2017. T. 47, N 6. pp. 834–846.

11. Поляков С. А., Бородин А. Е. Обнаружение дефекта взаимной блокировки с помощью статического анализа // Труды Института системного программирования РАН. 2020. Т. 32, N 5. С. 21–34.

12. Бородин А. Е., Горемыкин А. В., Вартанов С. П., Белеванцев А. А. Поиск уязвимостей небезопасного использования помеченных данных в статическом анализаторе Svace // Труды Института системного программирования РАН. 2021. Т. 33, N 1. С. 7–32.

13. Бершадский А. М., Бождай А. С., Евсеева Ю. И., Гудков А. А. Исследование и разработка методов динамического анализа кода для создания самоадаптивного программного обеспечения // Моделирование, оптимизация и информационные технологии. 2018. N 2 (23). С. 108–120.

14. Blatter L., Kosmatov N., Gall P., Prevosto V., Petiot G. Static and Dynamic Verification of Relational Properties on Self-composed C Code // Lecture Notes in Computer Science. 2018. N 10895. pp. 44–62.

15. Герасимов А. Ю., Саргсян С. С., Курмангалеев Ш. Ф., Акопян Д. А., Комбинирование динамического символьного исполнения, статического анализа кода и фаззинга // Труды Института системного программирования РАН. 2018. Т. 30, N 6. С. 25–37.

16. Baldoni R., Coppa E., Delia D. C., Demetrescu C. A Survey of Symbolic Execution Techniques // ACM Computing Surveys. 2018. T. 51, N 3. pp. 1–39.

УДК 910.3:004.942
ГРНТИ 20.23.27

АНАЛИЗ МЕТОДОВ ВИЗУАЛИЗАЦИИ ОБЪЕКТОВ РЕАЛЬНОГО МИРА В ГИС

О. Н. Колбина, Е. А. Кушаков, Д. С. Матюхин, Н. В. Яготинцева

Российский государственный гидрометеорологический университет

Статья посвящена анализу методов визуализации объектов реального мира в геоинформационной системе. Определены особенности использования каждого метода, а также временные и качественные требования для использования каждого из методов. Рассмотрена законодательная база, регламентирующая разработку геоинформационных систем для визуализации объектов реального мира. Цель исследования – сформулировать рекомендации по использованию методов визуализации объектов реального мира при разработке геоинформационной системы. Задачи: рассмотреть современное состояние принципов разработки геоинформационных систем и способов визуализации информации, законодательную базу, регламентирующую разработку геоинформационных систем, и проверить наличие единства принципов разработки, ориентируясь на законодательную базу. Актуальность работы: на сегодняшний день создано множество методов визуализации объектов реального мира в геоинформационной системе, однако нельзя назвать ни один из них универсальным или прорывным в своей сфере использования.

геоинформационная система, анализ, моделирование, визуализация.

Современное общество постоянно изучает окружающий нас мир с помощью моделей карт, которые создают, просматривают и редактируют в геоинформационных системах. В настоящее время наблюдается тенденция использование геоинформационных систем в разных областях применения, так как всё больше внимания уделяется отображению на картографической проекции [1]. Однако добавление объектов в модель осуществляется двумя методами визуализации объектов реального мира в геоинформационную систему: наложение слоёв и замена слоёв. Но при этом каждый из способ визуализации предназначен для работы с видом графики: растровой или векторной. На данный момент существует государственный стандарт по геоинформационным системам, а именно ГОСТ Р 52438-2005 ГЕОГРАФИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, который регламентирует правила использования геоинформационных систем. Разработка геоинформационных систем сопровождается решением двух проблем: в выборе способа визуализации и отсутствием документов, регламентирующих разработку геоинформационных систем. Имея информацию о временных

ресурсах и качестве аппаратных характеристик, имеется возможность выбора метода визуализации, но при этом стоит учитывать, что если необходимо отображение на геоинформационной системе рельефа, то предпочтение стоит отдавать растровой графике. В существующих государственных стандартов, регламентирующих использование геоинформационных систем, отсутствуют требования к аппаратной части и временным характеристикам, что затрудняет разработку [2]. Поэтому при создании геоинформационной системы выбор метода осуществляется на ранее полученном опыте.

Наложение слоёв – метод визуализации объектов реального мира, работающий по принципу соединения отдельно существующих слоёв в единую модель, с которой пользователь в дальнейшем работает (рис. 1).

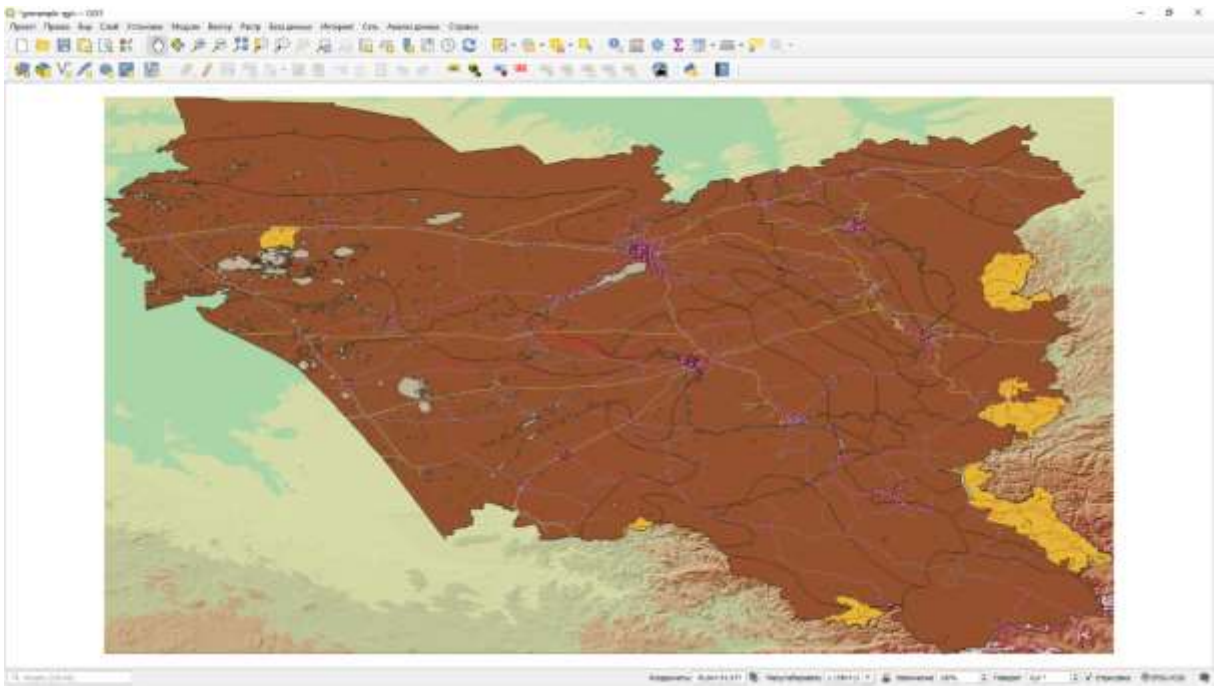


Рис. 1. Модель, созданная с помощью метода «Наложение слоёв»

Для осуществления такого метода геоинформационной системе на вход подаются исходные данные в виде слоёв на карте, а затем с помощью программного кода происходит отображение на экран в виде двумерной карты с отметками [3].

Пример наложения слоёв с помощью программного кода (PyQGIS):

```
p = Qpainter()
p.begin(img)
p.setRenderHint(QPainter.Antialiasing)
render = QgsMapRenderer()
lst = [layer.getLayerID()] # add ID of every layer
render.setLayerSet(lst)
rect = QgsRectangle(render.fullExtent())
```

```
rect.scale(1.1)
render.setExtent(rect)
render.setOutputSize(img.size(), img.logicalDpiX())
render.render(p)
p.end()
img.save("render.png","png")
```

Для данного метода в качестве временных характеристик можно рассматривать только время создания модели, так как в дальнейшем модель превращается в растровое изображение.

Время загрузки модели – 8 секунд.

При двойном увеличении объектов в модели время загрузки модели становится – 8,5 секунд, при четверном – 9 секунд, а при десятикратном – 10,5 секунд.

Качественными характеристиками для данного метода выступают изменение качества при изменении масштаба и возможность дальнейшей работы без потери продуктивности при изменении масштаба.

Так как модель становится растровым изображением, то при изменении масштаба происходит и ухудшение качества, что отрицательно влияет на продуктивность работы с моделью.

Замена слоёв – метод визуализации объектов реального мира, работающий по принципу показа в определённом месте слоя, заменяющего нынешний, при изменении масштаба (рис. 2).

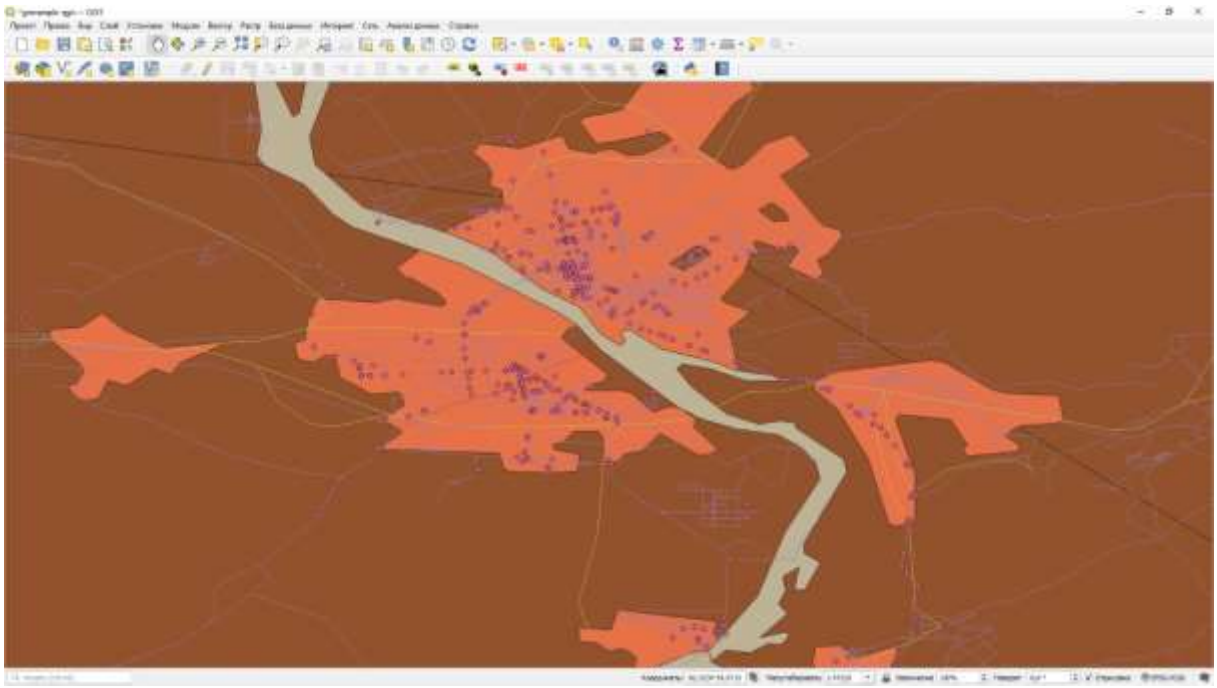


Рис. 2. Модель, созданная с помощью метода «Замена слоёв»

Для осуществления такого метода геоинформационной системе на вход подаются исходные данные в виде слоёв на карте, а затем с помощью программного кода меняется отображение на экране при изменении масштаба [4].

Пример замены слоёв с помощью программного кода (PyQGIS):

```
layers = QgsMapLayerRegistry.instance().mapLayers()
lst = layers.keys()
render.setLayerSet(lst)
render.setDestinationCrs(layers.values()[0].crs())
render.setProjectionsEnabled(True)
```

Для данного метода в качестве временных характеристик выступают время создания модели и время замены слоёв при изменении масштаба и перемещении по карте.

Время загрузки модели – 8 секунд.

При двойном увеличении объектов в модели время загрузки модели становится – 8,5 секунд, при четверном – 9 секунд, а при десятикратном – 10,5 секунд.

Время замены слоёв при изменении масштаба – 2 секунды.

При двойном увеличении объектов в модели время загрузки модели становится – 2,5 секунды, при четверном – 3 секунды, а при десятикратном – 4,5 секунды.

Время замены слоёв при перемещении по карте – 1,5 секунды.

При двойном увеличении объектов в модели время загрузки модели становится – 2 секунды, при четверном – 2,5 секунды, а при десятикратном – 4 секунды.

Качественными характеристиками для данного метода выступают изменение качества при изменении масштаба и возможность дальнейшей работы без потери продуктивности при изменении масштаба.

При изменении масштаба не происходит ухудшение качества, из-за чего продуктивность работы с моделью никак не ухудшается.

Изучив полученные данные, можно сделать вывод, что при увеличении количества объектов в модели для нахождения затрачиваемого времени действует следующая формула:

$$t = t_0 + 0.25 * n ,$$

где t – необходимое время, t_0 – время при начальных условиях, n – кратность увеличения количества объекта.

Сравнение временных и качественных характеристик методов визуализации объектов реального мира в геоинформационной системе представлено в таблице 1.

ТАБЛИЦА 1. Сравнительная таблица методов визуализации объектов реального мира в геоинформационной системе

Метод визуализации объектов реального мира в геоинформационной системе	Качество модели	Время загрузки модели	Время прогрузки данных при изменении масштаба	Время прогрузки данных при перемещении по карте
Наложение слоёв	Низкое	8 секунд	0 секунд	0 секунд
Наложение слоёв, увеличенный в 2 раза	Низкое	8,5 секунд	0 секунд	0 секунд
Наложение слоёв, увеличенный в 4 раза	Низкое	9 секунд	0 секунд	0 секунд
Наложение слоёв, увеличенный в 10 раза	Низкое	10,5 секунд	0 секунд	0 секунд
Замена слоёв	Высокое	8 секунд	2 секунды	1,5 секунды
Замена слоёв, увеличенный в 2 раза	Высокое	8,5 секунд	2,5 секунды	2 секунды
Замена слоёв, увеличенный в 4 раза	Высокое	9 секунд	3 секунды	2,5 секунды
Замена слоёв, увеличенный в 10 раза	Высокое	10,5 секунд	4,5 секунды	4 секунды

Проанализировав полученные данные, можно сделать вывод, что метод визуализации «Наложение слоёв» за счёт понижения качества модели увеличивается скорость и уменьшается время загрузки модели, но при этом обе модели имеют недоставток в виде большого времени для загрузки модели из-за постоянного сохранения в памяти технического устройства пользователя.

Анализ показал, что в настоящий момент существует два метода визуализации объектов реального мира в геоинформационной системе: наложение слоёв и замена слоёв, однако каждый из них содержит как преимущества, так и недостатки. Однако нельзя назвать лучший метод, так как

приходится выбирать между временем и качеством [5]. Если необходим более быстрый вариант, то здесь подойдёт использование метода «Наложение слоёв». Если необходим более качественный вариант, то стоит обратиться к методу «Замена слоёв».

В процессе анализа было выявлено, что необходимо разработать метод, который оптимизирует аппаратные ресурсы для обработки и отображения больших данных и дальнейшего его анализа с применением геоинформационных технологий.

Список используемых источников

1. Комин Н. А., Костяшин Н. А., Адамацкий К. Д., Яготинцева Н. В., Колбина О. Н. Геоинформационная система экологического мониторинга Санкт-Петербурга // Информационные технологии и системы: управление, экономика, транспорт, право. 2020. № 2 (38). С. 6–14.

2. ГОСТ Р 52155-2003. Географические информационные системы федеральные, региональные, муниципальные. М.: Изд-во стандартов, 2004. 243 с.

3. Ковин Р. В., Марков Н. Г. Геоинформационные системы: учебное пособие. Томск : Изд-во Томского политехнического университета, 2008. 175 с.

4. Фатхуллин Д. Р., Колбина О. Н. Использование спутников и ГИС для мониторинга экологической обстановки в арктическом регионе // Информационные технологии в образовании: межвуз. сб. науч. тр. / Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 117–121.

5. Борисова Ю. С. Создание условных знаков в геоинформационной среде QGIS для изображения сетей коммуникаций на крупномасштабных топографических планах // Актуальные вопросы землепользования и управления недвижимостью: межвуз. сб. науч. тр. / Уральский государственный горный университет. Екатеринбург, 2021. С. 52–61

6. Соколов С. Н., Родькин А. П. Области применения и перспективы развития геоинформационных систем как информационно-коммуникационных технологий // Современные исследования в науках о Земле: ретроспектива, актуальные тренды и перспективы внедрения: материалы III междунар. науч.-практ. конф. Астрахань, 05 июня 2021 г. Астрахань: ИД «Астраханский университет», 2021. С. 133-139

УДК 004.054
ГРНТИ 81.96

АНАЛИЗ ВОЗМОЖНЫХ УГРОЗ, СВЯЗАННЫХ С АРХИТЕКТУРОЙ НУЛЕВОГО ДОВЕРИЯ (ZTA)

А. А. Колесников, Н. Д. Косырев

Академия Федеральной службы охраны Российской Федерации

В данной статье кратко описана архитектура с нулевым доверием и возможные угрозы при использовании этой архитектуры. Целью данной работы является ознакомление с угрозами безопасности архитектуры нулевого доверия для более качественного обеспечения безопасности при переходе на эту архитектуру.

архитектура нулевого доверия (ZTA), нулевое доверие (ZT).

На каждом предприятии существует риск кибератак. В сочетании с существующими политиками и рекомендациями по кибербезопасности, правильно внедренная и поддерживаемая ZTA может снизить общий риск и защитить от распространенных угроз.

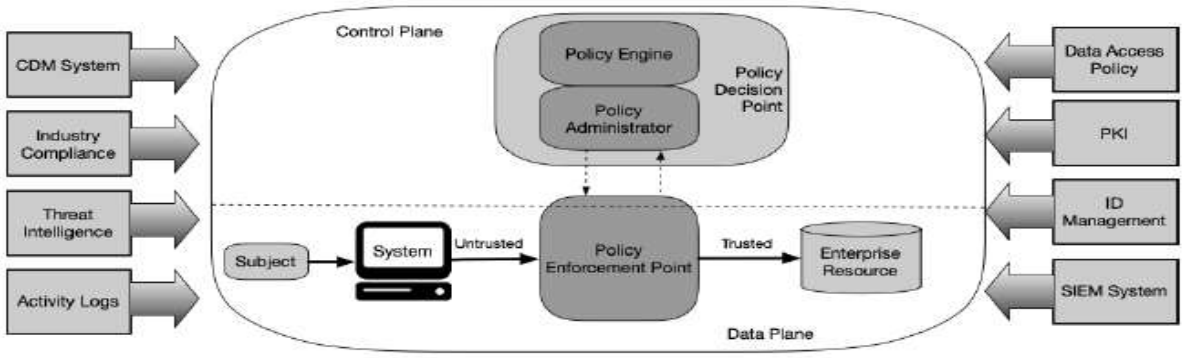


Рисунок. Архитектура с нулевым доверием [1]

Рассмотрим угрозы, которые могут иметь место в ZTA.

Подрыв процесса принятия решений

Ключевыми компонентами являются в ZTA механизм администратор политик (PA) и механизм политик (PE). Корпоративные ресурсы не взаимодействуют между собой если это не согласованно или не настроено PE (Policy Engine) и PA (Policy Administrator). Работу предприятия могут нарушить ошибки, допущенные администратором настраивающий правила PE.

Аналогично, дискредитированный PA может предоставить доступ к ресурсам, которые в противном случае не были бы одобрены. Сокращение сопутствующих рисков означает, что PE и PA необходимо контролировать и правильно настраивать, а всевозможные изменения необходимо регистрировать и проверять.

Отказ в обслуживании или нарушение работы сети

Главным компонентом для доступа к ресурсам в ZTA является PA. Ресурсы не могут взаимодействовать друг с другом без разрешения PA и соответствующих настроек. В случае если нарушитель нарушает или ограничивает доступ к PEP или PE/PA, это может неблагоприятно повлиять на работу предприятия. Вполне вероятно, что нарушитель имеет возможность перехватить трафик к PEP или PA и заблокировать его частично или для всех учетных записей пользователей предприятия. В таких случаях затрагивается только часть субъектов предприятия. Операционная ошибка может помешать функционированию всего предприятия, если механизм политик или компонент администратора политик станут недоступны из сети. Также существует риск того, что ресурсы предприятия могут быть недоступны из PA, поэтому даже если доступ предоставлен субъекту, PA не может настроить путь связи из сети. Это может произойти из-за DDoS-атаки или просто из-за неожиданного интенсивного использования.

Украденные учетные данные

ZTA, политики безопасности и отказоустойчивости, организованные по правилам, уменьшают риск получения нарушителем широкого доступа через украденные учетные данные или внутреннюю атаку. Отсутствие неявного доверия в ZT на основе сетевого расположения означает, что нарушителям необходимо завладеть устройством или учетной записью существующими на предприятии, чтобы закрепиться на нем. Правильно реализованная ZTA должна предотвращать доступ скомпрометированной учетной записи или актива к ресурсам, выходящим за рамки его обычной. Нарушители могут применять фишинг, социальную инженерию или комбинировать атаки для получения доступа к учетным записям. Для снижения риска потери информации из скомпрометированной учетной записи используется MFA для запросов на доступ. Однако, если нарушитель имеет действующие учетные данные, он все еще может получить доступ к ресурсам, которые предоставлены этой учетной записи. Алгоритм доверия работающий в ZTA с большей вероятностью обнаружит и быстро отреагирует на эту атаку, чем в традиционной сети.

Видимость в сети

Для выявления и реагирования на потенциальные атаки весь трафик проверяется и регистрируется в сети, а также подлежит анализу. В корпоративной сети часть трафика остается непрозрачной для инструментов сетевого анализа. Это трафик, который может исходить от активов, не имеющихся в организации или приложений/сервисов, не поддающихся пассивному мониторингу. Если организация не может выполнять полную проверку пакетов или исследовать зашифрованный трафик, оно должно пользоваться другими инструментами для оценки возможного нарушителя и обнаружения активного нарушителя или имеющегося вредоносного ПО в сети.

Хранение информации

Если на предприятии информация о мониторинге сети хранится и анализируется, то эти данные могут стать целью для нарушителей. Эти ресурсы так же, как и документы по сетевой архитектуре, должны быть защищены. Нарушитель успешно получивший доступ к этой информации, сможет воспроизвести примерную архитектуру предприятия и обнаружить активы для дальнейшей атаки. В ZTA существует инструмент управления, который используется для кодирования политик, он может быть целью нарушителей. Так же, как и хранимый трафик, этот компонент содержит политики доступа к ресурсам и по ним нарушитель может найти наиболее ценные учетные данные. Для хранения данных, должны быть предусмотрены надежные средства защиты для недопущения несанкционированного доступа. Эти ресурсы имеют большое значение для безопасности предприятия, и, следовательно, должны иметь максимально ограничительные политики доступа и доступ к ним должен осуществляться только из назначенных учетных записей администратора.

Использование собственных форматов данных или решений

Для принятия решений о доступе ZTA анализирует различных источники данных, а именно: информацию о запрашивающем субъекте, внешней и корпоративной разведке используемых активах, а также анализе угроз. Активы, которые используются для хранения и обработки этой информации, часто не имеют общего открытого стандарта обмена информацией и взаимодействия. Это приводит к тому, что предприятие будет привязано к большому количеству поставщиков из-за проблем с их совместимостью. При наличие у одного поставщика сбоев или проблем с безопасностью, предприятие может ощутить трудности в переходе к новому поставщику, так как это может повлечь за собой большие затраты как в денежном эквиваленте, так и по времени. Чтобы снизить такие риски, предприятия должны

проводить анализ поставщиков услуг на комплексной основе и учитывать такие факторы, как меры безопасности поставщиков, затраты предприятия на переключение и т. д.

Использование не персонифицированных субъектов (NPE), в администрировании ZTA

Для решения задач по безопасности в корпоративных сетях развертываются искусственный интеллект и другие программные средства. Эти компоненты должны взаимодействовать с компонентами управления ZTA иногда вместо администратора-человека. Возможность наличия ложных срабатываний таких как (безобидные действия, ошибочно принимаемые за атаки) и ложных срабатываний, влияющих на состояние безопасности предприятия такие как (атаки, принимаемые за обычные действия) является самым большим риском при использовании автоматизированных технологий для настройки и применения политик. Этот риск можно уменьшить с помощью постоянной перенастройки анализа для исправления ошибочных решений и улучшения процесса принятия решений. Риск заключается в том, что нарушитель может заставить или побудить NPE выполнить какую-либо задачу, на выполнение которой нарушитель имеет права. Если нарушитель может работать с NPE, он может перенастроить его и получить с помощью NPE более объемный доступ к данным или побудить его выполнить какую-либо задачу от своего имени. Также существует риск того, что злоумышленник может получить доступ к учетным данным NPE и выдать себя за него при выполнении задач.

Список используемой источников

1. NIST Special Publication 800-207 Zero Trust Architecture, February 2020. 50 p.

Статья представлена
профессором кафедры Безопасности сетевых технологий Академии ФСО России
кандидатом технических наук, доцентом А. А. Полковым.

УДК 004.9
ГРНТИ 06.73.45:81.93.29

ДЕЦЕНТРАЛИЗОВАННЫЕ ПРИЛОЖЕНИЯ И WEB 3.0

А. А. Колесников, В. И. Прокопенков

Академия Федеральной службы охраны Российской Федерации

В данной статье раскрывается понятие децентрализованных приложений, описываются механизмы работы и сферы их применения. Основным средством, рассматриваемым в работе, является блокчейн Ethereum. Описано приложение-аукцион и частично разобран его программный код и а также главные вопросы децентрализации приложений. Целью данной работы является децентрализация основных услуг, предоставляемых людям, с дальнейшим повышением безопасности и надёжности.

смарт-контракт, блокчейн, Ethereum, Dapp-приложение.

В 1990-х, когда Интернет стал общедоступным и появились первые браузеры, зародилась первая концепция сети Web 1.0. Большая часть пользователей Интернета являлась скорее потребителями, чем созидателями. Это обусловлено высокими требованиями к техническим навыкам. Данная проблема была решена только к 2000 году, когда были созданы сетевые протоколы, позволяющие пользователям гибко использовать Интернет в своих руках. Веб-сайты улучшились в графическом плане, а информацию стало проще загружать в сеть, также, как и следить за ней со стороны сетевых администраторов. Такая концепция существует и по сей день и носит название Web 2.0.

Следующий шаг в развитии Интернета лежит в основе децентрализации сети, в которой пользователи могут с уверенностью сказать, что их действия не отслеживаются. Такой концепцией выступает Web3.0, которая существует, но частично и требует глубокой проработки.

Видение, которое сформировали основатели блокчейнов было гораздо шире, чем концепция смарт-контрактов. Оно означало переосмысление интернета и создание новой системы децентрализованных приложений (DApps) с названием web3 [2]. Основная идея Web3 DApp-приложений состоит в децентрализации всех возможных аспектов функциональности приложений, таких как: хранилища, механизмы обмена сообщениями, системы наименований и т. д.

Само по себе DApp-приложение – это полностью или частично децентрализованное приложение. Его теоретическими аспектами децентрализации являются:

– серверное ПО (логика приложения);

– клиентское ПО;
– хранилище данных;
– взаимодействие с помощью сообщений;
– разрешение имен.

У DApp-приложений множество преимуществ, которыми не может похвастаться типичная централизованная архитектура. Основными из них являются:

•Устойчивость. Поскольку логика контролируется смарт-контрактом, серверная часть DApp-приложения является полностью распределенной и управляется блокчейн-платформой. В отличие от приложений, которые были запущены на центральном сервере, DApp всегда остается доступным (при условии постоянной непрерывной работы самой платформы).

•Прозрачность (транспарантность). Тот факт, что Dapp-приложение находится в блокчейне, позволяет кому угодно просмотреть его код и получить более четкое представление о его функциях. Любое взаимодействие с ним будет навсегда сохранено в блокчейн [1].

•Сопротивляемость к цензуре. Пока пользователь имеет доступ к узлу распределенного реестра (или содержит его запущенным у себя, если это необходимо), он может взаимодействовать с Dapp без какого-либо централизованного контроля. Никакой поставщик услуг или даже владелец смарт-контракта не может изменить код, развернутый в сети.

Серверная часть. DApp-приложения используют смарт-контракты для хранения программного кода. Это в своем роде замена серверной стороны, которая входит в состав обычных приложений. Главной особенностью является высокая стоимость вычислений, выполняемых смарт-контрактом, которую требуется минимизировать. Именно поэтому нужно определить какие из аспектов приложения нуждаются в доверенной и децентрализованной платформе исполнения.

Например, платформа смарт-контрактов Ethereum позволяет создать архитектуру, в которой сеть из смарт-контрактов может вызывать и обмениваться между собой данными, а также динамически читать или даже делать записи собственных состояний переменных. При развертывании собственного смарт-контракта его программный код также могут использовать другие разработчики. Важными аспектами, которые следует учитывать при проектировании смарт контрактов являются:

1. Невозможность изменения кода после их развертывания;
2. Размер DApp-приложения.

Клиентская часть. В отличие от программного кода DApp-приложения, которая требует от разработчиков понимания EVM и новых языков наподобие Solidity, клиентский интерфейс децентрализованного приложения может пользоваться стандартными веб-технологиями (HTML, CSS, JavaScript и др.). Например, к Ethereum клиентская часть обычно подключается через

JavaScript-библиотеку web3.js, которая идет в комплекте с интерфейсными ресурсами и предоставляется браузеру веб-сервером.

Хранилище данных. Из-за высокой стоимости и низкого ограничения на газ смарт-контракты плохо подходят для хранения или обработки больших объемов информации. Именно поэтому большинство DApp-приложений используют внесетевые (off-chain) сервисы хранения данных, другими словами, они хранят объемные данные за пределами блокчейна Ethereum, на специальных платформах. Эти платформы могут быть как централизованными (например, облачная БД), так и децентрализованными, будучи размещенными на следующих платформах:

- IPFS – децентрализованное хранилище с прямой доставкой контента, распределяющее хранимые объекты между участниками P2P-сети. Основная цель IPFS – заменить HTTP в качестве протокола для доставки веб-приложений. Сами файлы хранятся в IPFS, и в отличие от веб-приложений, размещаемых на единственном сервере, могут быть извлечены из любого узла данной системы.
- Swarm (решение экосистемы Ethereum) – P2P-система хранения данных, похожая на IPFS. Главное отличие заключается в использовании доступа к веб-сайту через децентрализованную P2P-систему вместо центрального веб-сервера.

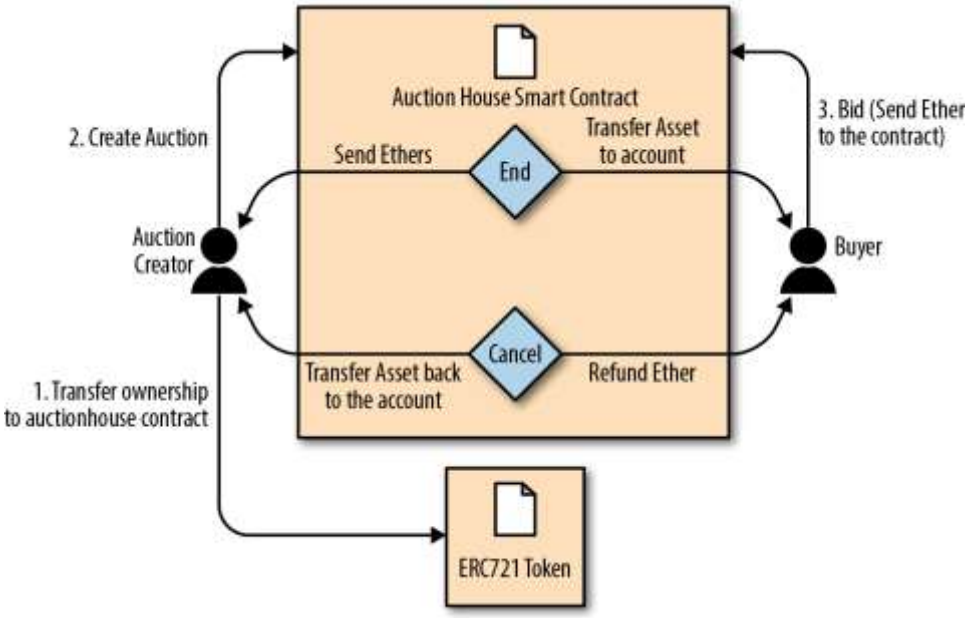


Рис. 1. DApp-приложение: пример простого децентрализованного аукциона

Теперь рассмотрим DApp-приложение на блокчейне Ethereum, в котором будет реализован децентрализованный аукцион. Данное приложение позволит пользователю зарегистрировать уникальный токен, который представ-

ляет собой некоторый актив, например дом, машину и т.д. Владение токеном после его регистрации передается приложению-аукциону, с помощью которого он может быть выставлен на продажу. Аукцион регистрирует токены, предлагая другим пользователям сделать ставки для приобретения любого из зарегистрированных токенов. По окончании аукциона владение на токен передается победителю торгов. Общая схема аукциона представлена на рис. 1.

Данное приложение опирается на два смарт-контракта, которые необходимо развернуть на блокчейне Ethereum: AuctionRepository и DeedRepository.

Для начала рассмотрим контракт DeedRepository, показанный на рис. 2. Это взаимозаменяемый токен, совместимый с ERC721.

```
pragma solidity ^0.5.16;
import "./ERC721/ERC721Token.sol";
/** * @title Repository of ERC721 Deeds
    * This contract contains the list of deeds registered by users.
    * This is a demo to show how tokens (deeds) can be minted and added
    * to the repository. */
contract DeedRepository is ERC721Token {
    /** * @dev Created a DeedRepository with a name and symbol
        * @param _name string represents the name of the repository
        * @param _symbol string represents the symbol of the repository */
    constructor(string memory _name, string memory _symbol)
        public ERC721Token(_name, _symbol) {}
    /** * @dev Public function to register a new deed
        * @dev Call the ERC721Token minter
        * @param _tokenId uint256 represents a specific deed
        * @param _uri string containing metadata/uri */
    function registerDeed(uint256 _tokenId, string memory _uri) public {
        _mint(msg.sender, _tokenId);
        addDeedMetadata(_tokenId, _uri);
        emit DeedRegistered(msg.sender, _tokenId); }
    /** * @dev Public function to add metadata to a deed
        * @param _tokenId represents a specific deed
        * @param _uri text which describes the characteristics of a given deed
        * @return whether the deed metadata was added to the repository */
    function addDeedMetadata(uint256 _tokenId, string memory _uri) public returns(bool){
        _setTokenURI(_tokenId, _uri);
        return true; }
    /** * @dev Event is triggered if deed/token is registered
        * @param _by address of the registrar
        * @param _tokenId uint256 represents a specific deed */
    event DeedRegistered(address _by, uint256 _tokenId); }
```

Рис. 2. DeedRepository.sol: deed-токен стандарта ERC721

Рассматриваемый в примере децентрализованный аукцион использует контракт DeedRepository для выпуска и отслеживания токенов для каждого аукциона. Работа самого аукциона управляется контрактом AuctionRepository. Поскольку код данного контракта слишком длинный, на рисунке 3 показаны его основное определение и структуры данных.

```
contract AuctionRepository {

    Auction[] public auctions;      // Array with all auctions
    mapping(uint256 => Bid[]) public auctionBids;       // Mapping from auction index to user bids
    mapping(address => uint[]) public auctionOwner;        // Mapping from owner to a list of owned auctions
    struct Bid {        // Bid struct to hold bidder and amount
        address payable from;
        uint256 amount; }
    struct Auction {        // Auction struct which holds all the required info
        string name;
        uint256 blockDeadline;
        uint256 startPrice;
        string metadata;
        uint256 deedId;
        address deedRepositoryAddress;
        address payable owner;
        bool active;
        bool finalized; }
contract AuctionRepository {
    Auction[] public auctions;      // Array with all auctions
    mapping(uint256 => Bid[]) public auctionBids;       // Mapping from auction index to user bids
    mapping(address => uint[]) public auctionOwner;     // Mapping from owner to a list of owned auctions
        struct Bid {        // Bid struct to hold bidder and amount
        address payable from;
        uint256 amount; }
        struct Auction {        // Auction struct which holds all the required info
        string name;
        uint256 blockDeadline;
        uint256 startPrice;
        string metadata;
        uint256 deedId;
        address deedRepositoryAddress;
        address payable owner;
        bool active;
        bool finalized; }
```

Рис. 3. ActionRepository.sol: главный смарт-контракт аукциона

Нетрудно заметить, что в данных смарт-контрактах нет специальной учетной записи или роли с особыми привилегиями по отношению к Dapp-приложению. У каждого аукциона есть владелец со специальными возможностями, но у самого приложения-аукциона нет привилегированного пользователя.

Именно это помогает децентрализовать управление приложением и отойти от какого-либо контроля по окончании его развертывания. У некоторых приложений есть одна или несколько учетных записей со специальными возможностями, например: удаление, перезапуск контракта и т. д. Такие функции управления добавляются в приложение для того, чтобы избежать потенциальных проблем, которые могут возникнуть из-за ошибки в коде [1].

Функции управления особенно сложно реализовать, поскольку они неоднозначны. С одной стороны, привилегированные учетные записи содержат в себе опасность. В случае взлома они могут подорвать безопасность всего приложения. С другой стороны, если таких учетных записей нет вовсе, теряется возможность восстановления в случае нахождения ошибки.

При разработке Dapp-приложения следует определиться с тем, хотите ли вы сделать смарт-контракты по-настоящему независимыми, производя

их запуск без дальнейшего контроля, или же вам нужны привилегированные учетные записи с потенциальным риском их компрометации. Опасность риска присутствует в любом из вариантов, но в долгосрочной перспективе настоящие децентрализованные приложения не смогут предоставлять привилегированный доступ для отдельных учетных записей – это противоречит децентрализации.

Список использованных источников

1. Andreas Antonopoulos, Gavin Wood. Осваиваем Ethereum: децентрализированные приложения (DApps) : пер. с англ. : Эксмо 2021. 521с.
2. «Web 3.0: от зари интернета до метавселенных». URL: https://rb.ru/analytics/web-3-0.

Статья представлена
профессором кафедры Безопасности сетевых технологий Академии ФСО России, кандидатом технических наук, доцентом А. А. Полковым.

УДК 004.725
ГРНТИ 49.33.35:47.39.29

СРЕДСТВО УПРАВЛЕНИЯ РАЗВЕДЗАЩИЩЕННЫМ ДОСТУПОМ НА ОСНОВЕ ЦЕПОЧКИ ПРОКСИ-СЕРВЕРОВ И СЕРВИСОВ VPN

А. А. Колесников, К. И. Сячин

Академия Федеральной службы охраны Российской Федерации

В статье раскрываются понятия виртуальной частной сети (VPN), прокси-сервера и технологии Tor-браузера. Описаны основные способы обеспечения защищенности интернет-соединения с использованием этих технологий, а также показан пример реализации цепочки прокси-серверов как средства управления разведзащищенным доступом на основе сервиса VPN. Целью работы является повышение надежности и безопасности передачи трафика для доступа к целевому ресурсу или серверу в сети «Интернет».

анонимность в сети «Интернет», VPN, цепочка прокси-серверов, Tor-браузер.

С развитием интернет-технологий все большую актуальность приобретает проблема анонимности в сети «Интернет». При работе с сетью пользователи хотят обеспечить свою приватность, минимизировать возможность

нарушения конфиденциальности передаваемых ими данных, а также получить доступ к региональному контенту. Для этого используются различные технологии: VPN-сервисы (Virtual Private Network – виртуальная частная сеть), прокси-серверы, Tor-браузер. Разберем эти понятия подробнее.

VPN – это технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, например, сети «Интернет». «Виртуальная» означает независимость от физической топологии сети. «Частная» означает ее использование ограниченным кругом лиц. Таким образом, VPN – это сервис, позволяющий защитить приватные данные при пользовании сетью «Интернет» независимо от физической топологии сети.

VPN применяется:

– для удаленной работы. через сервис VPN можно получить доступ к данным и приложениям организации при удаленной работе;

– объединения или изоляции отделов внутри организации;

– обеспечения безопасности при использовании публичных (общественных) сетей;

– получения доступа к региональному контенту;

– обеспечения анонимности в чети «Интернет» (скрытие собственной геолокации, ip-адреса, браузера, с которого производился доступ в сеть) [1].

Прокси-сервер – это промежуточный сервер в компьютерных сетях, который является посредником между пользователем и целевым ресурсом (сервером) и позволяет пользователю как выполнять запросы к другим сетевым службам (службам-демонам), так и получать ответы.

Прокси-сервер используется:

– для предоставления доступа в сеть «Интернет» пользователям локальной сети;

– снижения нагрузки на канал во внешнюю сеть и увеличения скорости получения пользователем информации путем ее кэширования (для тех прокси, которые имеют свой кэш);

– защиты локальной сети от внешнего доступа (в этом случае внешний пользователь будет видеть только ip-адрес прокси сервера, а информация об ЭВМ локальной сети ему недоступна);

– обеспечения анонимности в сети «Интернет». Прокси-сервер скрывает данные об ip-адресе пользователя, отправляющего запрос. Целевой ресурс (сервер) видит только ip-адрес прокси сервера;

– получения доступа к региональному контенту.

Tor-браузер (The Onion Router) – свободное и открытое программное обеспечение для реализации луковой маршрутизации. Это система прокси серверов, позволяющее устанавливать защищенное анонимное сетевое соединение. Анонимизация трафика обеспечивается за счет использования распределенной сети серверов – узлов. Технология Tor также обеспечивает

защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом.

Примеры реализаций технологий обеспечения приватности

VPN между серверами

Самый простой способ – это VPN между серверами или цепочка прокси-серверов. На первом этапе настроен VPN-тоннель между пользователем и сервером 1, на втором этапе – между сервером 1 и сервером 2. Так продолжается непосредственно до выхода в сеть «Интернет». Такая реализация имеет ряд недостатков, в числе которых:

– каждый промежуточный сервер имеет доступ к незашифрованным данным пользователя (на каждом этапе MTU (Maximum Transmission Unit не меняется);

– все промежуточные сервера можно увидеть при трассировке маршрута [2].

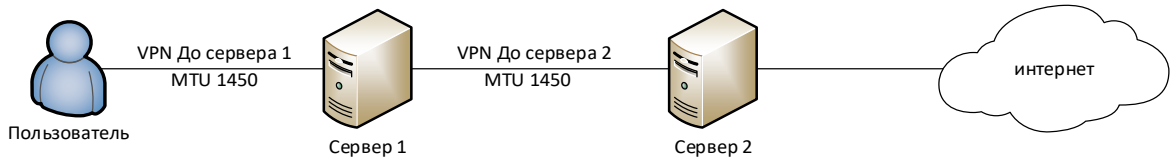


Рис. 1. Схема реализации «VPN между серверами»

VPN через прокси

Такой способ удобнее цепочки из прокси-серверов, потому что с помощью VPN легко маршрутизировать весь системный трафик в тоннель. В этом режиме прокси-сервер не видно при трассировке маршрута.

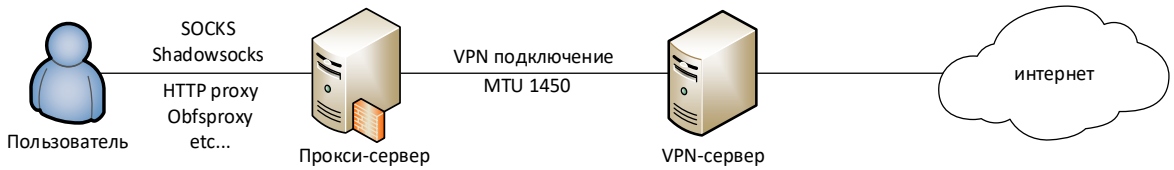


Рис. 2. Схема реализации «VPN через прокси»

Tor-браузер

Этот способ дает наилучшие показатели анонимности. Для обеспечения приватности технология Tor пропускает трафик через промежуточные серверы – узлы [3].

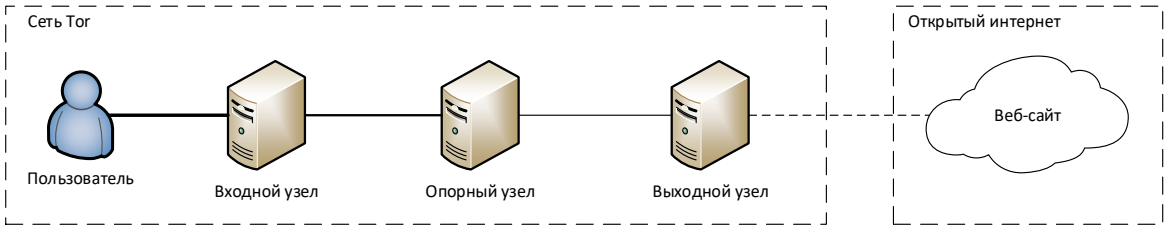


Рис. 3. Схема реализации технологии «Tor»

Три промежуточных сервера обеспечивают отличный уровень приватности пользователя:

– каждый узел знает ip-адрес только предыдущего узла – на последнем узле исходный ip-адрес потеряется;

– трафик пользователя завернут в три слоя защиты – первый и второй узел не имеют понятия об исходном трафике, а отправляет запрос в открытый интернет только выходной узел;

– чем больше узлов, тем безопаснее и быстрее работает сеть.

Технология луковой маршрутизации имеет свои недостатки:

– в сети Tor можно найти огромное количество криминального контента, из-за чего ей уделяется огромное внимание со стороны правоохранительных органов. Используя эту технологию, можно привлечь лишнее внимание (для обеспечения анонимности лучше использовать Tor совместно с другой технологией, например, с VPN);

– по сути, узлы – это пользователи сети Tor. Владельцы выходных узлов несут ответственность за исходящий от них трафик;

– владельцы выходных узлов видят проходящий через них трафик и могут отследить пользователя по косвенным признакам;

– из-за многоразового шифрования трафика, сеть Tor работает очень медленно [4].

В таблице 1 приведен перечень популярных VPN-сервисов и некоторые их характеристики.

ТАБЛИЦА 1. Перечень популярных VPN-сервисов и некоторые их характеристики

Перечень VPN-сервисов	Характеристики				
	Алгоритм шифрования трафика	Совместимость с ОС и сервисами	Ведение лог-файлов	Количество доступных серверов	Стоимость (в месяц)
NordVPN	AES-256	Windows, macOS, Android, iOS, Linux, Chrome, Firefox и роутеры	–	5 339	11,99 $
ExpressVPN	AES-256	Windows, Mac, Android, iOS, Chromebook, Kindle Fire,	–	3 000	12,95 $

Перечень VPN-сервисов	Характеристики				
	Алгоритм шифрования трафика	Совместимость с ОС и сервисами	Ведение лог-файлов	Количество доступных серверов	Стоимость (в месяц)
		веб-браузеры и роутеры			
Surfshark	AES-256	Windows, Mac, Linux, Chrome, Firefox, FireTV, Apple TV	–	Более 3 200	12,95 $
IPVanish	AES-256	Windows, Mac, Android, iOS, Amazon FireTV, Linux, Chrome OS и роутеры	–	Более 2 000	10,99$
OpenVPN	AES-256	Windows, macOS, iOS, Android, Linux, на маршрутизаторах, FreeBSD, OpenBSD, NetBSD, Solaris	–		0-3120 $ (зависит от количества подключений)
CyberGhost	AES-256	Windows, Mac, Linux, Android, iOS, веб-браузеры, стриминговые устройства и роутеры	–	Более 7 600	10,99 $

Пример реализации в локальной сети на основе цепочки прокси-серверов и сервиса VPN

Рассмотрим алгоритм реализации управления прохождением трафика в цепочке прокси-серверов для доступа к целевому ресурсу (серверу). Передача трафика между прокси-серверами происходит через OVPN-туннель.

1. ЭВМ-менеджер подключается к службе VPN (в данном случае используется OpenVPN). На каждом прокси-сервере в цепочке установлен служба-демон (агент), управляющий заменой конфигурационных файлов.

2. ЭВМ-менеджер дает команду службе-демону на замену файла конфигураций. При этом пути прохождения трафика по цепочке могут быть различными.

3. После принятия команды, служба-демон первого в цепочке прокси-сервера меняет конфигурационный файл на своем сервере и устанавливает соединения со вторым прокси-сервером. Установив соединение, служба-демон передает данные о третьем прокси-сервере службе-демону второго.

4. Службы-демоны последующих прокси-серверов поступает аналогично демону первого прокси-сервера.

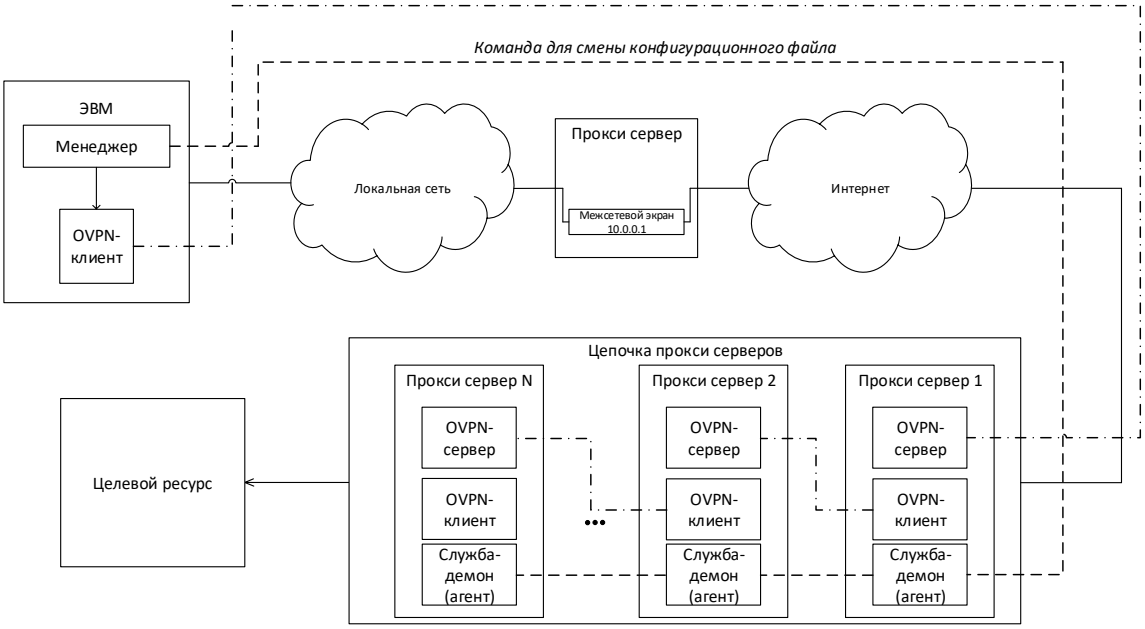


Рис. 4. Схема применения технологии

Для обеспечения защищенного соединения между серверами прокладывается OVPN-туннель – за это на каждом прокси-сервере отвечают OVPN-клиент и OVPN-сервер. Путь прохождения трафика по цепочке прокси-серверов устанавливается ЭВМ-менеджером. При использовании цепочки прокси-серверов с управлением заменой конфигурационных файлов и использовании VPN соединения достигаются хорошие показатели приватности соединения и исходный ip-адрес практически невозможно отследить.

Список использованных источников

1. VPN: ещё раз просто о сложном // Блог "Хабр": сайт. 2005–2022. URL: https://habr.com/ru/post/534250/.

2. Как работает Tor // Блог "Хабр": сайт. 2005–2022. URL: https://habr.com/ru/post/357128/. – Дата обращения: 28.03.2022.

3. Анонимность в Tor: что нельзя делать // Блог "Хабр": сайт. 2005–2022. URL: https://habr.com/ru/post/329756/.

4. Дык Буй Минь, Хуи Нгуен Нгок, Линь Лай Тхи, Хю Нгуен Ба, Чыонг Нгуен Динь Принцип работы tor-браузера // Проблемы Науки. 2017. № 1 (83). URL: https://cyber-leninka.ru/article/n/printsip-raboty-tor-brauzera.

5. Что такое VPN, Proxy, Tor? Разбор // Блог "Хабр": сайт. 2005–2022. URL: https://habr.com/ru/company/droider/blog/549212/.

Статья представлена
профессором кафедры Безопасности сетевых технологий Академии ФСО России кандидатом технических наук, доцентом А. А. .Полковым.

УДК 004.056
ГРНТИ 81.96

ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМЫ ИНТЕГРАЦИИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

А. А. Колесников, А. М. Чистякова

Академия Федеральной службы охраны Российской Федерации

В работе перечислены и дана краткая характеристика способам и подходам внедрения решения интеграции данных. Процесс интеграции данных стал одним из основных компонентов общего процесса управления данными, однако не существует универсального способа интеграции.

интеграция данных, управление данными, безопасность, консолидация данных.

Общеизвестно, что сегодня различные предприятия генерируют значительные объемы данных в своей повседневной деятельности. Данные являются одним из наиболее важных компонентов, и, взятые в целом, могут раскрыть стратегически важную информацию. Поскольку огромные объемы данных производятся каждую секунду, от них не будет никакого толка, если их не обработать должным образом, не провести анализ и не интегрировать в единый формат. Массы данных могут накапливаться и в конечном итоге становятся неуправляемыми. Именно в этих случаях и полезна интеграция данных [1].

Термин «интеграция данных» можно интерпретировать по-разному в зависимости от контекста. На первый взгляд, концепция довольно проста. Поскольку большинство предприятий хранят данные в нескольких базах данных, им приходится получать доступ к данным из разных источников и интегрировать их в единое представление.

С технической точки зрения интеграция данных – это процесс объединения данных из разных источников в единое унифицированное представление. Процесс интеграции включает использование таких подходов, как ETL (*Extract, Transform, Load* – извлечение, преобразование, загрузка), сопоставление, очистка и преобразование. В конечном счете, интеграция данных позволяет инструментам аналитики получать ценную информацию.

При этом интеграция данных довольно сложный подход. Не существует универсального способа интеграции данных, и методы постоянно развиваются. Тем не менее, процесс обычно включает в себя несколько общих элементов, таких как главный сервер, сеть источников данных и клиенты, получающие доступ к информации при взаимодействии с главным сервером.

Таким образом, появляется возможность систематически консолидировать данные из различных исходных систем и преобразовывать их в значимую и полезную информацию.

Чтобы получить целостное представление о целевой клиентской базе, нужно объединить информацию и данные из своей системы, приложений для работы с клиентами, программного обеспечения для автоматизации, электронной почты и т. д. Анализ данных становится не выполнимым, если необходимые данные не извлекаются из контролируемых источников информации.

Процесс интеграции анализируемых данных стал одним из основных компонентов общего процесса управления данными. Поскольку объем больших данных и потребность в оперативном обмене существующими информационными показателями продолжают расти, все чаще появляется необходимость использовать интеграцию данных.

Важно понимать основные принципы современной интеграции данных:

•*DevOps*. Это новый стандарт создания и реализации хранилищ данных и приложений;

•*Безопасность*. Теперь она носит системный характер и больше не является второстепенной задачей;

•*Доставка данных*. Крайне важно обеспечить ее по запросу и в режиме реального времени, поддерживая современные подходы и приложения;

•*Большое количество данных*. Со временем данные перерастают в озера данных и большие данные, распространенные в большинстве хранилищ;

•*Рабочие нагрузки*. Данные и рабочие нагрузки распределяются между общедоступными облаками, частными облаками и традиционными системами хранения данных.

Интеграция данных стала заметной в большинстве отраслей и теперь воспринимается как единственный шаг к раскрытию их полного потенциала [2]. Когда есть вся необходимая информация в одном месте, можно найти и использовать наиболее актуальные и точные сведения. Это дает конкурентное преимущество различным предприятиям.

Несколько способов, внедрения решения для интеграции данных:

•Использование больших данных.

Аналитика больших данных позволяет накапливать ценную информацию из неструктурированных, структурированных и частично структурированных данных. В результате одновременно можно интегрировать и комбинировать данные и использовать их для получения необходимой информации для принятия важных решений.

•Программное обеспечение CRM (*Customer Relationship Management* – управление взаимоотношениями с клиентами).

Предприятия используют программное обеспечение CRM для сбора информации о клиентах. Интеграция данных позволяет определять и пользоваться преимуществами, которыми обладают ценные данные.

•Аналитика.

Интеграция данных помогает собирать и преобразовывать данные в соответствии с требуемыми структурами аналитики. При этом она позволяет использовать свои критически важные процессы, такие как отчетность, информационные панели, управление эффективностью, расширенную аналитику, а также использовать тактические подходы и стратегии.

•Видимость.

Интеграция данных позволяет отслеживать и контролировать данные на протяжении всего процесса [3].

Существует множество способов и подходов к технологии интеграции данных, и можно без труда выбрать тот, который будет наиболее подходить под потребности пользователя. Каждый процесс представляет функции, которых нет у других.

Различные подходы к интеграции данных:

•Корпоративная служебная шина (ESB – *enterprise service bus*).

ESB считается критическим аспектом интеграции данных. Он предназначен для объединения множества приложений в «шинной» архитектуре. ESB помогает распределять задачи между подключенными компонентами и выступает в качестве промежуточного программного обеспечения, расположенного между набором приложений и фреймворком.

•Платформа интеграции как услуга (iPaaS).

iPaaS предоставляет централизованную консоль для управления, регулирования и интеграции облачных приложений с помощью инструментов, соединяющих облачные службы и приложения. Решения iPaaS полезны для масштабирования потребностей в производительности, структурирования интеграции на основе приложений и добавления функциональных возможностей продукта для повышения ценности их деловых отношений.

•ETL (*Extract, Transform, Load*).

Как следует из названия, необходимые данные извлекаются, преобразуются и загружаются из разрозненных источников и преобразуются в стандартный формат, что делает анализ общих данных более удобным.

•Хранилище данных.

Хранилище данных – это еще один способ консолидации и синхронизации данных. Пользователи предпочитают этот подход, поскольку хранилище данных предоставляет им достаточно информации для дальнейшего анализа.

•Консолидация данных.

Наиболее предпочтительным подходом к интеграции данных является консолидация. Поскольку необходимо извлекать, перемещать и преобразовывать огромное количество данных, процесс может усложниться. Консолидация данных – отличный способ упростить доступ к информации.

Таким образом, интеграция данных приносит пользу во всем: от доставки информации в режиме реального времени до обогащения данных, анализа данных о клиентах и аналитики. Можно сказать, что первоначальный вариант использования решения для интеграции данных – это управление клиентскими данными. Интеграция в большей степени предназначена для:

•Уменьшение сложности данных.

Как было сказано ранее, обычно администраторы работают с использованием сотен приложений и внутренних систем. Среди этих сотен приложений могут быть тысячи интерфейсов. С планом интеграции данных можно справиться со сложностями, упростить соединения и упростить стандартную доставку данных в любую систему.

•Повышение доступности данных.

Интеграция и накопление данных в единой платформе упрощает получение, проверку и анализ данных сотрудниками или партнерами. Когда данные легко доступны, руководителям проектов становится проще интегрировать любую информацию, которая необходима, поддерживать актуальность данных и обмениваться результатами. Постоянная доступность данных является ключом к обмену знаниями.

•Упрощение совместной работы с данными.

Теперь можно более эффективно сотрудничать благодаря доступу к нужным данным. Совместная работа требует обмена информацией, а благодаря простоте обмена между внутренними командами можно выполнять анализ информации более упорядоченным образом.

•Целостность данных.

Интеграция данных помогает очистить и проверить информацию, которая используется. Очень важно, чтобы данные были надежными, без ошибок, дублирования и несоответствий. Правильная стратегия интеграции может помочь сделать данные более актуальными.

В дальнейшем на первое место выходит процесс обеспечения информационной безопасности огромных объемов информации при реализации механизмов интеграция данных в информационных системах.

Список используемых источников

1. Бунин Г. П., Плущевский М. Б. Стандартизация и унификация: современный взгляд, проблемы и пути их преодоления : информационно-аналитическое и практически

ориентированное обзорно-справочное пособие: справочник // Директ-Медиа. 2019. С. 69–78.

2. Левшун Д. С. Унификация взаимодействия киберфизических систем с источниками данных // Информационные технологии и телекоммуникации. 2018. № 6 (3). С. 28–47.

3. Сенько А. В. Работа с BigData в облаках. Обработка и хранение данных с примерами из Microsoft Azure // Информационные технологии и телекоммуникации. 2018. № 6 (3). С. 12–24.

Статья представлена
профессором кафедры Безопасности Сетевых технологий академии ФСО России кандидатом технических наук, доцентом А. А. Полковым.

УДК 004.9
ГРНТИ 06.73.45:81.93.29

СМАРТ-КОНТРАКТЫ И ИХ БЕЗОПАСНОСТЬ

А. А. Колесников, И. М. Шендевицкий

Академия Федеральной службы охраны Российской Федерации

В данной статье раскрывается понятие смарт-контрактов, описываются механизмы работы и сферы их применения. Основным средством, рассматриваемым в работе, является блокчейн Ethereum. Описан процесс компиляции смарт-контракта и преобразования его в байт-код с помощью языка высокого уровня Solidity, а также главные вопросы безопасности смарт-контрактов. Целью данной работы является повышение надежности отношений между людьми при совершении ими двухсторонних сделок в Интернете.

смарт-контракт, блокчейн, Ethereum, финансы.

Термин смарт-контракт на протяжении многих лет используется для описания широкого набора разных концепций. Смарт-контракт может быть определен как договор между двумя и более сторонами об установлении, изменении или прекращении юридических прав и обязанностей, в котором часть или все условия записываются, исполняются и обеспечиваются компьютерным алгоритмом автоматически в специализированной программной среде.

С точки зрения соглашений могут быть выделены следующие виды смарт-контрактов:

- Контроль имущественных отношений – владение и проведение операций с цифровыми активами, включая криптовалюты и токены.

•Финансовые сервисы – торговое финансирование, торговля на бирже, участие в аукционах и иное;

•Кредитные обязательства – исполнение обязательств по различным формам банковских кредитных продуктов.

•Социальные сервисы – процедуры проведения голосований, выборов, процессы страхования;

•Организация управления доставкой и хранением товаров.

Практика использования смарт-контрактов на сегодняшний день сводится в основном к частичной автоматизации отдельных аспектов соглашений, таких как обмен цифровыми активами, например, обмен денежных средств на имущественные права. Однако, весьма вероятно, что по мере развития инфраструктуры и платформ на основе технологии блокчейн смарт-контракты перестанут быть только дополнением к бумажной версии документа и станут основным гарантом исполнения обязательств сторон при заключении соглашений, обеспечив переход к цифровым контрактам без необходимости их подтверждения бумажными документами [1].

Одним из примеров алгоритма, заложенного в смарт-контракте, является учет активов и осуществление операций с ними в соответствии с установленным в смарт-контракте набором условий. Алгоритм в соответствии с правилами смарт-контракта подтверждает выполнение условий контракта и автоматически определяет, должен ли указанный актив перейти к одному из участников сделки или остаться у текущего участника.

В частности, под смарт-контрактом понимается неизменяемые компьютерные программы, которые детерминистически выполняются на виртуальной машине EVM (Ethereum Virtual Machine) и являются частью сетевого протокола Ethereum – то есть запускаются на глобальном децентрализованном компьютере Ethereum.

Несмотря на то что в дальнейшем идея смарт-контракта получила широкое распространение на волне роста популярности криптовалют, смарт-контракты не обязательно должны быть связаны с технологией блокчейн, цифровыми валютами или отсутствием посредника. Смарт-контракты обычно разрабатывают на языках высокого уровня, например solidity, но перед запуском их необходимо скомпилировать в низкоуровневый байт-код, который и выполняется в EVM. После компиляции они развёртываются на платформе Ethereum. Каждый контракт идентифицируется с помощью адреса, который выводится из транзакции для создания контрактов. Этот адрес используется в качестве получателя, посылая ему средства или вызывая его функции.

Стоит отметить, что у создателя смарт-контракта нет никаких ключей, он не получает никаких особых привилегий на уровне протокола. Все смарт-контракты могут быть выполнены только в результате вызова со стороны

транзакции, инициированной учётной записью EOA (Externally Owned Account). Контракты могут вызывать учетные записи друг друга по цепочке, но первый из них всегда вызывается из EOA с помощью транзакции. Код контракта невозможно изменить. Однако контракт по заданному адресу может быть удалён вместе с его кодом и внутренним состоянием, в результате чего останется пустая учётная запись.

Безопасность – это один из самых важных аспектов, которые следует учитывать при написании смарт-контрактов. Ошибки вызывают убытки и могут стать источником уязвимости. Смарт-контракты выполняются именно так, как они написаны разработчиками, что не всегда совпадает с их намерениями. Более того, все смарт-контракты являются публичными, и любой пользователь может с ними взаимодействовать путем создания транзакций. Злоумышленники могут воспользоваться любой уязвимостью, а потери почти никогда не удается возместить. Программисту смарт-контрактов необходимо быть знакомым с наиболее распространенными рисками обеспечения безопасности, чтобы иметь возможность не допускать использования шаблонов, из-за которых контракты могут быть подвержены данным рискам.

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >0.4.0;

contract Faucet {
    address owner;
    uint256 sendAmount;
    mapping (address => uint) lastSent;
    uint blockLimit;
    function Faucet(){
        owner = msg.sender;
        sendAmount = 1000000000000000000;
        blockLimit = 5;
    }
    function getBalance() returns (uint){
        return address(this).balance;
    }
    function getWei() returns (bool){
        if(lastSent[msg.sender]<(block.number-blockLimit)&&address(this).balance>sendAmount){
            msg.sender.send(sendAmount);
            lastSent[msg.sender] = block.number;
            return true;
        } else {
            return false;
        }
    }
    function sendWei(address recp) returns (bool){
```

Рисунок. Пример кода смарт-контракта Faucet на языке Solidity

Реентерабельность. Одной из характерных черт смарт-контрактов Ethereum является способность вызывать и использовать код из других внешних контрактов. К тому же контракты обычно работают с эфиром, отправляя его по адресам разных внешних пользователей. Эти операции тре-

буют выполнения внешних вызовов. Внешние вызовы могут быть перехвачены злоумышленниками, которые способны заставить контракт выполнить дальнейший код (через функцию fallback) [2].

Атаки такого рода могут происходить, когда контракт отправляет эфир по неизвестному адресу. Злоумышленник может аккуратно создать такой с внешним адресом, который имеет вредоносный код в функции fallback. Таким образом, когда контракт пошлет на этот адрес эфир, он вызовет активацию вредоносного кода. Обычно такой код вызывает функцию из уязвимого контракта, выполняя те операции, которые не были задуманы разработчиком.

Арифметическое переполнение и антипереполнение. В виртуальной машине Ethereum для целых чисел предусмотрены типы данных фиксированного размера. Это означает, что целочисленную переменную можно представить лишь с помощью определенного диапазона чисел. Например, uint8 может хранить числа только в диапазоне от 0 до 255. Если попытаться сохранить в uint8 значение 256, получится 0. Неосторожность может привести к реализации уязвимости переменных в Solidity; например, если не проверять пользовательский ввод или выполнять вычисления, результаты которых выходят за рамки типов данных.

Переполнения и антипереполнения возникают, когда операция, требующая сохранения числа или фрагмента данных фиксированного размера, сохраняет значение, выходящее за пределы типа данных переменной. Например, в результате вычитания 1 из переменной типа uint8, равной 0, получится число 255 [1]. Переменные фиксированного размера можно считать циклическими. Такого рода арифметические подвохи позволяют злоумышленникам использовать код в своих целях, создавая неожиданные логические потоки выполнения. В качестве защиты от уязвимостей принято использовать или создавать математические библиотеки, которые заменяют стандартные математические операторы сложения, вычитания и умножения

Иллюзия энтропии. Все транзакции в блокчейне Ethereum являются детерминистическими операциями перехода состояния. Это означает, что каждая транзакция модифицирует глобальное состояние всей экосистемы Ethereum предсказуемым образом, без неопределенности. Фундаментальное последствие этого состоит в том, что в Ethereum не существует источника энтропии или случайных данных.

Распространенная проблема состоит в использовании переменных из будущего блока, содержащих информацию о блоке транзакции, значения которого (такие как хеши, временные метки, номера блоков) еще не известны. Это вызвано тем, что данные значения контролируются майнером, который генерирует блок, и поэтому они не являются по-настоящему случайными. Источник энтропии должен находиться вне блокчейна. Для этого

можно использовать взаимодействие участников с системой как схемы обязательств или изменить модель доверия на группу участников. Иначе это можно сделать с помощью централизованной сущности взаимодействующая со случайным оракулом. Переменные блока не следует использовать в качестве источника энтропии, так как майнеры могут ими манипулировать.

DoS-атаки – это очень широкая категория атак, но в ее основе лежат атаки, в которых пользователи могут парализовать работу контракта на какое-то время или, в некоторых случаях, навсегда. Из-за этого в таких контрактах может быть безвозвратно заблокирован эфир [2]. Сделать невыполнимым работу контракта можно разными способами. Смарт-контракты не должны перебирать структуры данных, которые могут быть подвержены манипуляциям со стороны внешних пользователей. Рекомендуется применять шаблон выведения средств. В случаях, когда для изменения состояния контракта требуется привилегированный пользователь, бывает, что владелец становится не дееспособным, то можно использовать защитный механизм. Решение этой проблемы заключено в создании контракта с множественными подписями, либо применение в контракте временной блокировки.

Смарт-контракты обладают значительными преимуществами по сравнению с традиционными бумажными формами заключения соглашений. Использование смарт-контрактов обладает рядом преимуществ. Возможность отказа от доверенных посредников. Отсутствие посредников позволяет участникам смарт-контракта работать на более выгодных условиях, что, в свою очередь, выражается в сокращении временных и финансовых затрат. Исполнение условий контракта происходит значительно быстрее за счет автоматизации процессов по сравнению со стандартным механизмом выполнения договора. Вся необходимая документация (не только финансовая) является частью одного смарт-контракта. Выполнение необходимых проверок, визирований, расчетов и других действий происходит моментально в нужной последовательности. Высокий уровень защищенности сторон соглашения друг от друга, так как условия контракта записываются в электронном виде и непосредственно сам контракт хранится в распределенной сети. Это делает невозможным внесение изменений в его условия без согласования другой стороной. Применение инструментов смарт-контракта дает импульс к появлению новых бизнес-моделей, что оказывает влияние на повышение конкуренции и развитие новых сервисов на финансовом рынке. При этом стоит учитывать, что, насколько бы ни была совершенна технология, всегда присутствует риск реализации уязвимостей в ИТ-системах.

Список использованных источников

1. Andreas Antonopoulos, Gavin Wood. Осваиваем Ethereum: создание смарт-контрактов и децентрализированных приложений : пер. с англ. : Эксмо 2021. 521 с.
2. Фролов А. В. Создание смарт-контрактов Solidity для блокчейна Ethereum. Практическое руководство.

Статья представлена
профессором кафедры Безопасности сетевых технологий Академии ФСО России, кандидатом технических наук, доцентом А. А. Полковым.

УДК 004.9
ГРНТИ 50.47; 73.31.81

ПРОТОТИПИРОВАНИЕ ЗАДАЧ УЧЕТА ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

Д. А. Колмакова, Я. А. Плетнев, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается проблема расширения состава учетных данных о корпоративных транспортных средствах и их актуализации за счет автоматизации оборудования высокоавтоматизированного транспорта, доступности телекоммуникационной инфраструктуры и агрегирование данных непосредственно в программном обеспечение подразделений служб эксплуатации. Представлены результаты формирования требуемой номенклатуры учетных данных, состава программного изделия, обоснования среды разработки и варианты пользовательского интерфейса как прототипирование задач учета данных в интеллектуальных транспортных системах.

учет данных, разработка, транспорт.

Активно развиваемые решения по автоматизации и интеллектуализации транспортных средств обусловливает появление в них коммуникационной многослойности, которая позволяет перейти от частных инфокоммуникационных задач детектирования различных объектов, позиционирования для безопасности дорожного движения, к обеспечению передачи в реальном масштабе времени через верхние сетевые слои коммуникаций новых потоков данных о состоянии транспортного средства и оборудовании либо непосредственно, либо через головной транспорт автоколонн в подразделения служб эксплуатации через корпоративные автоматизированные системы предприятий.

Существующий цифровой разрыв между развитием высокоавтоматизированного транспорта и технической готовностью к информационному взаимодействию программных средств предприятий можно значительно сократить за счет внедрения обоснованного в [1] агрегатора данных корпоративного мониторинга транспорта, который размещается непосредственно в подразделениях служб эксплуатации.

Требования к разрабатываемому агрегатору данных сформулированы в [2]. Агрегатор данных представляет собой функционально-распределенную систему модулей экспорта/импорта данных (обработки данных, ориентированных на определенную совокупность источников данных) и дополнительных задач модуля анализа в структуре программного средства корпоративного мониторинга транспорта, как представлено на рис. 1.

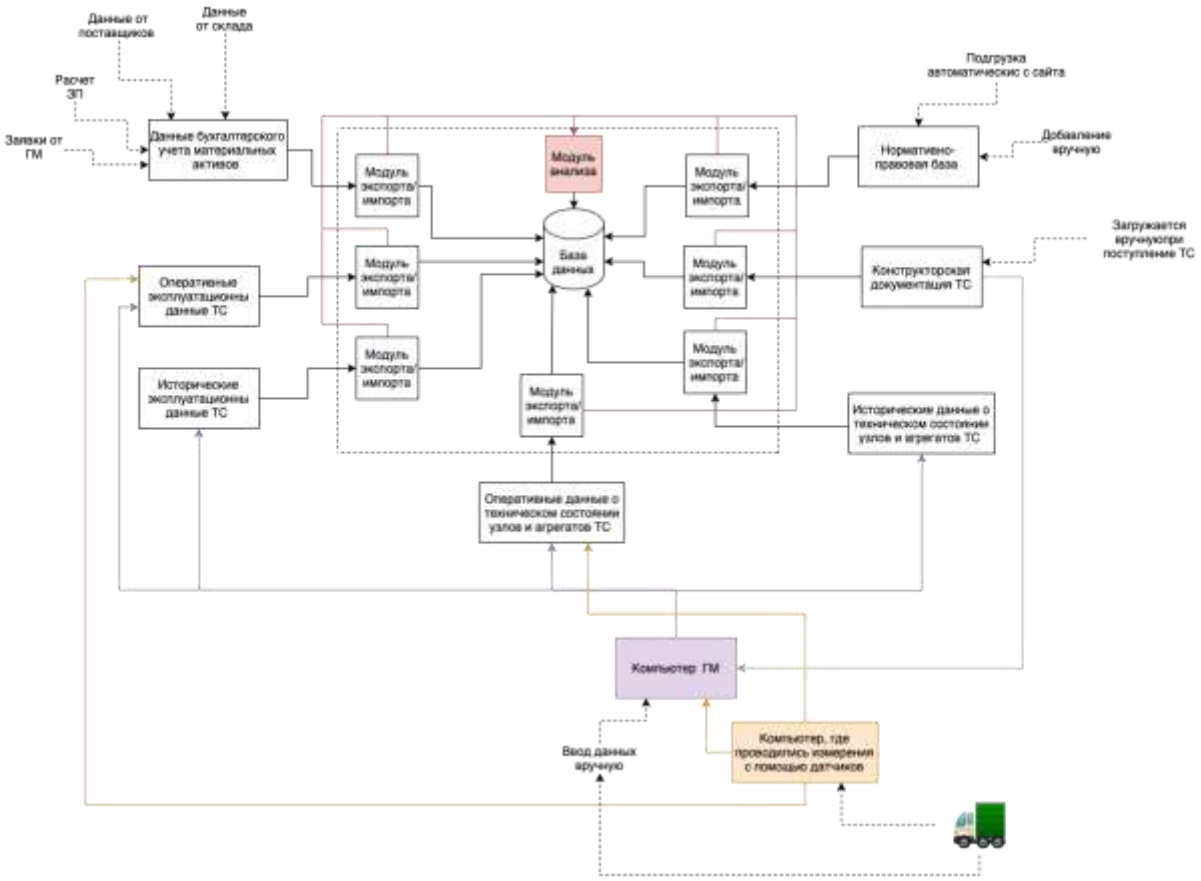


Рис. 1. Информационно-логическая модель программного средства корпоративного мониторинга транспорта

В ходе работы был проведен анализ существующих практик разработки программного обеспечения в части языков программирования, средств разработки, используемых баз данных и систем управления ими, а также ряда других аспектов с целью рационального использования имеющихся ресурсов и сокращения непроизводительных затрат времени.

Целесообразность применения тех или иных языков программирования можно определить исходя из рейтинга по индексу TIOBE Programming Community, который определяется количеством выдачи в 25 поисковых системах (например, Google, YouTube и др.) по запросу «язык программирования». По состоянию на 01.01.2022 рейтинг по 20 языкам программирования возглавляют: Python – 13,58 %; C – 12,44 %; Java – 10,66 %, C++ – 8,29 %, C# – 5,68 % [3].

Выбор стека технологий при разработке агрегатора проведен на основании анализа следующих данных: среда и способ выполнения; лицензия; импортозамещение; экосистема и комьюнити (поддержка); доступность специалистов; наличие подробной документации; стоимость поддержки; кроссплатформенность; возможность интеграции с другими решениями.

Наиболее предпочтительным подходом является разработка веб-приложения с микросервисной архитектурой, в котором сложное приложение разделено на несколько небольших независимых сервисов, взаимодействующих между собой посредством кроссплатформенного API. Вариант микросервисной архитектуры представлен на рис. 2.

Рис. 2. Микросервисная архитектура ([4])

Язык программирования C# выбран для разработки серверной части системы (backend), как наиболее подходящий для агрегатора по предъявленным критериям.

Язык программирования JavaScript выбран для разработки клиентской части агрегатора, как прототипно-ориентированный сценарный язык программирования, используемый для создания и управления динамическим содержимым веб-сайта, то есть всем, что перемещается, обновляется или иным образом изменяется на веб-странице, не требуя от пользователя перезагрузки веб-страницы вручную.

Visual Studio Code компании Microsoft определена средой разработки с учетом результатов выбора языков программирования, как автономный редактор исходного кода, работающий в Windows, macOS и Linux. VS Code подходит для языка JavaScript и веб-разработчиков, обладает множеством расширений, поддерживающих любые языки программирования [5].

Прототип пользовательского интерфейса агрегатора данных для специалистов подразделений эксплуатации корпоративного транспорта, как пер-

вое промежуточное системотехническое решение в условиях технологического развития высокоавтоматизированного транспорта и формирования многослойных коммуникаций интеллектуальной транспортной системы (инфраструктуры), представлен на рис. 3. Прототип разработан в соответствии с требованиями ГОСТ Р ИСО 9241-161-2016.

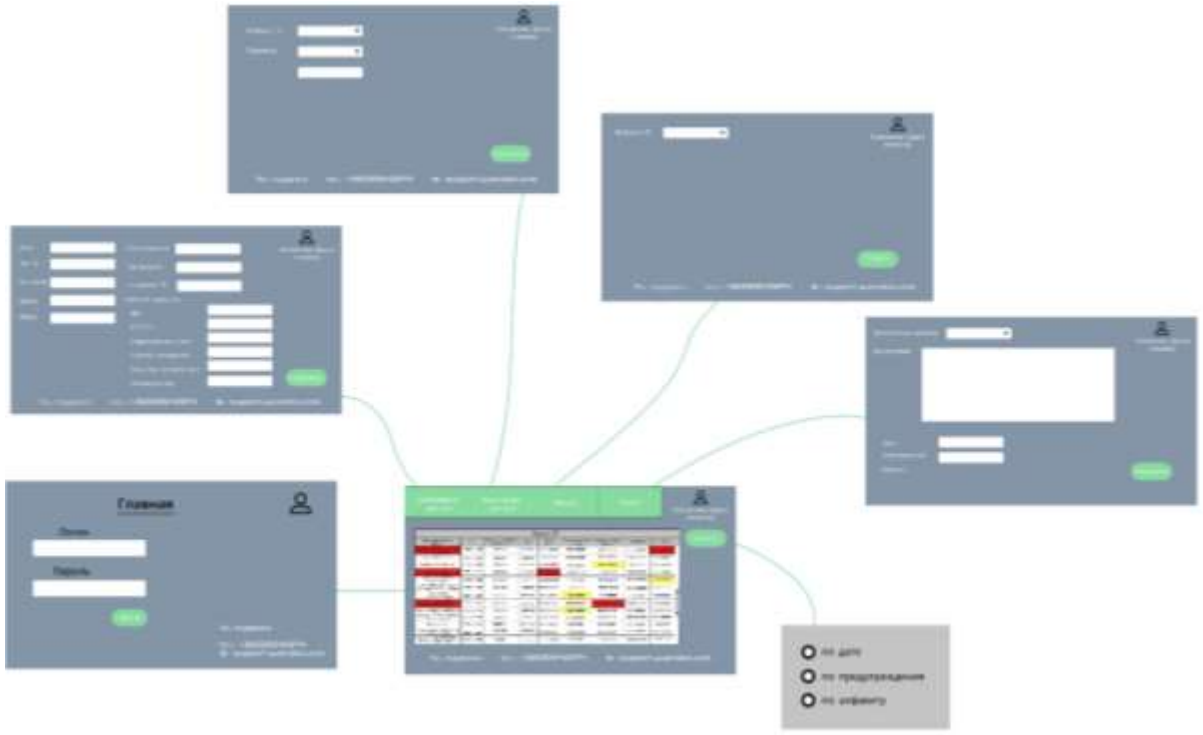


Рис. 3. Интерфейс пользовательского приложения агрегатора данных

Таким образом поиск решений по прототипированию задач учета данных в интеллектуальных транспортных системах на современном этапе можно свести к разработке и реализации предлагаемого агрегатора данных для специалистов подразделений эксплуатации корпоративного транспорта, что сократит цифровой разрыв в развитии и внедрении технологий.

Список используемых источников

1. Колмакова Д. А. Анализ технического уровня систем учета данных транспортного средства // Студенческие научные исследования: сборник статей IX Международной научно-практической конференции. В 2 ч. Ч. 1. Пенза: МЦНС "Наука и Просвещение". 2021. С. 90–95.

2. Колмакова Д. А., Плетнев Я. А., Шестаков А. В. Требования к агрегатору данных корпоративного мониторинга транспорта // Программа и порядок проведения: Всероссийская научно-методическая конференция магистрантов и их руководителей "Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021) 30 ноября – 2 декабря 2021. С.27.

3. Индекс TIOBE за январь 2022 года. URL: https://www.tiobe.com/tiobe-index (дата обращения: 28.01.2022).

4. Радченко Г. И. Распределенные вычислительные системы // кафедра СП ЮУРГУ, 2016. С. 24. URL: https://glebradchenko.susu.ru (дата обращения: 28.01.2022).

5. Семейство продуктов Visual Studio. URL: https://visualstudio.microsoft.com/ru (дата обращения: 26.01.2022).

УДК 004.9
ГРНТИ 20.01.45

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ VR В НАУЧНОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Н. А. Колосков, Е. И. Палеева, И. С. Пузанов, Д. Б. Рождественский, С. С. Сергиенко, А. В. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описываются направления применения технологий VR в образовательной и научной деятельности, выявляются преимущества этих технологии при их использовании в вузах. Приводятся результаты подробного сравнительного анализа внедрения технологий VR в передовых учебных заведениях России и зарубежья. Делаются выводы о степени распространенности технологий VR в учебных и научно-исследовательских подразделениях вузов в настоящее время.

образование, наука, высокотехнологичные проекты, инновационные технологии.

Применение VR-технологий в образовательном процессе улучшает передачу теоретических знаний студентам. Использование виртуальной реальности позволяет воздействовать не только на аудиальное или визуальное, но и комбинировать их для более яркого воздействия на студента. Повышение практических навыков помогает обучающимся быстрее адаптироваться к реальным ситуациям и усиливать эффективность процессов, связанных с получением новых знаний. Исключаются риски «поломки» дорогостоящего оборудования (станков, приборов), и причинения вреда здоровью обучающегося [1].

При применении виртуальной реальности можно выделить следующие преимущества: наглядность; вовлеченность; эффект присутствия; безопасность; фокусировка; эффективность [2].

Использование VR технологий в разных сферах образования позволяет использовать улучшать образовательные процессы. Например, в сфере здравоохранения существует множество образовательных программ, где дистанционное обучение применяется мало: хирургия, зубное протезирование

и пр. VR же позволяет осуществлять обучение в том числе частично с применением дистанционной формы без потери качества и даже с ростом эффективности обучения [3]. VR технологии в образовании применяются для дистанционного обучения, погружении в историю, визуализации объектов, эмоциональной реакции, виртуальных стажировок.

В исследовании был выполнен сравнительный анализ использования технологий виртуальной реальности в российских университетах.

1. Институт машиностроения, материалов и транспорта (СПб).

Уже с середины 2010-х использует программно-аппаратный комплекс виртуального окружения X-sided CAVE 3D. Система используется для анализа и оценки результатов моделирования технических систем – больших энергоустановок, моделей кораблей, самолетов, промышленных агрегатов. В 2016 году ИММТ начал использовать для этого шлемы HTC Vive для анализа результатов предсказательного моделирования [4].

2. Дальневосточный федеральный университет (Владивосток). Сегодня выступает важным центром VR-экспертизы в академической среде. ВУЗ первым запустил магистерскую программу по виртуальной и дополненной реальности [5].

3. Южный федеральный университет (Ростов-на-Дону). Была открыта лаборатория VR/AR-инструментов, ее задача — предоставить виртуальные среды экспериментов аспирантам-физикам и математикам, которые ставят эксперименты по фотонике и квантовым вычислениям [5].

*4. Томский политехнический университет (ТПУ). В*недряет VR-моделирование в обучение. На сайте университета есть виртуальная модель геологического полигона, для курсов «Геология», «Прикладная геология», «Технология геологической разведки», «Нефтегазовое дело». ТПУ первым открыл студентам VR-копию единственного действующего учебного реактора в России [5].

5. Институт прикладной математики и компьютерных наук (Томск). В 2019 году запустил магистерскую программу по VR и уже приступил к подготовке специалистов в области виртуальной и смешанной реальности.

6. Тихоокеанский государственный медицинский университет (Владивосток). Превым начал использовать VR в подготовке студентов к врачебной практике. Используются платформы решений MedVR, в них обучающийся отрабатывает принципы общей врачебной практики. Затем в интернатуре он встречается с реальными пациентами [5].

7. Сибирский государственный медицинский университет (СибГМУ). Начал внедрять свою VR-программу, планирует использовать виртуальную реальность для подготовки нейрохирургов, неврологов и медицинских кибернетиков

8. Самарский государственный медицинский университет (СамГМУ. В данный момент вуз разрабатывает VR-комплексы по реабилитации слуха.

Отработка одной из самых сложных практик в этой области – хирургическая операция на среднем ухе – теперь происходит в наглядной форме без риска совершить непоправимую ошибку [6].

Летом 2020 был запущен крупный проект по моделированию социальных и научных процессов с помощью VR и нейросетей в московских университетах: НИУ ВШЭ, ИПУ, ГТУ и в университете «Синергия». В рамках проекта ученые проектируют оборудование для изучения космоса, создают виртуальные прототипы в области робототехники, информатики и биотехнологий [5]. Анализ использования технологий виртуальной реальности в различных российских университетах приведен в таблице 1.

ТАБЛИЦА 1. Анализ использования технологий VR в российских вузах

Университет	Целевые направления, использующие VR	Используемое оборудование	Формат использования
ИММТ (СПб)	Машиностроение	Программно-аппаратный комплекс VR окружения 3-sided CAVE 3D, шлем	Научная деятельность, преподавание сложных дисциплин
ДВФУ (Владивосток)	Медицина, цифровое проектирование, 3D-моделирование, разработка программ	Шлемы и очки	Аудиторные занятия, преподавание сложных дисциплин
ЮФУ (Ростов-на-Дону)	Физика и математика, компьютерная графика, VR-технологии в играх	Рабочие станции, шлемы, гарнитура	Аудиторные занятия, выполнение учебных и исследовательских проектов, развитие творческих способностей
ТПУ (Томск)	Gприкладная геология, технология геологической разведки, нефтегазовое дело, создание приложений	Очки VR, бесконтактный сенсорный контроллер, джойстики	Научная деятельность, использование VR-технологий во время защит учебно-ознакомительных практик, учебно-исследовательских работ
ИПМКН (Томск)	Химия, разработка образовательных программ, разработка приложений	Очки VR, шлем, джойстики	Научная деятельность, аудиторные занятия, развитие творческих способностей
ТГМУ (Владивосток)	Врачебная практика	Специализированная медицинская VR-платформа	Аудиторные и дистанционные занятия, преподавание сложных дисциплин - обучение врачебной практике

Университет	Целевые направления, использующие VR	Используемое оборудование	Формат использования
СибГМУ (Томск)	Нейрохирургия, неврология, медицинская кибернетика	VR-платформа	Выполнение учебных и исследовательских высокотехнологичных проектов
СамГМУ (Самара)	Медицина	Системы виртуальной реальности	Выполнение учебных и исследовательских высокотехнологичных проектов
СПбГУТ (СПб)	Информационные технологии визуализации данных	Шлем и джойстики	Аудиторные занятия, развитие творческих способностей, использование для ВКР и для участия в грантах

Таким образом, можно сделать вывод, что большинство университетов используют технологии виртуальной реальности для выполнения прорывных инновационных научных проектов. Наиболее серьезные работы проводятся в медицинских университетах, где VR-технологии используют для обучения будущих врачей, позволяя им практиковаться и для выполнения научных открытий, разработок новых методов выявления болезней, реабилитации пациентов. Иногда наблюдается постепенное внедрение технологий VR в учебный процесс для повышения интереса к предмету со стороны студентов и более легкой подачи материала. Закупаются установки VR для развития творческих способностей студентов, которые позволяют им работать над собственными проектами.

Если рассматривать развитие VR технологий в зарубежных вузах, то можно отметить, что полноценное применение VR технологий в образовании на текущий момент не наблюдается, в основном в университетах ведутся дисциплины посвященные возможностям VR.

Массачусетский технологический институт, Кембридж, Массачусетс. Центр продвинутой виртуализации этого института объединяет студентов и экспертов, а также служит студией и лабораторией для поддержки творческих проектов и исследовательских предприятий. Основанная в 1985 году, MIT Media Lab является междисциплинарной исследовательской организацией, которая позволяет студентам, преподавателям и исследователям работать вместе над проектами по дисциплинам социальная робототехника, физические и когнитивные протезы, новые модели и инструменты обучения, биоинженерия сообщества, модели для устойчивых городов и другие. Также действует программа магистратуры в области медиаискусства и наук (MAS) [7].

Стэнфордский университет, Стэнфорд, Калифорния. Основные дисциплины включают в себя курсы «Как сделать VR: Введение в дизайн и разработку виртуальной реальности», «Кодирование для социального блага» (компонент VR), «Интерактивное моделирование для обучения роботов», «Компьютерная графика: анимация и моделирование» и др. Студенты CS (computer science), заинтересованные в AR/VR, имеют дополнительные возможности для совместной работы над проектами и повышения квалификации через несколько центров и лабораторий. Это Центр компьютерных исследований в области музыки и акустики (CCRMA) Virtual + Augmented Reality Design Lab, Virtual Human Interaction Lab (VHIL) и Медицинский нейрохирургический центр моделирования и виртуальной реальности Медицинской школы. Программа виртуальной реальности и иммерсивных технологий в Стэнфорде является «первой клинически ориентированной академической деятельностью, посвященной изучению иммерсивных технологий», таких как AR/VR, «в условиях психического и поведенческого здоровья в широком спектре дисциплин».

Мэрилендский университет, Колледж-Парк, Мэриленд. Это флагман Университетской системы Мэриленда (USM), которая состоит из 12 учреждений, трех региональных центров и одного системного офиса. Основанная в 1856 году, UMD обслуживает 40 700 студентов, обучающихся по 300 академическим программам. Программы для начинающих специалистов AR/VR предлагаются в Колледжах искусств и гуманитарных наук (ARHU) и компьютерных, математических и естественных науках (CMNS). Варианты включают степень бакалавра в области иммерсивного медиадизайна и степени бакалавра, магистра, и доктора философии компьютерных наук с уклоном в AR/VR [8].

По результатам анализа можно сделать следующие выводы относительно использования технологий виртуальной реальности в образовании и научной деятельности. В первую очередь удалось достигнуть понимания, насколько процесс обучения может стать оптимальнее, а исследования – успешнее. Также удалось достигнуть повышения эффективности образования с применением технологий VR. Но, следует отметить, что пока внедрение виртуальной реальности повсеместно в образовательный процесс затруднено из-за высокой стоимости оборудования.

Список используемых источников

1. Мальцева С. М., Сидоров А. Н., Захарова Э. А. Возможности и ограничения применения VR технологий в образовании при подготовке обучающихся технических специальностей // Образование и наука в современном мире. Инновации. 2021. N 5. С. 6–14.

2. Михальчук В. Д., Газизов А. Р. Виртуальная реальность или внедрение VR-систем в образование // Сборник научных статей 4-й Международной научной конференции перспективных разработок молодых ученых. 2019. С. 125–128.

3. Соснило А. И. Применение технологий виртуальной реальности (VR) в менеджменте и образовании// Управленческое консультирование. 2021. N6. С. 158–163.

4. Программно-аппаратный комплекс виртуального окружения (CAVE 3D). URL: https://immit.spbstu.ru/computer_aided_virtual_enviroment_system/ (дата обращения: 10.02.2022)

5. Павел Овчинников. Как российские университеты становятся центрами VR-компетенций. URL: https://mixr.ru/2021/01/13/vr-university/(Дата обращения: 10.02.2022)/

6. Гусенцова Ксения. Приморские студенты-медики учатся и работают в виртуальной реальности. URL: https://primorsky.ru/news/224534/?special_version=Y& (дата обращения: 10.02.2022).

7. Campus Technology. 9 Amazing Uses for VR and AR in College Classrooms. URL: https://edscoop.com/virtual-reality-technology-universities/

8. Animation Career Review. Top 50 Augmented/Virtual Reality (AR/VR) Colleges in the U.S. 2021 College Rankings. URL: https:// www.animationcareerreview.com/articles/top-50-augmentedvirtual-reality-arvr-colleges-us- 2021-college-rankings (дата обращения: 10.02.2022).

УДК 004.942
ГРНТИ 28.17.19

ВЫБОР ГРАФОВЫХ СРЕДСТВ АНАЛИЗА И ОЦЕНКИ СТРУКТУРНЫХ РИСКОВ ПРОЕКТОВ

Д. А. Криволапов, К. А. Фролова, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются пути снижения затрат с обеспечением приемлемого качества на системы поддержки принятия решений Заказчика сложных инфраструктурных проектов за счет комплексирования системотехнических решений, реализующих различные функциональные задачи, на основе оперативного использования типовых свободно распространяемых программных средств общего применения и их бесшовного взаимодействия. Исследуются процедуры анализа и выбора программных средств для сбора актуальных пространственных данных в атрибутах спецификаций развертываемых объектов (линейных и площадных), общность контролируемых параметров различных проектов и уровень взаимовлияния результатов их поэтапной реализации, а также процедуры анализа и выбора программных средств графового моделирования. Представлены результаты применения варианта комплексирования выбранных программных средств.

сети связи, инфраструктурный проект, риск-параметры, графовая модель.

При проектировании и развертывании сетей связи решаются, как правило, комплексные задачи инфраструктурных проектов. Инфраструктурные

проекты относятся к группе сложных проектов, в которых технические, экономические и временные показатели имеют определенный уровень взаимозависимости от результатов их поэтапной реализации. Для управления реализацией инфраструктурных проектов заказчиками создается система поддержки принятия решений, которая должна выполнять различные функциональные задачи с требуемым качеством при минимальных затратах.

При развертывании или обеспечении функционирования проектов реализуется задача визуализации представления их топологических характеристик и некоторых атрибутов, связанных с наличием сетевых элементов, их сетевых характеристик, таких как связность, мощность связности, для представления их в графическом виде (графовая модель).

Результаты решения проектов не являются статическими или законченными, все они находятся в динамическом состоянии по построению различных компонент, их модернизации или их умощнению.

Соответственно, для такого рода топологических структур присущи различные риски, связанные с реализацией проектов по модернизации и совершенствованию [1], особенно те, которые имеют наибольший негативный эффект при их наступлении в результате либо несвоевременного, либо некачественного выполнения запланированных работ, так называемые «риск-параметры».

Вместе с тем в системах поддержки принятия решений таких проектов осуществляют плановый мониторинг различных показателей с целью своевременного предотвращения ситуаций, связанных с наступлением событий при фактическом наступлении риска.

Для обеспечения математической и алгоритмической поддержки рациональных решений по управлению риск-параметрами проектов предлагается проводить расчет риск-параметров с применением комплексных методик оценки как топологических характеристик, так и атрибутов, которые представляют сведения о влиянии нескольких риск-параметров различных программных мероприятий или работ, которые ведутся по различным темам и собственным независимым траекториям [2].

Топологическими характеристиками являются координаты сетевых устройств и оборудования (линейных и площадных объектов), соответствующие характеристики их функционирования, а также сетевые характеристики обеспечения устойчивости и живучести информационных направлений и направлений связи.

Представление текущего состояния результатов инфраструктурного проекта возможно в виде топологической структуры с применением программных средств геоинформационных систем (ГИС) (рис. 1). Например, иерархическая радиальная структура требует поддержания функционирования (совершенствования) регенерационных участков, линий связи, необслу-

живаемых усилительных пунктов, распределительных устройств, мультиплексного оборудования доступа к линиям связи, соответствующее оборудование маршрутизации (коммутации) для распределения или формирования информационных потоков, трактов. Стадии развития участка сети связи в два этапа с использованием средств ГИС представлены на рис. 2–3.

Рис. 1. Состояние инфраструктурного проекта

Рис. 2. Результаты 1 этапа инфраструктурного проекта

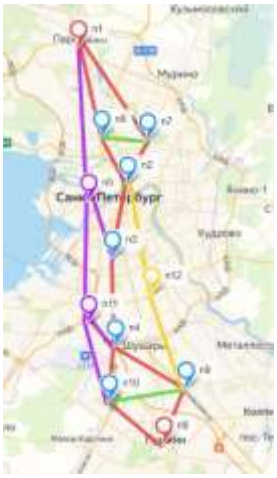


Рис. 3. Результаты 2 этапа инфраструктурного проекта

Оценка результатов мониторинга состояния реализации инфраструктурных проектов может быть обеспечена только на основе графовых моделей, например, в виде взвешенного неориентированного графа. Вершины и ребра такого графа будут соответствовать географическому расположению реальных объектов инфраструктуры.

С целью выбора возможного применения и оперативного использования типовых свободно распространяемых программных средств общего применения и их бесшовного взаимодействия проведен анализ существующих решений.

Результаты оценки применимости пяти графовых программных средств для задач моделирования инфраструктурных проектов приведены в таблице и на рис. 4.

ТАБЛИЦА. Оценка программных средств для использования в модуле компьютерных систем графового моделирования

Параметр	Наименование программного обеспечения				
	yEd	Gephi	Tulip	Cytoscape	Graphviz
1. Возможность работы на разрешенных операционных системах в органах исполнительной власти	1	1	1	1	1
2. Применяемые средства разработки	0,8	0,8	0,7	0,8	0,6

Параметр	Наименование программного обеспечения				
	yEd	Gephi	Tulip	Cytoscape	Graphviz
3. Распространение	0,5	0,8	0,8	0,8	0,8
4. Поддерживаемые форматы импорта данных	0,6	0,5	0,6	0,8	0,3
5. Поддерживаемые форматы экспорта данных	0,9	0,6	0,3	0,9	0,6
6. Наличие функционала для оценки структурных рисков	0,3	0,3	0,3	0,4	0,1

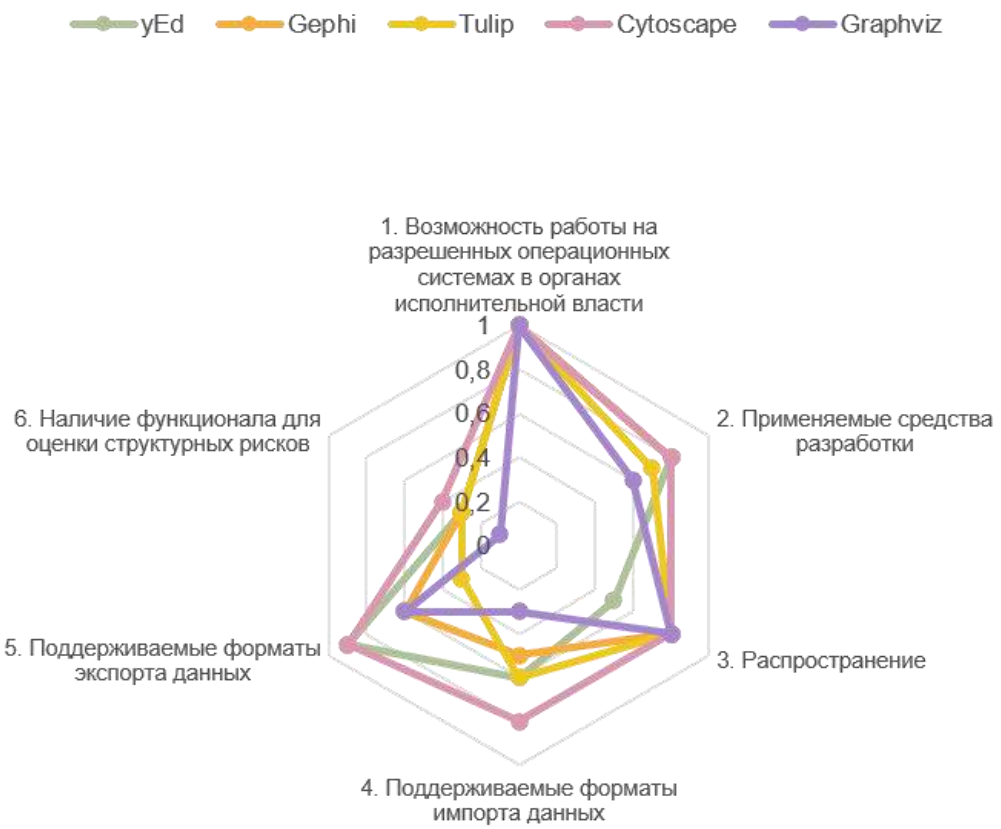


Рис. 4. Результаты оценки существующих графовых программных средств

С целью валидации свободно распространяемого программного обеспечения Cytoscape[1], наиболее рационального графового программного средства, построена графовая модель исходного состояния сети связи (рис. 5), графы этапов развития сети (рис. 6–7), соответствующие представленным структурам на рис. 2–3.

[1] Cytoscape (URL: https://cytoscape.org/).

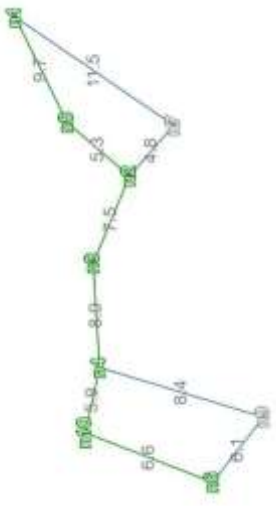


Рис. 5. Графовая модель исходного инфраструктурного проекта

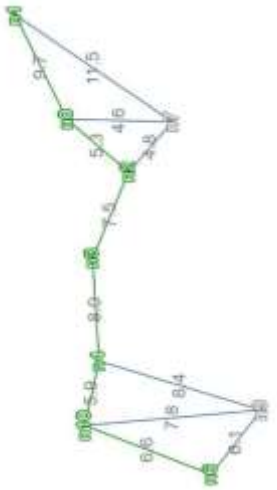


Рис. 6. Результат 1 этапа инфраструктурного проекта

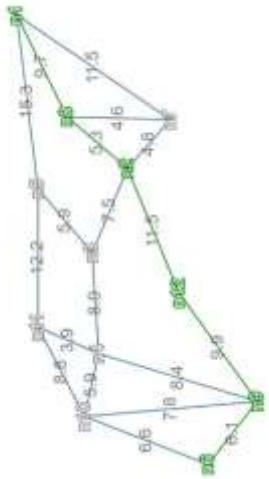


Рис. 7. Результат 2 этапа инфраструктурного проекта

Проведенный анализ функциональных возможностей существующих программных средств графового моделирования выявил необходимость дополнительной реализации модуля экспорта/импорта данных для бесшовного их взаимодействия с программными средствами геоинформационных систем и средствами визуализации систем поддержки принятия решений Заказчика инфраструктурных проектов.

Реализацию интегрированного использования данных в управлении процессами поддержания функционирования подсистем и проектами развития элементов взаимовлияющих подсистем топологических инфраструктур сложных систем можно представить посредством разработки и внедрения дополнительного модуля системы компьютерного моделирования данных мониторинга уровня реализации локальных проектов по созданию (модернизации) элементов, подсистем и инфраструктур сложных систем в целом.

Предлагается функциональная структура комплекса программ, который реализует интегрированное использование данных в управлении инфраструктурными проектами, которая представлена на рис. 8.

Предложенное решение может быть реализовано в среде информационной системы «Генеральная схема развития сетей связи и инфраструктуры хранения и обработки данных Российской Федерации» Минцифры России [3], которая реализует указанные процедуры с возможностью предоставления данных пользователям электронных цифровых генеральных схем и ответственным за кластеры элементов.

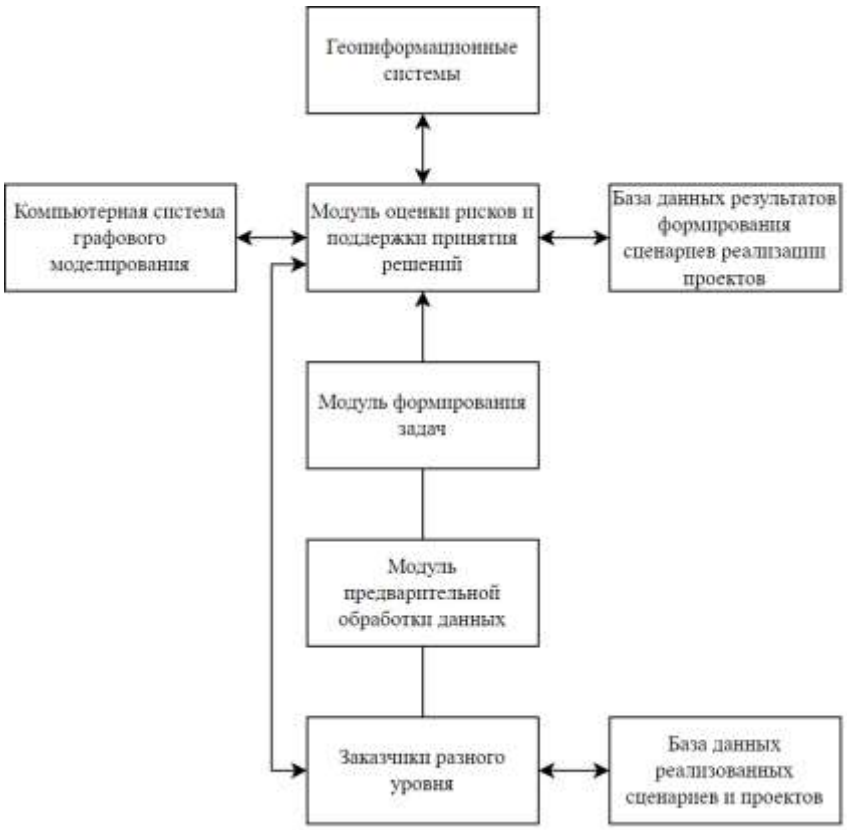


Рис. 8. Комплекс программных средств моделирования инфраструктурного проекта

Таким образом, в качестве путей снижения затрат с обеспечением приемлемого качества на системы поддержки принятия решений Заказчика сложных инфраструктурных проектов предлагается комплексирование системотехнических решений, реализующих различные функциональные задачи, на основе оперативного использования типовых свободно распространяемых программных средств общего применения и их бесшовного взаимодействия.

Список используемых источников

1. Шибаева В. С., Спасская Н. А. Риски инфраструктурных проектов в условиях развития цифровой экономики // Инновационная экономика и современный менеджмент, 2019. № 2. С. 10–13.

2. Шестаков А. В., Фролова К. А., Плетнев Я. А. Геоинформационные системы в управлении и мониторинге техногенных объектов. Схемы и QR-ссылки: учебное пособие. СПб. : Любавич, 2021. 100 с. ISBN 978-5-907440-62-3.

3. Девяткин Е. Е., Иванкович М. В., Володина Е. Е. Стратегическое управление сетями связи Российской Федерации как главная задача развития информационной инфраструктуры // Электросвязь, 2020. № 9. С. 24–29.

УДК 004.4’277.4
ГРНТИ 28.17.31

СТИЛИ ЭЛЕКТРОННОЙ ТАНЦЕВАЛЬНОЙ МУЗЫКИ КОНЦА XX ВЕКА: СТРУКТУРНО-ТЕХНОЛОГИЧЕСКИЙ АНАЛИЗ

Д. Д. Кузьмина, Г. Г. Рогозинский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Первые электронные инструменты появились в начале XX века, но электронная музыка как самостоятельный жанр возникла во второй половине XX века – начале XXI века и сегодня охватывает десятки направлений от экспериментальной академической музыки до популярной электронной танцевальной музыки. В данном исследовании авторы рассматривают стили и подстили, в которых используется чистый электронный звук. Общее свойство рассматриваемых стилей – это инструмент Roland TB-303, который оказал значительное влияние на электронную культуру 90-х годов. Исходя из проведённого исследования, авторы представляют общую модель формирования стилей электронной танцевальной музыки.

моделирование, сети петри, roland tb303, электронная музыка.

Электронная танцевальная музыка, какой её знают сейчас, пришла из первых поколений рейвов.

Чикаго во второй половине 1980-х был местом возникновения хаус-музыки. После долгих лет поиска и экспериментов появилось новое звучание: эйсид-хаус (англ. *acid house*). Звук эйсид-хауса создавался на синтезаторе басовой линии *Roland TB*-303. Машина могла создавать необычные звуки при непоследовательном (не по инструкции) использовании кнопок и переключателей. Компания *Roland* произвела всего 20 000 единиц, и к 1985 году *TB*-303 можно было найти в магазинах с бывшими в употреблении товарами по выгодным ценам, чем и воспользовалось большинство диджеев. Таким образом, благодаря синтезатору басовой линии, и появилось это необычное звучание в музыкальных композициях стиля эйсид-хаус [1].

1980-е гг. стали отправной точкой и расцветом множества стилей, где ключевую роль сыграл *Roland TB*-303 (рис. 1).

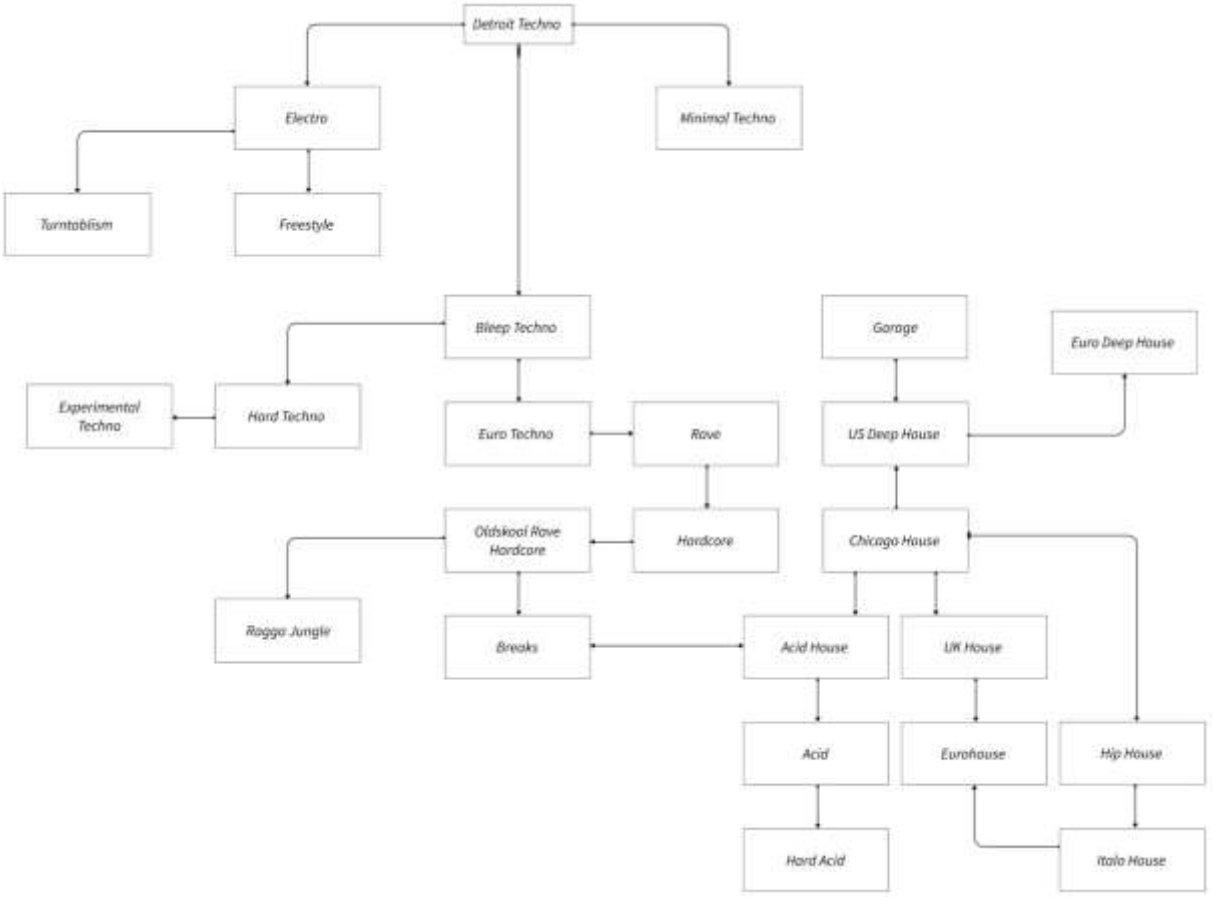


Рис. 1. Граф формирования стилей электронной танцевальной музыки

Специфическое звучание детройтского техно (англ. *detroit techno*) можно объяснить тем, что люди, стоявшие у истоков этой музыки, не могли позволить себе большого количества специального оборудования. Монофонический синтезатор, пара драм-машин и четырехканальный пульт часто были полным комплектом детройтского техно-музыканта [2]. Отсюда в композициях звучат, как правило, только четыре слоя. И чтобы один техно-трек был не совсем похож на другой, работе с этими звуками придавалось особое значение.

Звучание электро (англ. *electro*) характерно использованием аналогового синтеза звука для написания музыкальных композиций, и обильного вкрапления эффектов эхо, задержки, реверберации, обработанного вокодером вокала и лирики на научно-фантастическую и футуристическую тематику. Характерной особенностью электро является применение драм-машин для создания ритмической основы композиций – наиболее узнаваемое звучание электро придает драм машина *Roland TR*-808 [3].

Эсид-хаус (англ. *acid house*) – стиль электронной музыки, относящийся к категории хаус-музыки. *Roland* и в этом стиле сыграл решающую роль. В то время как правильное использование *TB*-303 заключалось в том, чтобы

записать мелодию баса, установить контроллеры на желаемые уровни и затем нажать кнопку воспроизведения секвенции, никто в Чикаго в середине 80-х на самом деле этого не делал. Вместо этого они постоянно вращали контроллеры в процессе игры. Звук, который получился, и стал узнаваемым для эйсид-хауса [1].

Гараж (англ. *garage*) официально не получал своего стереотипного «гаражного» звучания до 90-х годов. До этого момента технически это был диско-звук. В какой-то момент в самом начале 90-х в нем появился характерный ритм малого барабана, который с тех пор стал стандартным ритмическим паттерном почти для всей музыки *Garage*.

Все вышеупомянутые стили электронной танцевальной музыки связывает использование минимума выразительных средств, чёткая структурность и присутствие *Roland TB*-303.

Поскольку одной из задач работы является создание алгоритмов автоматической генерации электронной танцевальной музыки, то начнём с формализации композиционного процесса [4].

Мы понимаем музыкальную композицию *C* как декартово произведение множеств *D, B, S* и *T*:

$$C: D \times B \times S \times T \rightarrow Y, \quad (1)$$

где D; d_i, $i = 1 \ldots N$ – множество паттернов драм-машины,

B; b_j, $j = 1 \ldots K$ – множество паттернов басового синтезатора,

S; s_l, $l = 1 \ldots M$ – множество паттернов секвенсора,

T; $T \subset \mathbb{Z}$, $\#T < t_{\max}$ – множество временных точек.

Для каждого множества паттернов мы определяем условия переходов, которые мы называем композиционный план:

$D \times Q^D \rightarrow D$ – композиционный план переключения паттернов D,

$B \times Q^B \rightarrow B$ – композиционный план переключения паттернов B,

$S \times Q^S \rightarrow S$ – композиционный план переключения паттернов S.

Все условия переходов составляют вместе композиционную модель:

$$Q = \{Q^D, Q^B, Q^S\}. \quad (2)$$

На примере реализации вышеизложенной математической модели для множества D присутствует ось дискретного времени T с обозначенными моментами старта паттернов от 1 до t_{max} и граф выбора паттерна d_i для каждого момента времени. Цифры над стрелками соответствуют вероятности выбора маршрута переключения паттерна (рис. 2).

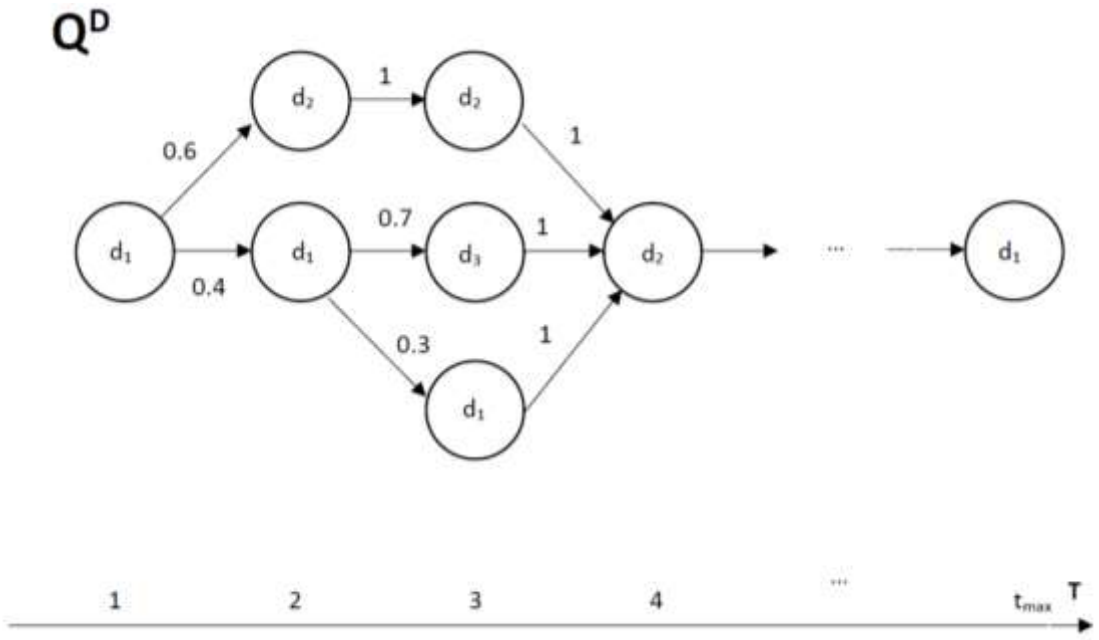


Рис. 2. Концептуальная композиционная модель Q^D

Для создания концептуальной композиционной модели использованы цепи Маркова [5].

Недостаточная разработанность темы чревата тем, что музыка, которая создаётся алгоритмами всё ещё является феноменом, несмотря на существующие современные технологии и методологию производства подобных музыкальных композиций. Данное исследование призвано решить проблему отсутствия практических моделей, которые могли бы дать возможность продюсерам продолжать развивать направление генеративной музыки.

Благодаря анализу эволюции стилей электронной танцевальной музыки 90-х годов XX века, выявлены общие характерные особенности, которые позволили предложить формальное описание музыкальной композиции, выделено понятие композиционной модели, создана концептуальная композиционная модель для одного из паттернов; а также выявлена необходимость выполнить сбор статистики для уточнения параметров композиционной модели.

Список используемых источников

1. History of the Rave Scene: How DJs Built Modern Dance Music. URL: https://djtechtools.com/2013/12/19/history-of-the-rave-scene-how-djs-built-modern-dance-music/ (дата обращения: 24.01.2022)

2. Manning Peter. Electronic and computer music. New York: Oxford University Press, 1985

3. Simon Reynolds. Energy Flash: A Journey Through Rave Music and Dance Culture. New York : Soft Skull Press, 2012

4. Эдельман С. Л. Математическая логика. М.: Высшая школа, 1975. 176 с.

5. Definition of Markov chain in US English by Oxford Dictionaries. URL: https://www.lexico.com/en/definition/markov_chain (дата обращения: 20.01.2022)

УДК 654.024
ГРНТИ 49.39.29

К ВОПРОСУ ОБЕСПЕЧЕНИЯ СВОЕВРЕМЕННОГО И ПОЛНОГО ОБМЕНА ИНФОРМАЦИОННЫМИ РЕСУРСАМИ В ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В. И. Курносов, А. А. Павлович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается место и роль единого информационного пространства в системе государственного управления, требования к обмену информационными ресурсами и обоснования выбора технологии распределенного реестра для обеспечения своевременного и полного информационного обмена.

информационное пространство, система государственного управления, технологии распределенного реестра, системы управления базами данных.

Работы последних лет по повышению качества информационной поддержки процессов управления сосредотачивались главным образом на создании технических средств, автоматизированных и телекоммуникационных систем, предназначенных для обработки и передачи информации [1, 2]. При этом ставилась задача обеспечения возможности оперативного и целенаправленного использования информации на основе внедрения современных информационных технологий. Однако по-прежнему остается актуальным вопрос обеспечения полноты и своевременности предоставления информации, необходимой для решения задач государственного управления.

Анализ служебной деятельности должностных лиц органов государственного управления (ОГУ) показывает, что информационный обмен осуществляется с использованием практически всех видов связи, а уровень применения того или иного вида связи зависит как от самого органа управления, так и от уровня иерархии его в системе государственного управления. При этом, информация в виде сообщений, образующих информационные потоки

(потоки сообщений), циркулирующая в системе управления может поступать от органов управления в объекты управления и в обратном направлении. Если под интенсивностью потока сообщений, циркулирующего от органа управления к объекту управления и наоборот (между взаимодействующими органами, объектами управления), понимать количество сообщений *Q*, входящих и исходящих в системы управления в единицу времени *T*, то модель информационного потока в системе управлении можно представить как суммарную интенсивность потока сообщений всех видов информации, циркулирующих на информационных направлениях системы управления, состоящую из входящих и исходящих потоков информации: управления $\lambda_{\text{у}}^{\Sigma}$; о состоянии органов (объектов) управления $\lambda_{\text{с}}^{\Sigma}$; о внешних возмущающих факторах (ВВФ) $\lambda_{\text{п}}^{\Sigma}$; из решения должностного лица (ДЛ) $\lambda_{\text{к}}^{\Sigma}$

$$\lambda_{\text{у}}^{\Sigma};=\lambda_{\text{у}}^{\Sigma}+\lambda_{\text{с}}^{\Sigma}+\lambda_{\text{п}}^{\Sigma}+\lambda_{\text{к}}^{\Sigma}+\lambda_{\text{увбд}}^{\Sigma}+\lambda_{\text{дв}}^{\Sigma}, \quad (1)$$

где $\lambda_{\text{у}}^{\Sigma}=\lambda_{\text{у}}^{\text{вх}}+\lambda_{\text{у}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений управления; $\lambda_{\text{с}}^{\Sigma}=\lambda_{\text{с}}^{\text{вх}}+\lambda_{\text{с}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений о состоянии органа, объекта управления; $\lambda_{\text{п}}^{\Sigma}=\lambda_{\text{п}}^{\text{вх}}+\lambda_{\text{п}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений о ВВФ; $\lambda_{\text{к}}^{\Sigma}=\lambda_{\text{к}}^{\text{вх}}+\lambda_{\text{к}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений из решения ДЛ; $\lambda_{\text{увбд}}^{\Sigma}=\lambda_{\text{увбд}}^{\text{вх}}+\lambda_{\text{увбд}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений по видам всестороннего обеспечения; $\lambda_{\text{дв}}^{\Sigma}=\lambda_{\text{дв}}^{\text{вх}}+\lambda_{\text{дв}}^{\text{исх}}$ – сумма интенсивностей входящего и исходящего потоков сообщений других видов информации; по видам всестороннего обеспечения $\lambda_{\text{увбд}}^{\Sigma}$; другие виды информации $\lambda_{\text{дв}}^{\Sigma}$.

Для обеспечения информационной связности и организации взаимодействия между всеми участниками действий необходимо иметь единое информационное пространство (ЕИП), в котором должны создаваться и циркулировать информационные потоки, обеспечивающие решение всех задач управления, обслуживания, а также осуществляться информационное взаимодействие ОГУ.

При этом важно, чтобы доступ к информационным ресурсам осуществлялся в любой точке этого пространства. Основным компонентом ЕИП, должна являться информационная инфраструктура, которая определяет его размеры и форму, обеспечивает создание и циркуляцию информационных потоков, а также функционирование и развитие ЕИП, организует сбор, обработку, поиск, хранение, анализ, распределение и распространение всей

циркулирующей в информационном пространстве информации. В основном информационные ресурсы (ИР) формируются в результате деятельности органов управления, функционирования автоматизированных систем, а также поступают из внешних источников. При этом ИР распределены по органам управления, где под ними понимаются документы, которым присваивается различный приоритет.

Основными требованиями к ЕИП являются полнота, эффективность, упорядоченность. Требование полноты предполагает достаточность хранящейся в ЕИП информации для решения различных задач. Требование эффективности предполагает достижение рационального соотношения между затратами на создание ЕИП и целевыми эффектами, получаемыми при его использовании. Требование упорядоченности предполагает четкое определение состава ЕИП и систематизацию всех информационных ресурсов, включаемых в него.

Проведенный анализ показал, что к обмену ИР в ЕИП предъявляются требования, изложенные в [1, 2], а характерной особенностью является необходимость сочетания богатого информационного наполнения с передовыми технологическими разработками. Это обусловлено тем, что наряду с новыми данными и документами большое значение могут иметь наличие особых методов обработки информации, доступа к хранилищу документов, структурных и семантических связей с остальными компонентами системы.

Существует ряд подходов по организации общего доступа к разделяемым информационным ресурсам, а каждая из выбираемых технологий обмена ИР в ЕИП обладает своими достоинствами и недостатками [3, 4]. При этом, традиционным подходом к хранению данных является – централизованная база данных (ЦБД). При данном походе все данные хранятся в одном месте, например, на «мэйнфрейме» или сервере. Пользователи в удаленных местах получают доступ к данным через глобальную сеть (WAN), используя прикладные программы, предоставляемые для доступа к данным. ЦБД должна быть способна удовлетворить все запросы, поступающие в систему, поэтому может легко стать узким местом. Но поскольку все данные хранятся в одном месте, их проще поддерживать и создавать резервные копии. Кроме того, легче поддерживать целостность данных, поскольку после того, как данные хранятся в централизованной базе данных, устаревшие данные больше не доступны в других местах.

Другим подходом является распределенная база данных (РБД) – это база данных, в которой данные хранятся на устройствах хранения, которые не расположены в одном и том же физическом месте, но база данных управляется с помощью центральной системы управления базами данных (СУБД).

В сравнении с ЦБД распределенные базы данных позволяют избежать узкого места, что обеспечивает балансировку нагрузки между несколькими серверами. Но поддержание актуальности данных в системе РБД требует

дополнительной работы, поэтому увеличивает стоимость обслуживания и сложность, а также требует дополнительного программного обеспечения (ПО) для этой цели. Кроме того, проектирование баз данных для РБД сложнее, чем для ЦБД.

В рассматриваемом аспекте основная решаемая задача – обеспечение доступа к ресурсам, а поскольку ресурсы распределенные, то функционирование обеспечивается специальной формой ПО – службами. В отличие от модели «клиент-сервер» тот или иной набор служб устанавливается здесь на каждом ресурсе. Множество служб должно удовлетворять структурным условиям - каждый тип служб должен иметь стандартный протокол доступа, в соответствии с которым реализуется прикладной интерфейс клиентов. В рамках стандартных протоколов допустимы различные способы реализации служб - множества служб на разных ресурсах должны быть согласованными. Это предполагает известную унификацию наборов служб на основе тождественности их семантики, а также наличие общих правил, регламентов и организационных соглашений, на которые опирается конфигурирование служб.

Следует отметить, что распределенный реестр (РР) – это база данных, которая распределена между несколькими сетевыми узлами или вычислительными устройствами. Каждый узел получает данные из других узлов и хранит полную копию реестра. Обновления узлов происходят независимо друг от друга. Ключевая особенность РР – отсутствие единого центра управления. Каждый узел составляет и записывает обновления реестра независимо от других узлов. Затем узлы голосуют за обновления, чтобы удостовериться, что большинство узлов согласно с окончательным вариантом. Голосование и достижение согласия в отношении одной из копий реестра определяют консенсус, этот процесс выполняется автоматически с помощью алгоритма. Как только консенсус достигнут, РР обновляется, и последняя согласованная версия реестра сохраняется в каждом узле.

Проведенный анализ показал, что из представленных подходов наиболее перспективным является технология распределенного реестра (block chain), которая позволяет реализовать данный подход на существующем вычислительном оборудовании, а также не требует дополнительных финансовых ассигнований.

В рассматриваемом аспекте «блокчейн» – это один из видов РР. Но не все распределенные реестры используют последовательность блоков для достижения достоверного консенсуса в распределенной системе защищенным от злоупотреблений способом. Блокчейн распределен в одноранговой сети и управляется с помощью этой сети. Так как это частный случай РР, он может существовать без центральной власти или управляющего сервера, а качество данных в блокчейне обеспечивается репликацией базы данных

и доверием, основанном на вычислениях. Однако структура блокчейна отличается от структуры других видов РР. Данные в блокчейне сгруппированы и организованы в блоки. Блоки соединены друг с другом и защищены криптографическими методами. В сущности, блокчейн – это постоянно растущий реестр записей. В блокчейн можно только добавлять данные. Нельзя удалять или изменять данные, сохраненные в предыдущих блоках.

Проведенный анализ работ в рассматриваемой предметной области [3, 4] показал, что существующие научные работы, направленные на совершенствование системы обмена ИР, не рассматривают вопросы обеспечения своевременного и полного обмена ИР в ЕИП на основе технологии РР. Данные особенности обусловливают необходимость поиска решений, позволяющих обеспечить своевременный и полный обмен ИР за счет технологии РР.

Для формализации данной задачи целесообразно введение следующих обозначений: $N = \{n_i\}$, $i = 1,..,n$ - множество органов управления (ОУ), объединяемых ЕИП; $U_y = \{u_y\}$, $y = 1,..,y$ – множество ДЛ i-го ОУ; $R_l = \{r_l\}$, $l = 1,...,l$ – объем ИР на i-м ОУ; $Q_i = \{q_l\}$, $l = 1,...,l$ – объем памяти ЭВМ на i-м ОУ; $P_{\text{пор}}$, $k = 1,...,K$ – вероятность поражения k-ым огневым средством; $\Lambda = \|\lambda_{i,j}\|$ $i,j = 1,..,n$ – матрица интенсивности обмена ИР между i,j ОУ; $X = \{x_{block}, x_t\}$ – параметры РР: x_{block} – длина блока РР; x_t – период обновления цепочки блоков РР; $P_{\text{св}}$ – вероятность своевременности обмена ИР в ЕИП; $P_{\text{п}}$ – вероятность полноты обмена ИР в ЕИП.

С учетом введенных обозначений задача декомпозируется на частные фрагменты, которые можно сформулировать следующим образом:

первое - разработать модель обмена ИР Met в ЕИП на основе применения технологии РР $X = \{x_{block}, x_t\}$:

$$M_{\text{ОИРЕИП}} = \langle N, U, R, Q, X, P_{\text{пор}}, \Lambda, P_{\text{св}}, P_{\text{п}} \rangle, \tag{2}$$

второе – разработать методику, обеспечивающую при заданном критерии своевременности обмена ИР $P_{\text{св}}(X) \geq P_{\text{св}}^{\text{треб}}$ повышение критерия полноты обмена ИР $P_{\text{п}}(X) \Rightarrow \max$, построенной на основе модель обмена ИР Met:

$$Met = \langle M_{\text{ОИРЕИП}}, A, Z \rangle \rightarrow P_{\text{п}} \mid P_{\text{св}}(X) \geq P_{\text{св}}^{\text{треб}}, \tag{3}$$

Учитывая обширность предметной области, а также разнообразие и развитие способов воздействий разработка должна быть проведена в следующих рамках исследования: рассматриваемое ЕИП – имеет статичные

структуру и количество пользователей; ЕИП объединяет все ресурсы всех ОУ; пользователями ЕИП являются все ДЛ ОУ.

Таким образом, на сегодняшний день поиск рационального соотношения пользования информационными ресурсами органами управления и пропускной способности сети, является наиболее важной и сложной задачей, требующей соответствующего решения. Данное решение должно учитывать предъявляемые жесткие требования к системе связи, а также сокращение длительности цикла управления и повышение качества подготовки принимаемых решений.

Существует множество технологий, позволяющих решить данное противоречие. Каждая из них характеризуется масштабом, сферами применения, инструментарием, целями, входными данными и получаемыми в результате информационными продуктами. Однако проведенный анализ показывает, что наиболее перспективным является технология распределенного реестра (block chain), которая позволяет реализовать данный подход на существующем вычислительном оборудовании и не требует дополнительных финансовых ассигнований. Кроме того, данная технология позволяет существенно снизить нагрузку на инфокоммуникационную систему ОГУ, а также предоставить всем должностным лица требуемую информацию.

Список используемых источников

1. Васильев Р. Б., Калянов Г. Н. Стратегическое управление информационными системами / под ред. Г. А. Левочкина, О. В. Лукинова. Москва: Интернет-университет информационных технологий, 2015. 510 с.

2. ГОСТ Р 43.0.32-2022 Информационное обеспечение техники и операторской деятельности. Управление деятельностью в технике.

3. Ивасенко А. Г., Гридасов А. Ю., Павленко В. А. Информационные технологии в экономике и управлении. М.: КноРус, 2017. 154 с.

4. Коротков Э. М. Исследование систем управления. М.: Юрайт, 2015. 228 с.

УДК 004.658
ГРНТИ 50.41.21

АНАЛИЗ ВОЗМОЖНОСТЕЙ СУБД POSTGRESQL ПО УПРАВЛЕНИЮ ДОСТУПОМ

А. Н. Лапко

Академия Федеральной службы охраны Российской Федерации

Статья посвящена анализу возможностей, предоставляемых СУБД PostgreSQL, по управлению доступом. Представлены SQL-команды управления ролями, наделения и отзыва у ролей привилегий, управления защитой на уровне строк. Выделены консольные утилиты, используемые для управления ролями. Приведены параметры ролей, используемые в SQL-командах и консольных утилитах. Описан интерфейс графического средства администрирования pgAdmin в части управления ролями и привилегиями.

управление доступом, СУБД PostgreSQL, роли, параметры роли, привилегии, наделение и отзыв привилегий, политика защиты на уровне строк.

В связи с переходом федеральных органов государственной власти на использование программного обеспечения с открытым исходным кодом система управления базами данных (СУБД) PostgreSQL становится наиболее востребованной для построения информационного хранилища автоматизированных систем. Одним из основных требований, предъявляемых к базовому функционалу СУБД, является возможность управления доступом к объектам базы данных (БД). К основным механизмам управления доступом СУБД PostgreSQL относят управление ролями, наделение и отзыв у ролей привилегий доступа к объектам БД, защиту таблиц на уровне строк [1].

СУБД PostgreSQL предоставляет возможность управления ролями с помощью SQL-команд, консольных утилит и графического средства администрирования pgAdmin. Основные SQL-команды, поддерживаемые СУБД PostgreSQL для управления ролями, представлены в таблице 1.

ТАБЛИЦА 1. SQL-команды управления ролями

Формат SQL-команды	Описание
`CREATE ROLE роль [ параметр ];`	создает новую роль
`ALTER ROLE роль [ параметр ];`	изменяет параметры роли
`GRANT роль TO роль [ WITH ADMIN OPTION ];`	наделяет роль другими ролями
`REVOKE [ ADMIN OPTION FOR ] роль FROM роль [ CASCADE ];`	отзывает у роли другие роли
`DROP ROLE роль;`	удаляет роль

Формат SQL-команды	Описание
`REASSIGN OWNED BY роль TO роль;`	передает все объекты БД, принадлежащие одной роли, другой роли
`DROP OWNED BY роль [ CASCADE ]`	удаляет все объекты БД, принадлежащие роли, и все права доступа
`SET ROLE роль;`	устанавливает роль в текущем сеансе

Дополнительные возможности управления ролями в СУБД PostgreSQL предоставляют консольные утилиты CREATEUSER и DROPUSER (табл. 2).

ТАБЛИЦА 2. Консольные утилиты управления ролями

Формат консольной команды	Описание
`createuser [ параметр_подключения ] [ параметр_роли ] название_роли`	создает новую роль
`dropuser [ параметр_подключения ] название_роли`	удаляет роль

При создании или изменении роли указываются ее параметры (табл. 3).

ТАБЛИЦА 3. Параметры роли

Параметр		Описание
SQL-команд	утилит	
SUPERUSER	-s (--superuser)	определяют наличие у создаваемой роли статуса суперпользователя
NOSUPERUSER	-S (--no-superuser)	
CREATEDB	-d (--createdb)	определяют наличие у создаваемой роли права управления БД
NOCREATEDB	-D (--no-createdb)	
CREATEROLE	-r (--createrole)	определяет наличие у создаваемой роли права управления ролями
NOCREATEROLE	-R (--no-createrole)	
INHERIT	-i (–inherit)	определяют способ использовать прав наделенных ролей (автоматически или с помощью команды SET ROLE)
NOINHERIT	-I (--no-inherit)	
LOGIN	-l (--login)	определяют право подключения к БД
NOLOGIN	-L (--no-login)	
REPLICATION	--replication	определяют право запуска процесса репликации
NOREPLICATION	--no-replication	
BYPASSRLS		определяют право пропускать политики защиты строк
NOBYPASSRLS		
CONNECTION LIMIT	-c (--connection-limit)	определяет максимальное количество параллельных подключений
PASSWORD	-P (--pwpromp)	определяет пароль создаваемой роли
VALID UNTIL		определяет срок действия пароля
IN ROLE	-g (--role)	определяет существующие роли, которыми наделяется создаваемая роль
ROLE		определяет существующие роли, которые наделяются создаваемой ролью

Параметр		Описание
SQL-команд	утилит	
ADMIN		определяет существующие роли, которые наделяются создаваемой ролью с правом ее передачи другим ролям

Альтернативную возможность управления ролями в СУБД PostgreSQL предоставляет средство администрирования pgAdmin [2]. Для создания новой роли в браузере объектов следует выделить узел «Роли входа» или «Групповые роли» и из контекстного меню этого узла выбрать пункт «Новая роль» или «Новая групповая роль». В открывшемся окне «Новая роль» (рис. 1) следует ввести название роли и другие ее параметры. Для изменения роли следует выбрать пункт «Свойства» из ее контекстного меню в браузере объектов и в открывшемся окне свойств роли внести требуемые изменения.

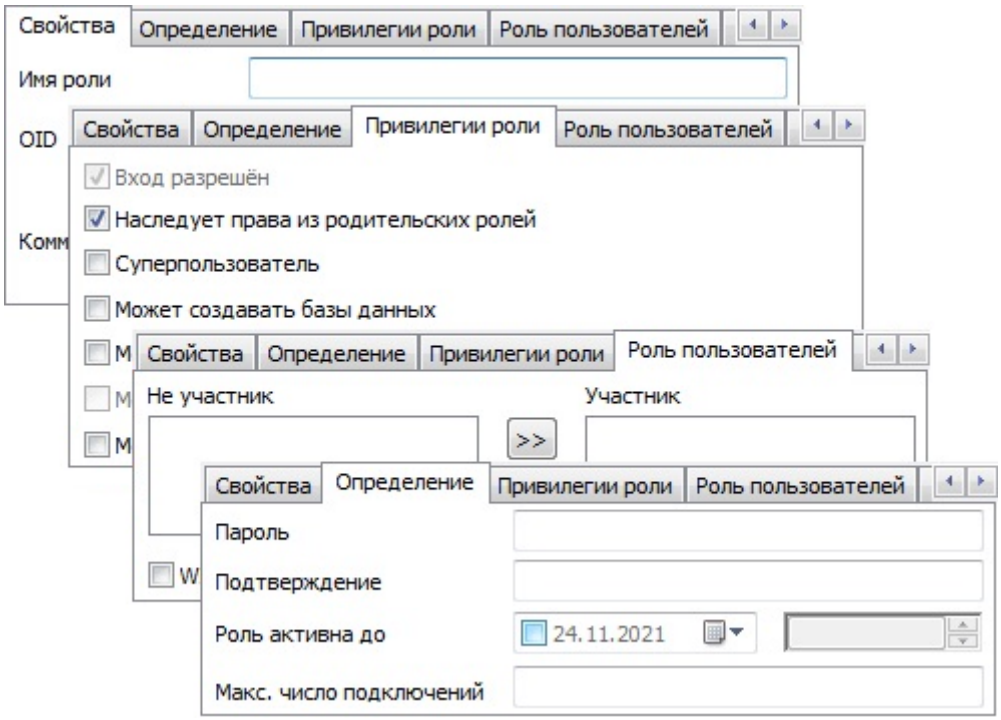


Рис. 1. Страницы окна «Новая роль»

Для удаления роли с помощью средства администрирования pgAdmin следует выбрать пункт «Удалить» из ее контекстного меню в браузере объектов. Перед удалением роли у нее должны быть отозваны все права доступа и удалены (переданы другим ролям) все принадлежащие ей объекты БД.

Наделение и отзыв у роли привилегий доступа к объектам БД в СУБД PostgreSQL можно реализовать с использованием SQL-команд GRANT и REVOKE (табл. 4).

ТАБЛИЦА 4. SQL-команды управления привилегиями доступа

Формат SQL-команды	Описание
`GRANT привилегия ON [ тип_объекта ] имя_объекта_БД TO роль [ WITH GRANT OPTION ]`	предоставить права доступа к объектам БД
`REVOKE [ GRANT OPTION FOR ] привилегия ON [ тип_объекта ] имя_объекта FROM роль [ CASCADE | RESTRICT ]`	отзывает права доступа к объектам БД

Предложение WITH GRANT OPTION SQL-команды GRANT дает право получателю привилегий передавать эти привилегии другим ролям.

Соответствие привилегий, используемых в SQL-команде GRANT, объектам БД представлено в таблице 5.

ТАБЛИЦА 5. Привилегии объектов БД

Объект БД		Привилегии
таблица	TABLE	SELECT, INSERT, UPDATE, DELETE, TRUNCATE, REFERENCES, TRIGGER
столбец таблицы	TABLE	SELECT, INSERT, UPDATE, REFERENCES
последовательность	SEQUENCE	USAGE, SELECT, UPDATE
функция	FUNCTION	EXECUTE
тип данных	TYPE	USAGE
схема	SCHEMA	CREATE, USAGE
табличное пространство	TABLESPACE	CREATE
БД	DATABASE	CREATE, CONNECT, TEMPORARY, TEMP

При назначении привилегий столбцам таблицы список привилегий в предложении GRANT должен иметь вид:

```
GRANT привилегия ( имя_столбца [, ...] ) [, ...]
```

Предложение GRANT OPTION FOR SQL-команды REVOKE позволяет отозвать у роли только право передачи привилегии другим ролям, оставляя саму привилегию у роли. CASCADE позволяет отозвать все зависимые привилегии, которые были получены от ролей, не являющихся владельцем объекта БД, но наделенных правом передачи отзываемых привилегий.

Средство pgAdmin предоставляет альтернативный способ назначения и отзыва у ролей привилегий доступа. Для наделения роли привилегией доступа к объекту БД следует выделить этот объект в браузере, из его контекстного меню выбрать пункт «Свойства», в открывшемся окне перейти на страницу «Привилегии» (рис. 2), выбрать требуемую роль, отметить соответствующие привилегии и нажать кнопку «Добавить/Изменить».

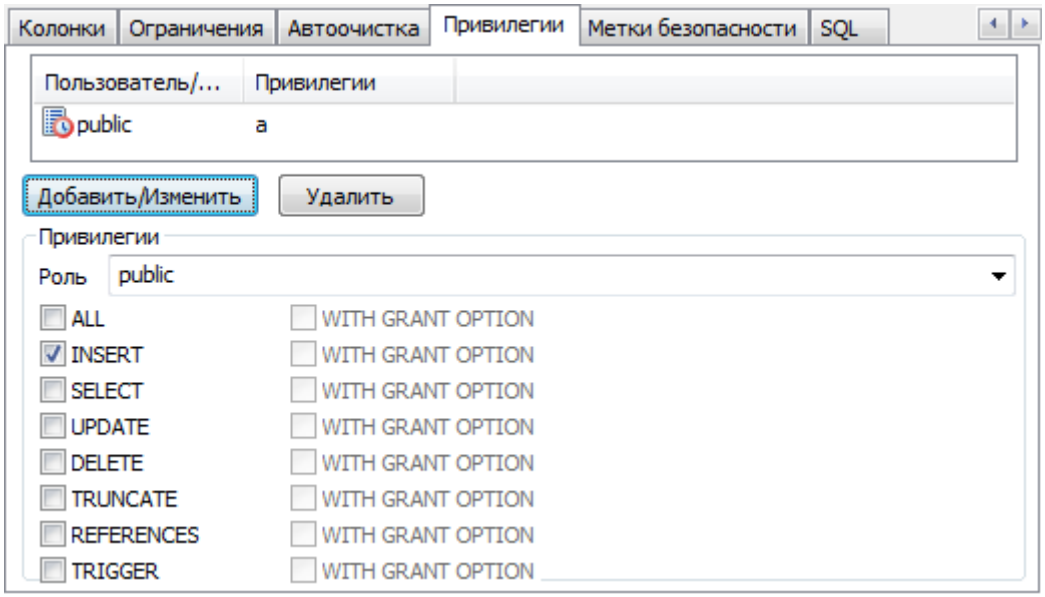


Рис. 2. Страница «Привилегии» окна свойств объекта

Для отзыва у роли привилегий доступа следует на странице «Привилегии», выбрать пакет привилегий, расположенный в верхней части страницы, а затем откорректировать его, сняв выделение с соответствующих привилегий и нажав кнопку «Добавить/Изменить», или удалить весть пакет привилегий, нажав кнопку «Удалить».

В дополнение к этому СУБД PostgreSQL предоставляет возможность защиты таблиц на уровне строк, которая ограничивает видимость и доступность строк при обращении к ним с помощью обычных запросов. Основные SQL-команды, поддерживаемые СУБД PostgreSQL для управления политикой защиты на уровне строк, представлены в таблице 6.

ТАБЛИЦА 6. SQL-команды управления политикой защиты

Формат SQL-команды	Описание

`CREATE POLICY политика ON таблица`
`[ AS { PERMISSIVE | RESTRICTIVE } ]`
`[ FOR ALL | SELECT | INSERT | UPDATE | DELETE ]`
`[ TO роль ] [ USING ( выражение ) ]`
`[ WITH CHECK ( выражение ) ]`
	создает политику защиты

`ALTER POLICY политика ON таблица [ TO роль ]`
`[ USING ( выражение ) ]`
`[ WITH CHECK ( выражение ) ]`
	изменяет политику защиты

`DROP POLICY политика ON таблица` `[ CASCADE | RESTRICT ]`	удаляет политику защиты
`ALTER TABLE таблица` `{ ENABLE | DISABLE }ROW LEVEL SECURITY;`	включает / отключает защиту

Ключевое слово PERMISSIVE создает разрешительную политику, а RESTRICTIVE – ограничительную. Видимыми и доступными остаются только те строки, для которых выражение USING возвращает TRUE. В запросах INSERT и UPDATE доступны только те строки, для которых выражение WITH CHECK возвращает TRUE. Если к запросу применяются несколько политик, то разрешительные политики объединяются дизъюнкцией, а ограничительные – конъюнкцией.

Проведенный анализ позволяет сделать вывод о том, что СУБД PostgreSQL позволяет управлять ролями, наделять и отзывать у ролей привилегии доступа к объектам БД, защищать таблицы на уровне строк. Основным средством реализации механизмов управления доступом являются SQL-команды, к дополнительным средствам можно отнести консольные утилиты и графический интерфейс средства администрирования pgAdmin.

Список используемых источников

1. Документация к PostgreSQL 13.5 // Постгрес Профессиональный, 2021. 2634 с. URL: https://postgrespro.ru/media/docs/enterprise/13/ru/postgres-A4.pdf (дата обращения: 17.01.2022).

2. Lapko, A. N. The analysis of the PostgreSQL DBMS capabilities for role management // Modern informatization problems in the technological and telecommunication systems analysis and synthesis. Yelm, WA, USA: Science Book Publishing House, 2022. PP. 252–256.

УДК 004.492.3:004.056.57
ГРНТИ 81.93.29

ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ В ДОКУМЕНТАХ MICROSOFT OFFICE, PDF-ФАЙЛАХ И АРХИВАХ

Н. А. Лебедев, Д. Р. Мамадалиев, Д. О. Маркин, А. В. Тезин

Академия Федеральной службы охраны Российской Федерации

В статье приводится описание особенностей вредоносных вложений в файлах различных форматов. Описаны меры противодействия вредоносным вложениям рассматриваемых типов, способы обнаружения. Разработаны рекомендации по безопасному использованию представленных форматов файлов.

вредоносные вложения, антивирусные средства, меры защиты от вирусов.

Развитие цифровой экономики требует совершенствования программного обеспечения (ПО), разработки информационных систем, выполняющим задачи в различных отраслях экономики, а также на уровне органов государственной власти. Вместе с тем совершенствуются и угрозы безопасности, включая вредоносное программное обеспечение (ВПО). Растущие потребности в обмене электронными документами делает их предметом особого внимания со стороны злоумышленников, использующих вредоносные вложения для реализации компьютерных атак.

У распространителей вредоносного ПО есть свои "любимые" форматы. В данной работе рассматриваются наиболее популярные файлы, скрывающих вредоносное ПО: документы *Microsoft Office*, *PDF*-файлы, *ZIP* и *RAR* архивы.

Документы Microsoft Office

На сегодняшний день сотрудники большинства организаций в повседневной деятельности используют офисные продукты компании *Microsoft*. Возможности *Microsoft Office* расширяются с использованием различных расширений, например, таких, как *Visual Basic, Object Linking and Embedding (OLE)* объекты, *ActiveX* и др. Как правило, именно использование расширений является точной проникновения троянских программы или иных классов ВПО в ЭВМ. Пример предупреждения, показ которого является основанием насторожиться показан на рис. 1.

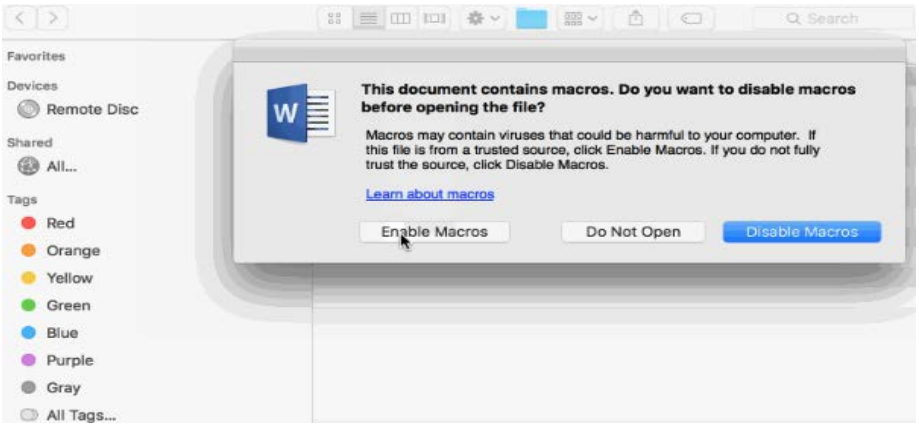


Рис. 1 Активация макросов документа *MS Word*

При положительном ответе, злоумышленник получает контроль над компьютером жертвы.

PDF-файлы

PDF-файлы – один из наиболее распространенных форматов обмена электронными документами. На рис. 2 показан результат попытки открытия

вредоносного *PDF*-файла [3]. Программа просмотра *PDF* запрашивает обновление. Жертва нажимает на подсказки и открывает файл "*updater*", после чего тот открывает веб-браузер по умолчанию и запрашивает запуск программы обновления.

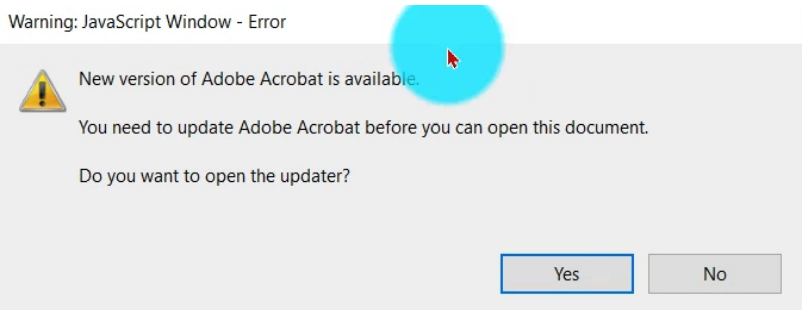


Рис. 2. Окно открытия исполняемого файла

После обновления предлагается запустить некий файл от неизвестного издателя. После нажатия кнопки «запустить» вредоносный файл запускается.

ZIP-архивы

На рис. 3 представлен пример [2] письма с вложенным *zip*-архивом как наиболее распространённого метода доставки вредоносных *zip*-архивов.

Жертва открывает вложенный файл. Внутри архива содержится исполняемый файл, после запуска которого происходит заражение компьютера.

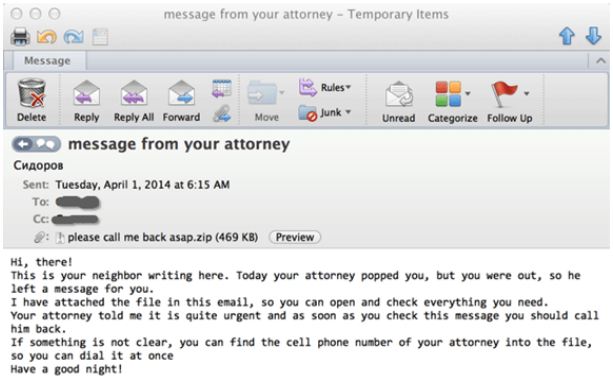


Рис. 3 Письмо с вредоносным zip-архивом

Популярные техники заражения ЭВМ вредоносными вложениями

Рассмотренные методы доставки вредоносных вложениях используют методы социоинженерных атак. С их помощью осуществляется первичный доступ к компьютерной системе.

В дальнейшем исполняемый вредоносный код выполняет действия по закреплению в системе. Например, за счет создания и запуска служб. Пример такой службы показан на рис. 4.

```
remnux@remnux:~$ httpd start
Starting web server: thttpd.
remnux@remnux:~$ fakedns
pyminifakeDNS:: dom.query. 60 IN A 172.16.80.128
```

Рис. 4 Запуск служб

Служба, показанная в примере, позволяет осуществить подмену сетевого адреса DNS-сервера и тем самым осуществить перехват и перенаправление запросов на доступ к сайтам с оригинальных на подставные и тем самым попытаться получить доступ к учетным данным пользователя, которые он использует на подставных сайтах.

Деструктивные действия такого типа достаточно хорошо определяются средствами *IDS* (*Intrusion Detection System* – система обнаружения вторжений), которая может осуществлять анализ потенциальной опасности *DNS*-запросов и другого сетевого трафика. Однако такие системы используются только в корпоративных сетях организации и требуют достаточно специфических навыков по настройке и внедрению.

Пример перехваченного сетевого пакета, формируемого вредоносным вложением показан на рис. 5.

Рис. 5. Содержимое пакета

В данном примере необходимо обратить внимание на параметр запроса *Agent*. При перехвате последовательности запросов данный параметр постоянно меняется так, как будто бы пользователь каждым новым запросом обращался к сайтам с разных веб-браузеров, а *IP*-адрес источника при этом остается неизменным.

Следы закрепления в системе, могут быть обнаружены и стандартными средствам операционной системы. Например, вредоносная программа может добавить параметры в реестре в разделе автоматически запускаемых программ при загрузке. Пример такой настройки показан на рисунке 6.

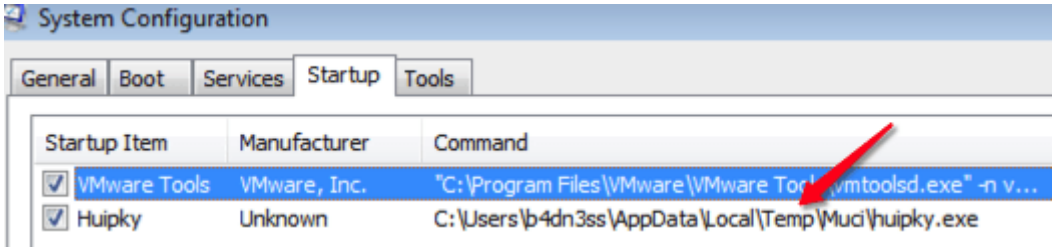


Рис. 6. Программы в автозапуске

Это же стандартное средство позволяет и удалить настройки, внесенные вредоносной программой.

Рекомендации по безопасной работе в сети Интернет

Важно понимать, как себя вести с потенциально опасными вложениями.

Отправлять в спам все письма с вложенными архивами или файлами в формате *DOCX* или *PDF* – слишком радикальный метод защиты, однако если отправитель неизвестен, то этот метод в большинстве случаев – единственно верный.

К основным рекомендация по работе в сети Интернет относятся [3].

Не открывайте подозрительные письма, пришедшие с незнакомых адресов. Если вы не понимаете, почему сообщение с такой темой оказалось в папке «Входящие» – скорее всего оно вам не нужно.

Если по долгу службы вам приходится работать с корреспонденцией от незнакомцев, тщательно проверяйте, с какого адреса пришло письмо, как называется вложение. Если что-то в оформлении сообщения вызывает у вас сомнения, просто закройте его.

Не разрешайте исполнение макросов для документов, пришедших по электронной почте, если ваша регулярная работа этого не требует.

Критически относитесь к ссылкам внутри файлов. Если вы не понимаете, зачем по ним переходить, просто игнорируйте. Если все же считаете, что по ссылке нужно перейти – лучше вручную ввести адрес соответствующего сайта.

Используйте защитные решения, которое уведомит вас об опасном файле и заблокирует его, а также предупредит при попытке перейти на подозрительный сайт.

Список используемых источников

1. Attachments in Phishing 102. URL: https://www.hoxhunt.com/blog/attachments-in-phishing-102 (дата обращения: 12.12.2021).

2. Phishing with a malicious .zip attachment. URL: https://cofense.com/malware-analysis-zip-attachment/ (дата обращения: 12.12.2021).

3. Топ-4 самых опасных типа вложенных файлов. URL: https://www.kaspersky.ru/blog/top4-dangerous-attachments-2019/22767/ (дата обращения: 12.12.2021).

УДК 004.05
ГРНТИ 81.93.29

ПОИСК ЦИФРОВЫХ СЛЕДОВ И АНАЛИЗ ИЗМЕНЧИВЫХ ДАННЫХ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

В. А. Липатников, А. А. Ломанов, А. Р. Низамов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В настоящее время существует необходимость автоматизации процесса поиска цифровых следов в ОС, основанной на ядре Linux, при этом сохраняя неизменность обрабатываемых данных. В статье описан разработанный программный комплекс для автоматизированного поиска цифровых следов в ОС, основанной на ядре Linux. Использование программного комплекса в значительной степени способствует ускорению процесса поиска цифровых следов ввиду того, что сбор изменчивых данных достаточно долгий и трудоемкий процесс. Программа отличается тем, что она имеет весь необходимый набор команд для извлечения изменчивых данных.

информационная безопасность, цифровые следы, изменчивые данные, операционная система.

Актуальность

Согласно распоряжению Правительства РФ № 1588 от 26 июля 2016 года – все федеральные органы исполнительной власти и государственные внебюджетные фонды должны перейти на использование отечественного офисного программного обеспечения с использованием программ, включённых в единый реестр российских программ для электронных вычислительных машин и баз данных [1]. В связи с этим повсеместно государственные структуры переходят на использование операционной системы, основанную на базе ядра Linux, следовательно, возникает потребность в изучении модификации, и дальнейшем усовершенствовании данной операционной системы.

Постановка задачи

Так как в ходе эксплуатации операционной системы на базе ядра Linux, могут возникать инциденты информационной безопасности, и как известно, одним из этапов реагирования на инцидент информационной безопасности является поиск цифровых следов, соответственно существует необходимость автоматизации процесса поиска цифровых следов в ОС Linux [2].

Объектом исследования является – операционная система, основанная на базе ядра Linux, а предметом исследования – способы извлечения обрабатываемых в операционной системе данных, а также анализ обрабатываемых данных. Цель исследования: разработать программный комплекс для автоматизированного поиска цифровых следов в операционной системе, основанной на ядре Linux. Задача – обоснование необходимости автоматизации процесса поиска цифровых следов и формирование перечня изменчивых данных необходимых для специалиста по поиску цифровых следов.

Решение

Существует достаточное количество изменчивых данных хранящихся на исследуемой системе под управлением ОС Linux [3]. В таблице описаны наиболее распространённые типы изменчивых данных и команды вывода данных, а также краткое описание этих данных с учетом ценности для специалиста по поиску цифровых следов.

ТАБЛИЦА. Типы, команды вывода и краткое описание изменчивых данных

Тип изменчивых данных	**Команда вывода данных**	**Описание данных**
Информация о дате и времени операционной системы.	«date»	Так как, исследуемая система могла быть не синхронизирована с сервером времени, часы могли сбиться, необходимо отметить различие во времени во время составления отчета.
Версия операционной системы	«uname -a»	Данная команда выводит следующую информацию: имя ядра, имя хоста, версия ядра, название операционной системы и т.д. Необходимо значить точную версию операционной системы, для проведения анализа памяти.
Сетевые интерфейсы	«ifconfig -a»	Данная команда показывает все сетевые интерфейсы в том числе и отключенные, IP-адреса назначенные данным интерфейсам, и маски сети, подозрительные локальные сетевые подключения, беспроводные интерфейсы и т.д.
Таблицы маршрутизации	«netstat -rn» «route»	С помощью данной команды можно узнать перенаправлялся ли

Тип изменчивых данных	Команда вывода данных	Описание данных
		трафик через интерфейс, контролируемый злоумышленником, были ли изменены какие-либо шлюзы и т. д.
Запущенные процессы	«ps -ef»	С помощью данной команды можно увидеть подозрительные процессы, запускаемые под пользователем root и т. д.
Смонтированные файловые системы	«df»	Используя данную команду можно увидеть смонтированы ли в системе какие-либо подозрительные тома или существуют ли необычные временные тома, которые исчезнут при перезагрузки системы.
Загруженные модули ядра	«lsmod»	С помощью данной команды можно выяснить, установлены ли неизвестные драйверы устройств.
Открытые порты	«netstat –anp»	С помощью данной команды можно узнать есть ли подозрительные открытые порты, так же в списке можно увидеть идентификатор процесса PID использующий тот или иной порт. Данная команда может быть использована для обнаружения программ использующие порты, которые они не должны использовать.
Список пользователей в прошлом и настоящем	«w» «who»	С помощью данной команды можно получить полную информацию обо всех пользователях, работающих в системе, а также время входа в систему для каждого пользователя.
Список неудачных входов в систему	«last»	С помощью данной команды можно увидеть список неудачных попыток входа в систему за выбранный промежуток времени.

Тип изменчивых данных	Команда вывода данных	Описание данных
История команд терминала	«history 50»	Данная команда выводит 50 последних введенных команд в терминале. Данные хранятся в хронологическом порядке.

Реализация программного обеспечения

С целью автоматизации поиска цифровых следов в операционной системе, основанной на ядре Linux, было принято решение разработать программное обеспечение (ПО).

Данное ПО было написано на языке Python 3. Интерфейс разработанного ПО представлен на рисунке.

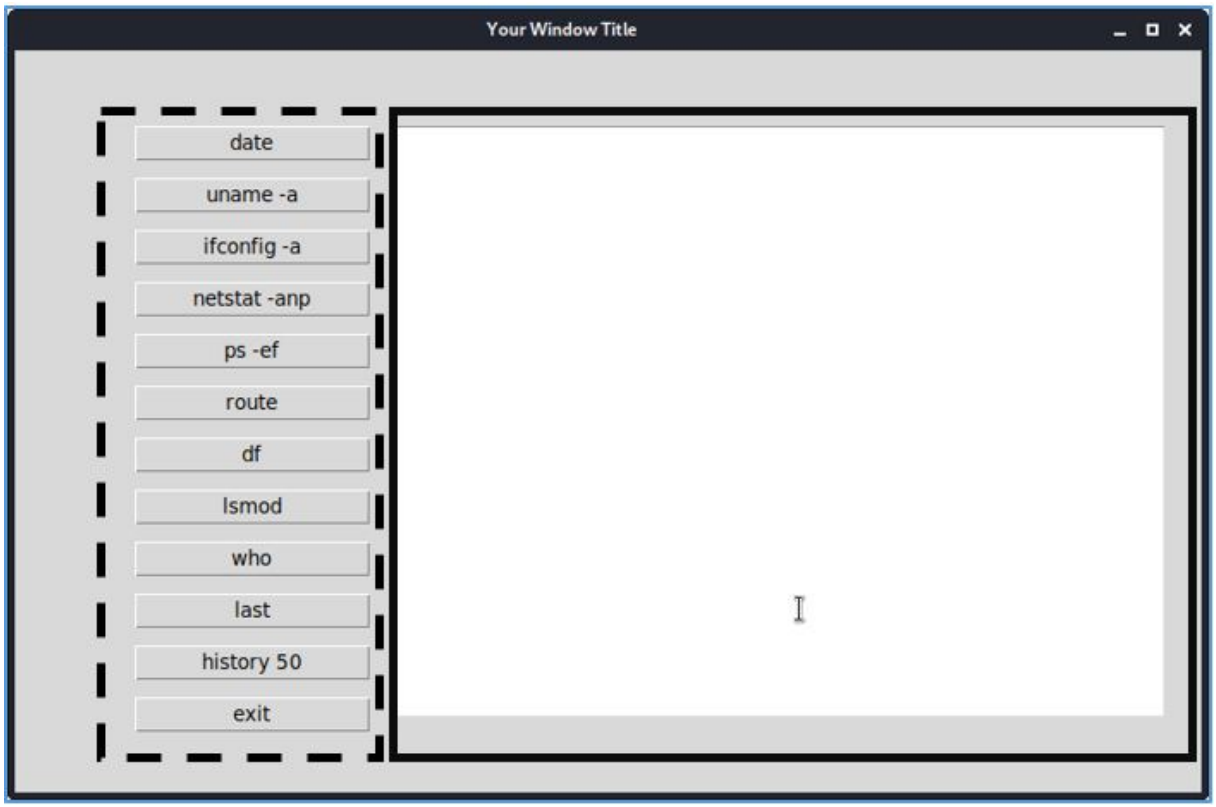


Рисунок. Интерфейс разработанного ПО для автоматизации поиска цифровых следов в операционной системе, основанной на ядре Linux.

Интерфейс программы разделен на блок с функциональными кнопками выделен пунктирной линией и блок вывода выполнения команд выделен сплошной линией. Результатом выполнения нажатий функциональных кнопок программы является вывод на экран выполнения команд терминала Linux. В программе заложена возможность масштабирования пользовательского интерфейса.

Выводы

Поиск цифровых следов в операционной системе Linux, является отнюдь не тривиальной задачей, так как необходимо учитывать множество фактов таких как: особенность проведения поиска цифровых следов в ОС Linux, сохранения целостности полученных доказательств, правила и особенность получения цифровых доказательств и т. д. Разработанная программа в значительной степени ускоряет процесс поиска цифровых следов в операционной системе Linux. Программа имеет интуитивно понятный интерфейс и набор всех команд необходимых для извлечения изменчивых данных с операционной системы Linux.

Список используемых источников

1. Об утверждении плана перехода органов исполнительной власти и государственных внебюджетных фондов на использование отечественного программного обеспечения: распоряжение Правительства России от 26.07.2016 года № 1588-р // КонсультантПлюс. ВерсияПроф. М., 2021.

2. Липатников В. А., Сокол Д. С. Модель нарушителя безопасной передачи информации в сетях VoIP-телефонии // В сборнике: Транспорт России: проблемы и перспективы – 2020. ФГБУН Институт проблем транспорта им. Н. С. Соломенко РАН. 2020. С. 187–192.

3. Костарев С. В., Карганов В. В., Липатников В. А., Технологии защиты информации в условиях кибернетического противоборства: науч. монография / Под общ. ред. В. А. Липатникова. СПб.: ВАС, 2020. 716 с. ISBN 978-5-91690-044-6

УДК 004.05
ГРНТИ 81.93.29

РАСПОЗНАВАНИЕ И АНАЛИЗ СЦЕНАРИЕВ ДИНАМИКИ МНОГОЭТАПНЫХ АТАК В СЕТЕВОМ ТРАФИКЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ МНОГОКРИТЕРИАЛЬНОГО КЛАССИФИКАТОРА

В. А. Липатников, А. А. Ломанов, А. Р. Низамов, А. А. Шевченко

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Предложен способ адаптивного управления защитой информационно-вычислительной сети на основе анализа динамики действий нарушителя за счет контроля си-

туационных параметров в противоборствующей обстановке на основе многокритериального классификатора при стохастической неопределенности. Метод содержит: мониторинг обстановки, распознавание последовательности действий нарушителя, процесс определения ситуационных параметров с достоверным прогнозом стратегии вторжений.

информационная безопасность, обнаружение вторжений, машинное обучение, классификатор.

Актуальность

Известно, что взломщики используют сложные методы реализации атак. Они проводят атаки, состоящие из нескольких этапов для достижения конечной цели [1, 2]. Наборы таких этапов известны также как многоэтапные атаки или сценарии атак. Многоступенчатый характер этих атак препятствует обнаружению вторжений, так как для понимания стратегии атаки и определения угрозы необходимо проанализировать множество отдельных действий [1]. Примером успешной многошаговой атаки можно назвать вирус WannaCry, который 12 мая 2017 года распространился по миру, заблокировав работу персональных компьютеров (ПК) не только отдельных пользователей, но и многих компаний. Подобные атаки подтолкнули исследователей и разработчиков к разработке систем защиты, направленных на отслеживание многошаговых атак.

Описание решения

Для реализации предложенного решения по моделированию работы программной реализации классификаторов сценариев динамики многоэтапных атак с различными параметрами проведена разработка алгоритма ее работы, представленного на рис. 1.

Рис. 1. Алгоритм моделирования работы программы

Алгоритм состоит из следующих действий:

1) на первом этапе происходит считывание входных данных, а именно данных ИТС СН. Далее происходит первичная обработка данных, выделение наиболее информативных полей с точки зрения классификации состояния сети;

2) на втором этапе происходит циклический анализ достоверности распознавания сценариев динамики многоэтапных атак с различными параметрами классификаторов. Для каждого классификатора рассматривается динамика изменения достоверности его работы при изменении определенного параметра. При этом остальные параметры также изменяются на каждой итерации внутреннего цикла. Таким образом осуществляется подбор параметров, при которых ошибка распознавания будет минимальна. Результатом процесса рассмотрения всего набора параметров является отчёт по ошибке распознавания для каждого сочетания параметров сценариев динамики многоэтапных атак.

Разработка программной реализации предложенного алгоритма

Разработка программной реализации разработанного алгоритма методов k-ближайших соседей, деревьев решений и Байесовского критерия для автоматической классификации объектов.

Для анализа динамики изменения достоверности распознавания сценариев динамики многоэтапных атак было решено перебирать значения определенного параметра из заданного массива во внутреннем цикле. По завершении перебора во внешнем цикле изменяются одновременно остальные параметры, не задействованные во внутреннем цикле, и выполняется новая итерация перебора указанного параметра. По завершении выполнения каждого внутреннего цикла строится график зависимости достоверности распознавания от изменения указанного параметра. Результатом работы всего внешнего цикла является семейство графиков зависимости достоверности распознавания классификатора от изменения его параметров.

Проведение анализа результатов моделирования работы программной реализации с различными параметрами

Проведение анализа результатов моделирования работы программной реализации с различными параметрами сценариев динамики многоэтапных атак.

В рамках моделирования проводилось исследование следующих параметров [3]. Для метода k-ближайших соседей:

– *n_neighbors,* количество соседей, используемых по умолчанию для запросов (от 2 до 10);

– *leaf_size*, размер листа. Это может повлиять на скорость построения и запроса, а также на объем памяти, необходимый для хранения дерева. Оптимальное значение зависит от характера проблемы. В рамках исследования рассматривались значения от 1 до 100;

– *p*, степенной параметр для метрики Минковского (от 1 до 75). Метрика – мера расстояния, неотрицательная, симметричная, если = 0, то объекты совпадают, часто требуется, чтобы выполнялось неравенство треугольника. Метрика Минковского определяется как

$$\rho_p(x, y) = (\sum_{i=1}^{d} |x_i - y_i|^p)^{1/p}$$

для p >= 1. При p ∈ (0, 1) данная функция метрикой не является, но все равно может использоваться как мера расстояния.

Для метода деревьев решений:

– *min_samples_split*, минимальное количество выборок, необходимое для разделения внутреннего узла (размерность от 0 до 1);

– *random_state*, управляет случайностью оценки (размерность от 0 до 10). Чтобы получить детерминированное поведение во время подгонки, этот параметр должен быть зафиксирован целым числом;

Для Байесовского критерия:

– *var_smoothing*, часть наибольшей дисперсии всех функций, которая добавляется к дисперсии для стабильности расчетов (размерность от 0,001 до 0,1).

В результате моделирования были получены зависимости вероятности ошибки распознавания от динамики изменений параметров классификаторов. Для метода k-ближайших соседей графики зависимостей приведены на рисунках 2–7.

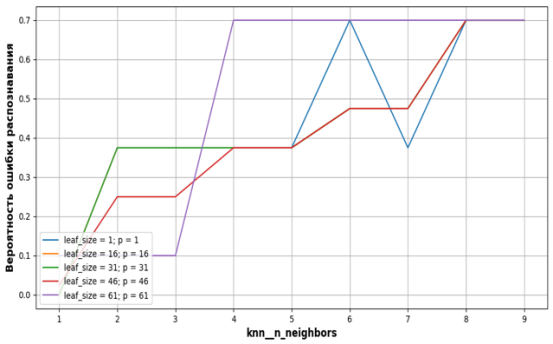


Рис. 2. Зависимость вероятности ошибки распознавания от количества соседей

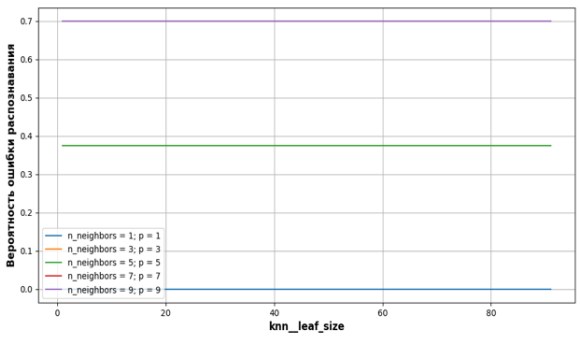


Рис. 3. Зависимость вероятности ошибки распознавания от размера листа

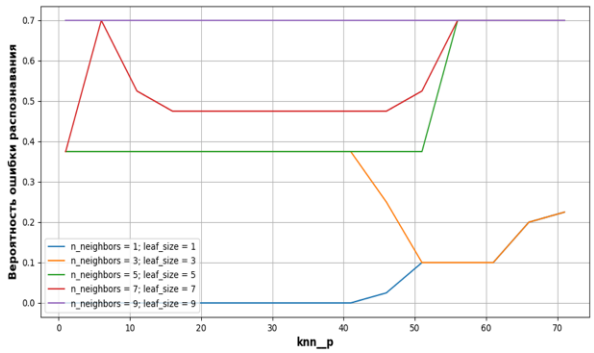


Рис. 4. Зависимость вероятности ошибки распознавания от степенного параметра

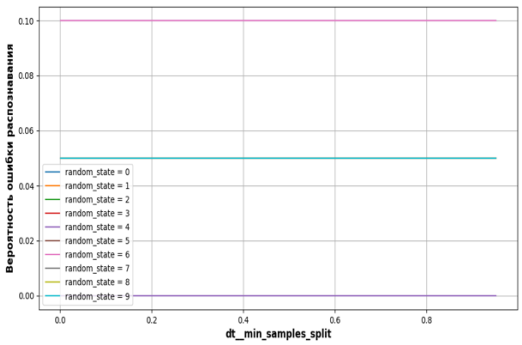


Рис. 5. Зависимость вероятности ошибки распознавания от минимального количества выборок

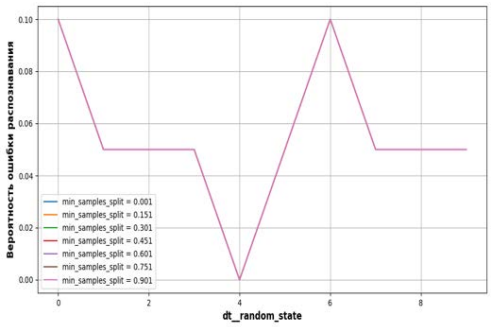


Рис. 6. Зависимость вероятности ошибки распознавания от случайности оценки

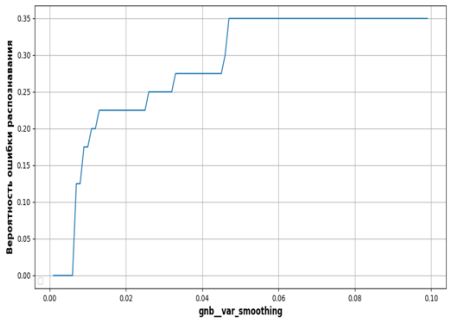


Рис. 7. Зависимость вероятности ошибки распознавания от наибольшей дисперсии всех функций

По результатам моделирования видно, что изменение размера листа и минимального количества выборок не влияют на динамику достоверности распознавания. С увеличением количества соседей ошибка распознавания заметно увеличивается. Также ошибка увеличивается с увеличением наибольшей дисперсии всех функций, разница заключается в плавности изменения. Ошибка распознавания при изменении степенного параметра сильно зависит от динамики изменения других параметров. Случайность оценки имеет ярко выраженное эффективное значение, равное 4, при котором ошибка распознавания нулевая.

Таким образом, с точки зрения влияния на динамику изменения достоверности распознавания сценариев динамики многоэтапных атак наиболее значимыми являются количество соседей и наибольшая дисперсии всех функций. Чем меньше их значение, тем выше достоверность распознавания.

Заключение

В результате работы был разработан алгоритм моделирования работы классификаторов сценариев динамики многоэтапных атак с разными параметрами с целью исследования зависимости достоверности распознавания от динамики их изменения. Была разработана программная реализация

предложенного алгоритма. Результатами проведенной работы являются исследованные зависимости достоверности распознавания от изменения параметров классификаторов и выводы о степени влияния каждого из них на общую динамику. Новизна предложенного подхода заключается в разработке алгоритма моделирования работы программной реализации с различными параметрами классификаторов и причинно-следственный анализ для обнаружения многоэтапных атак. Практическая значимость разработанного решения заключается в получении зависимостей достоверности распознавания от параметров каждого классификатора.

Список используемых источников

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, Springer-Verlag. 2005. V. 3685. pp. 311–324.

2. Кузнецов И. А., Липатников В. А., Шевченко А. А. Способ многофакторного управления безопасностью информационно-телекоммуникационной сети системы менеджмента качества предприятий интегрированных структур // Вопросы радиоэлектроники. 2016. № 6. С. 23–28.

3. Scikit-learn. URL: https://scikit-learn.org/

УДК 004.032.26
ГРНТИ 28.23.37

МЕТОДЫ АНАЛИЗА УСТОЙЧИВОСТИ НЕЙРОННЫХ СЕТЕЙ

В. Л. Литвинов, Е. А. Новиков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается вопрос устойчивости нейронных сетей. В частности, изучаются и сравниваются два различных подхода к постановке данного вопроса.

Первый из исследуемых подходов рассматривает процесс обновления весов в нейронной сети прямого распространения как обратную связь в системе управления, т.е. устойчивость системы эквивалентна сходимости процесса обучения. Второй подход рассматривает рекуррентную нейронную сеть как систему управления, т.е. устойчивость системы соответствует сходимости выходной функции к установившемуся значению.

Для исследуемых подходов приводится постановка вопроса, описывается актуальность, а также дается общее описание метода решения. Кроме того, описываются актуальные задачи, для которых решение рассматриваемого вопроса играет важную роль.

нейронные сети, многослойный персептрон, градиентные методы минимизации, градиентный спуск, динамическая система, идентификация динамических систем, устойчивость, рекуррентные нейронные сети.

Нейронные сети на текущий момент являются крайне мощным инструментом, применяемым для большого количества различных задач. Нейронные сети представляют собой [1] достаточно сложную модель с большим числом параметров, которая в ходе своей работы самоорганизуется и начинает выдавать некоторый требуемый результат. А когда идет речь о самоорганизации (иначе говоря, о сходимости некоторого параметра), то естественно возникает вопрос и об устойчивости рассматриваемой модели. Именно вопросу устойчивости, вариантам его постановки и методам анализа и посвящена данная работа.

Можно выделить два возможных варианта постановки вопроса устойчивости нейронных сетей. Первый вариант требует исследования устойчивости самого процесса обучения нейронных сетей, второй же – исследования устойчивости уже обученной модели нейронной сети. Рассмотрим теперь каждую из этих постановок более детально.

Первый вариант изначально описан в работе [2]. Авторами указанной работы показывается, что многослойный персептрон (многослойная нейронная сеть – МНС) в совокупности с процессом его обучения эквивалентен системе управления (СУ) с нелинейными обратными связями. При этом эти самые обратные связи отвечают за настройку весов данной сети, то есть осуществляют процесс обучения. Из этого напрямую вытекает постановка вопроса об устойчивости СУ, эквивалентной данной МНС, иначе говоря, об устойчивости МНС в смысле сходимости процесса её обучения.

Вопрос о сходимости обучения нейронных сетей на данный момент описан в значительном количестве авторитетных работ [3, 4]. Однако, предложенный в [2] подход позволяет рассмотреть данный вопрос совершенно с иной точки зрения, а также позволяет использовать крайне обширный инструментарий теории автоматического управления для анализа нейронных сетей. Основным методом анализа устойчивости нейронных сетей для данного подхода является метод Ляпунова.

Из описанного выше, можно сделать вывод, что данная постановка вопроса об устойчивости нейронных сетей является актуальной с теоретической точки зрения. Этот подход также имеет место для практического применения [5].

Рассмотрим теперь иной подход к постановке задачи устойчивости нейронных сетей. В частности, нас будут интересовать рекуррентные нейронные сети (РНС) [6].

Известно [7], что РНС используются для решения задачи идентификации динамических систем, иначе говоря, обученная РНС представляет собой приближенную модель динамической системы. Отсюда, естественно

возникает вопрос об устойчивости рассматриваемой модели, то есть, об устойчивости обученной нейронной сети.

Данная задача является значительно более актуальной. В частности, имеется значительное число недавних работ [8–10], которые исследуют данный вопрос с теоретической стороны. Кроме того, в работах [11, 12] рассматриваются практические вопросы применения РНС для моделирования динамических систем, что напрямую взаимосвязано с данным вопросом.

На текущий момент, нет общего метода анализа устойчивости РНС. Однако наилучший результат показывает анализ с помощью интегральных квадратичных ограничений (Integral Quadratic Constraints – IQC's [13]), основанный на классическом критерии устойчивости СУ [14]. На рисунке приведено сравнение результатов анализа с помощью IQC's и с помощью малых приращений (small gain).

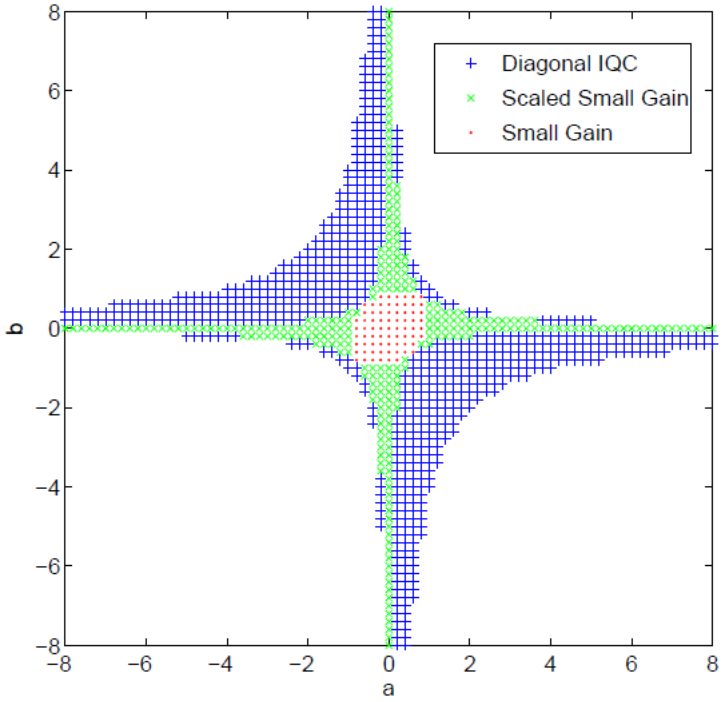


Рисунок. Сравнение методов анализа устойчивости РНС (взято из [8])

В качестве заключения, хотелось бы заметить, что оба рассмотренных подхода к определению понятия устойчивости и анализа нейронных сетей на этот предмет являются крайне актуальными и представляют значительный интерес с научной точки зрения.

Список используемых источников

1. Хайкин С. Нейронные сети: полный курс, 2-е издание. : пер. с англ. М. : Издательский дом «Вильямс», 2006. 1104 с.

2. Терехов В. А., Тюкин И. Ю. Исследование устойчивости процессов обучения многослойной нейронной сети. I // Автоматика и телемеханика. 1999. N 10. С. 136–143.

3. Поляк Б. Т. Введение в оптимизацию. М. : Наука, 1983. 384 с.

4. Вапник В. Н., Червоненкис А. Я. Теория распознавания образов (статистические проблемы обучения). М. : Наука, 1974. 416 с.

5. Глущенко А. И. Об эффективности настройки отдельных параметров пи-регулятора с помощью нейросетевого настройщика для компенсации возмущений при управлении нагревательными объектами // Управление большими системами. 2019. N 78. С. 71–105.

6. Elman J. Finding Structure in Time // Cognitive Science. 1990. N 14. C. 179–211.

7. Narendra K., Parthasarathy K. Identification and control of dynamical systems using neural networks // IEEE transactions on neural networks. 1990. N 1. С. 4–27.

8. Knight J. N. Stability analysis of recurrent neural networks with applications : дис. … д-ра техн. наук / James Nate Knight. Colorado, 2008. 116 с.

9. Иванов С. А. Устойчивость дискретных моделей стандартных конфигураций нейронных сетей с запаздывающими взаимодействиями : автореф. дис. … канд ф.-м. наук : 05.13.18 / Сергей Александрович Иванов. Челябинск, 2013. 16 с.

10. Клестов Р. А., Клюев А. В., Столбов В. Ю. Алгоритмическая устойчивость нейронных сетей глубокого обучения при распознавании микроструктуры материалов // Вестник Южно-Уральского государственного университета. 2021. N 21. С. 159–166.

11. Sun W., Braatz R. Smart process analytics for predictive modeling // Computers & Chemical Engineering. 2021. N 144. С. 107–134.

12. Bolt E. On Explaining the Surprising Success of Reservoir Computing Forecaster of Chaos? The Universal Machine Learning Dynamical System with Contrasts to VAR and DMD // Chaos: An Interdisciplinary Journal of Nonlinear Science. 2021. N 31.

13. Megretski A., Rantzer A. System Analysis via Integral Quadratic Constraints // IEEE Transactions on Automatic Control. 1997. N 42. С. 819–830.

14. Попов В. М. Об абсолютной устойчивости нелинейных систем автоматического регулирования // Автоматика и телемеханика. 1961. N 8. С. 961–979.

УДК 004.855.5
ГРНТИ 28.23.37

ПРИМЕНЕНИЕ МЕТРИКИ ВАССЕРШТЕЙНА И ШТРАФА ГРАДИЕНТА В ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОСЕТЯХ ДЛЯ СИНТЕЗА ВЫБОРКИ ЭЛЕКТРОФАЦИЙ

В. Л. Литвинов, Д. И. Руйго

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследование направлено на анализ влияния модификации модели синтезатора набора электрофаций на базе применения генеративно-состязательных нейросетей посред-ством внедрения расстояния Вассерштейна и штрафа градиента. Исследование показало, что модель синтезатора на базе WGAN-GP в значительной степени повышает качество исходной выборки электрофаций, что в свою очередь позволяет повысить точность модели контрольного классификатора.

литолого-фациальный анализ, спектральный анализ, геологоразведка, машинное обучение, классификация, генеративно-состязательные нейросети, WGAN-GP.

Собранные полевые данные электрокаротажа зачастую представляют собой информацию с грифом коммерческой тайны, что ограничивает возможность составления обучающих выборок, достаточных по размеру, для обучения моделей классификаторов с низким порогом значения функции потерь. Исследования по использованию нативной модели сети показало, что синтезированные сетью экзмемпляры седиментологических моделей для обучающей выборки не смогли повысить качества обучения классификатора [1].

Целью работы является исследование влияния добавления метрики Вассерштейна и штрафа градиента в моделях генеративно-состязательной нейросетей, разработанных для синтеза седиментологические модели фаций аналогичных моделям фаций, полученных эмпирическим путем.

Для достижения поставленной цели определены следующие задачи: определение наборов исходных данных для обучений моделей нейросетей; определение конфигурации WGAN; обучение моделей на исходных данных с последующей генерацией синтетических данных; проверка влияния внедрения метрики Вассшерштейна и штрафа градиента в модель сети GAN на качество обучения классифицирующей нейросети. Работа базируется на статье канадских и американских специалистов с представленной моделью сети WGAN-GP [2], исследовании Вивека Машкара по синтезу табличных медицинских данных [3] и исследовании Коди Неша по синтезу табличных данных для системы выявления банковских махинаций [4].

В работе предлагается исследовать качество синтеза набора данных в виде дискретных координат точек спектральных кривых седиметологических моделей. В качестве исходных данных используется 11 образцов модели фации средней части дельты [5].

Для оценки влияния добавления метрики Вассерштейна и штрафа градиента в модель генеративно-состязательной сети в исследовании проводится качественное сравнение полученной выборки синтезированной исходной моделью GAN [6] и модернизированной моделью WGAN-GP с идентичной конфигурацией слоев. Для синтеза экземпляров фаций в виде дискретных координат используется модель генератора с одним полносвязным скрытым слоем на 30 нейронов и модель дискриминатора с одним полносвязным скрытым слоем на 50 нейронов.

Первый запуск обучения сетей производился с параметром количества эпох равном 1 000. Как видно на графике (рис. 1) наилучшая сходимость функций ошибок модели GAN наблюдается на 705-й эпохе, модели WGAN-GP на 420-й эпохе. Копии моделей с указанных эпох были использованы для дальнейшего исследования.

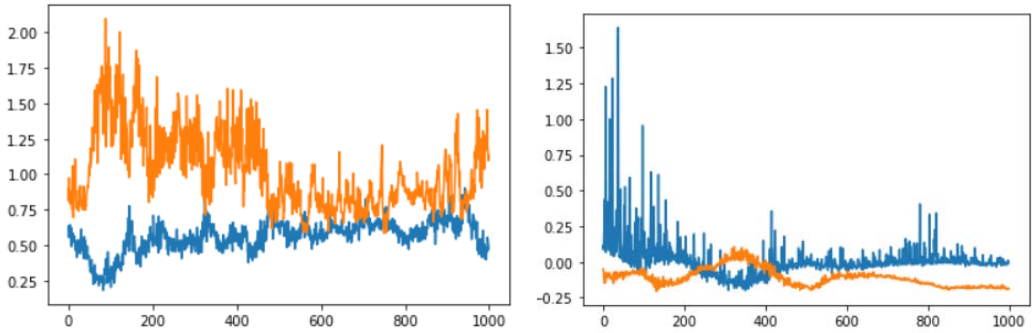


Рис. 1. Динамика функций ошибок моделей GAN и WGAN-GP

Продемонстрируем экземпляр синтезированного набора координат в виде восстановленной кривой фации. На рис. 2 синей линией продемонстрированы кривые синтезированных моделей.

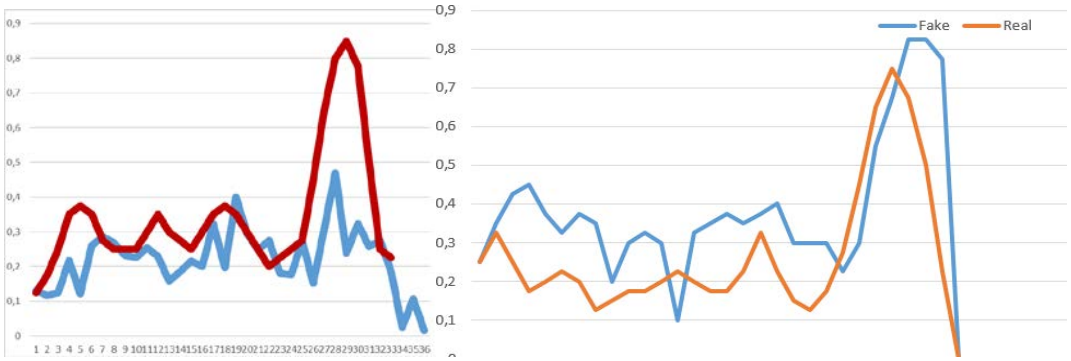


Рис. 2. Образцы синтезированных данных моделей GAN

Как видно, нейронная сеть смогла идентифицировать основные отличительные черты фации средней части дельты, однако в синтезированном набора данных перепады значения αПС между соседними точками более резкие, по сравнению с исходными данными.

Проверка степени влияния синтезированных данных на обучение классификаторов проводится через анализ результатов обучения классификатора. В качестве классификатора табличных данных используется модель нейросети TabNet [7]. На первом этапе модель обучается на исходных данных. На втором этапе набор данных удваиваются за счет добавление синтезированных данных. Обучение обеих моделей производится в течении 100 эпох. График динамики изменения функции ошибки классификации представлен на рис. 3.

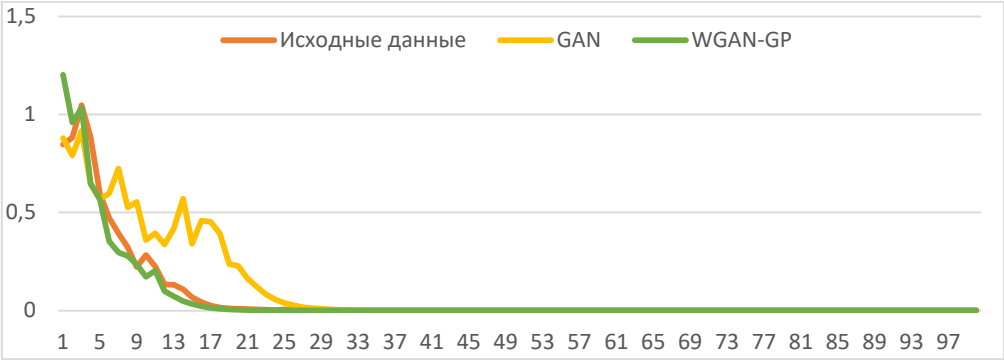


Рис. 3. Функции ошибок классификатора табличных данных

Результаты проделанной работы указывают на более высокое качество полученных синтезированных наборов данных посредством модели WGAN-GP по сравнению с моделью Vanila GAN. Исследование показало, что расширение выборки за счет синтезированных данных позволило снизить значение функции ошибки на 1,5% и увеличить скорость обучение на 2 эпохи.

Список используемых источников

1. Литвинов В. Л., Руйго Д. И. Разработка модели генерации обучающей выборки электрофаций на базе генеративно-состязательных нейросетей // Сборник лучших докладов конференции «Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021)». СПб., 2021. С. 378–382.

2. Ishaan Gulrajani. Improved Training of Wasserstein GANs // Montreal Institute for Learning Algorithms. URL: https://arxiv.org/pdf/1704.00028.pdf (дата обращения: 09.12.2021).

3. Vivek Maskara. Generating Tabular Synthetic Data Using GANs // Vivek Maskara. URL: https://www.maskaravivek.com/post/gan-synthetic-data-generation/ (дата обращения: 10.12.2021).

4. Cody Nash. Create Data from Random Noise with Generative Adversarial Networks // Developers. URL: https://www.toptal.com/machine-learning/generative-adversarial-networks (дата обращения: 10.12.2021).

5. Алексеев В. П. Литолого-фациальный анализ: Учебно-методическое пособие к практическим занятиям и самостоятельной работе по дисциплине "Литология". Екатеринбург: Изд-во УГГГА, 2003. 147 с.

6. Ian J. Goodfellow. Generative Adversarial Nets // Corell University. URL: https://arxiv.org/abs/1406.2661 (дата обращения: 13.12.2021).

7. Sercan O. Arık, Tomas Pfister. TabNet: Attentive Interpretable Tabular Learning. // Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 35 No. 8: AAAI-21 Technical Tracks 8, 2021. pp. 6679–6687.

УДК 004.8
ГРНТИ 28.17.31

ИССЛЕДОВАНИЕ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ МОДЕЛИРОВАНИЯ В ЗАДАЧАХ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ АЭРОПОРТОВ

В. Л. Литвинов, Д. А. Татуков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При проектировании и внедрении систем автоматизации для авиакомпаний и аэропортов большую роль играет имитационное моделирование. Оно позволяет с достаточной точностью определить расходы и прибыль системы и наглядно показать эффект от внедрения подобной системы в аэропорт. Имитационное моделирование позволяет построить модель на ранних этапах проектирования и оценить все риски системы. Рынок инструментальных средств моделирования бизнес-процессов достаточно велик и при проектировании систем необходимо правильно выбрать средство, которое будет наилучшим образом выполнять поставленные задачи. В работе проведен анализ и выбор инструментальных средств моделирования бизнес-процессов для проектирования системы автоматизации бизнес-процессов аэропорта.

информационная система, аэропорт, бизнес-процесс, моделирование, инструментальные средства.

По данным Министерства транспорта РФ уже к 2023 году расходы на развитие ИТ-инфраструктуры аэропортов увеличатся до 4,6 млрд $ (при темпах роста на уровне 3,8 %) [1]. Однако существуют ограничения, не позволяющие повсеместно внедрять ИТ- технологии. В таких проектах необходимо использовать дорогостоящие передовые технологии машинного зрения, искусственного интеллекта и другие. Проектирование, разработка и внедрение подобных систем стоят больших денег, только крупные авиакомпании и аэропорты могут позволить себе такие технологии.

В работе проведен анализ популярных инструментальных средств моделирования бизнес-процессов для проектирования системы автоматизации бизнес-процессов аэропорта: Witness, AnyLogic, Arena и FlexSim [2].

Witness – программный продукт для моделирования производственных систем. Он дает возможность гибкого моделирования рабочей среды, а также моделирования последствий различных хозяйственных решений [3].

Witness применяется для:

- анализа входных данных и результатов экспериментальных данных;
- для выявления правил и структуры данных;
- для повышения точности моделей.

Witness способен выявлять тенденции и сопоставлять данные на основе изучения данных модели, а также обеспечивает возможность определения фундаментальных связей, которые могут повысить уровень, принимаемых управленческих решений [3]. Рабочий интерфейс программы представлен на рис. 1.

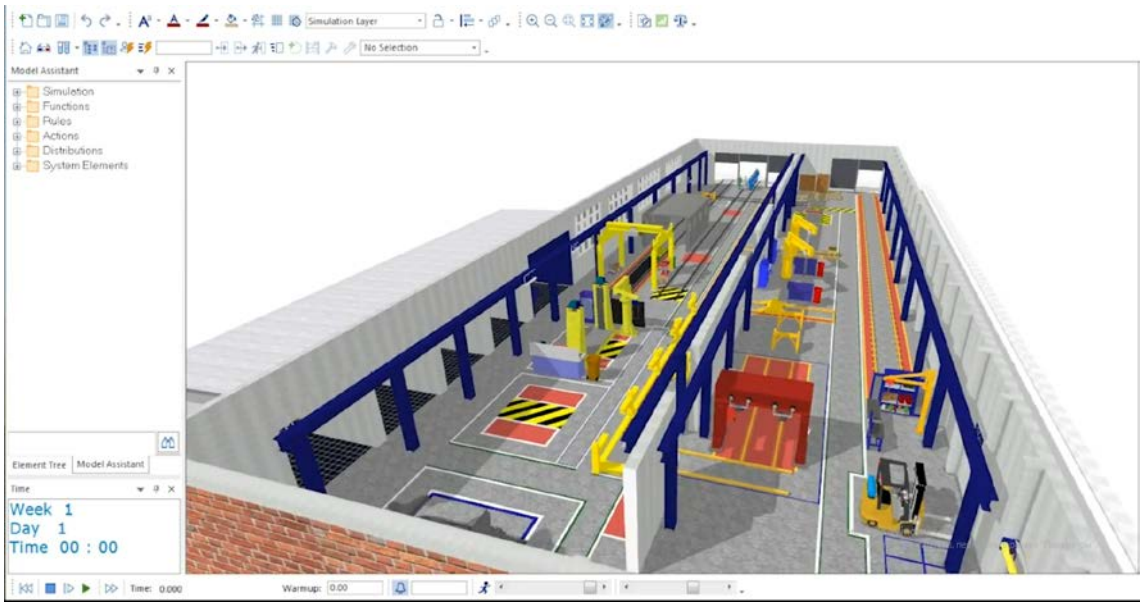


Рис. 1. Рабочий интерфейс Witness

AnyLogic — инструмент имитационного моделирования, позволяющий эффективно использовать и сочетать все существующие подходы к моделированию. Он имеет интуитивный графический интерфейс, который поддерживает графическое задание моделей и создание интерактивной 2D- и 3D-анимации для визуального отображения работы модели в реальном времени. AnyLogic применяется в управлении проектами, в различных социальных и экологических системах, в производственных процессах, здравоохранение и др. AnyLogic поддерживает моделирование систем как с дискретными, так и с непрерывными событиями, а также позволяет комбинировать их [4]. Рабочий интерфейс программы представлен на рис. 2.

Arena – это программное обеспечение для моделирования дискретных событий и автоматизации. Оно использует процессор и язык моделирования SIMAN. В Arena пользователь строит экспериментальную модель, размещая модули (коробки разной формы), представляющие процессы или логику. Соединительные линии используются для соединения этих модулей вместе и для определения потока сущностей. В то время как модули имеют определенные действия по отношению к сущностям, потоку и времени, точное представление каждого модуля и сущности по отношению к реальным объектам зависит от разработчика модели. Статистические данные, такие как

время цикла и уровни WIP (незавершенного производства), могут быть записаны и выведены в виде отчетов. Arena может быть интегрирована с технологиями Microsoft. Он включает VBA, поэтому модели могут быть дополнительно автоматизированы, если потребуются определенные алгоритмы. Он также поддерживает импорт блок-схем Microsoft Visio, а также чтение или отправку вывода в электронные таблицы Excel и базы данных Access [5]. Рабочий интерфейс программы представлен на рис. 3.

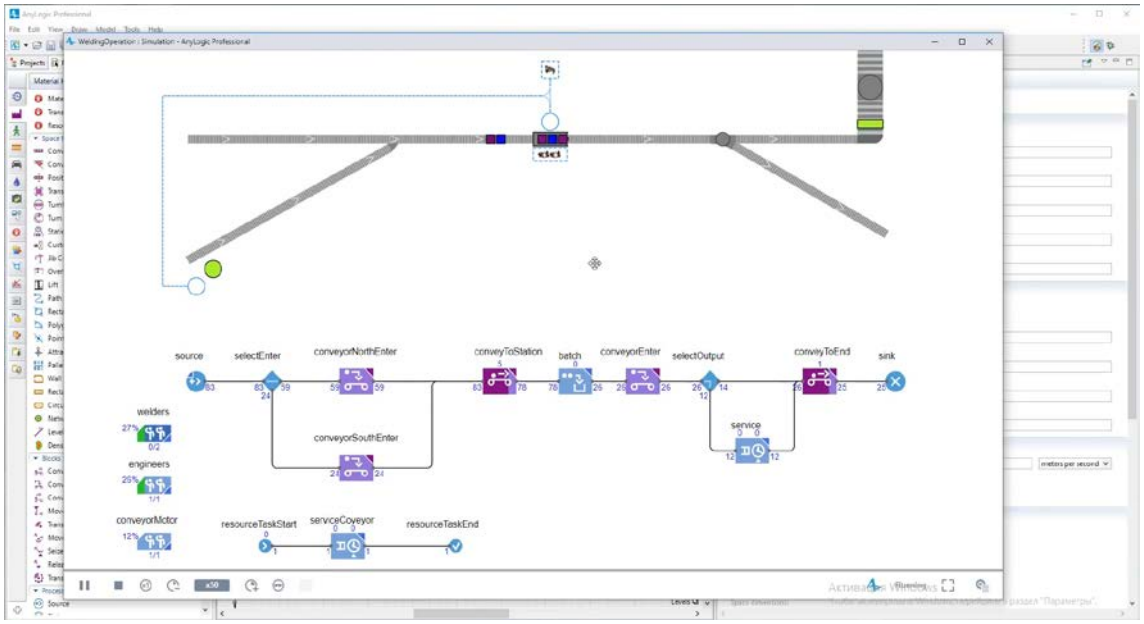


Рис. 2. Рабочий интерфейс AnyLogic

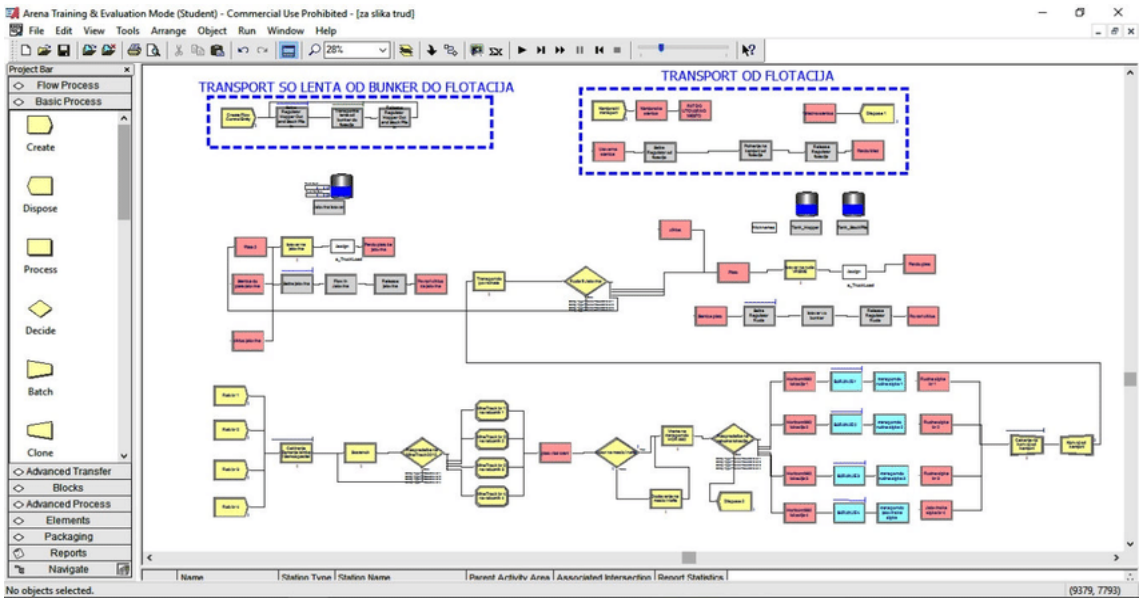


Рис. 3. Рабочий интерфейс Arena

Flexsim является программой для имитационного 3D-моделирования. Она моделирует, имитирует, предсказывает, и визуализирует системы в

производстве, обработки материалов, здравоохранения, складирования, горнодобывающей промышленности, логистики и других. Это одновременно мощная и удобная среда моделирования. Flexsim помогает оптимизировать текущие и запланированные процессы, выявить и уменьшить отходы, снизить расходы и увеличить доходы [6]. Рабочий интерфейс программы представлен на рис. 4.

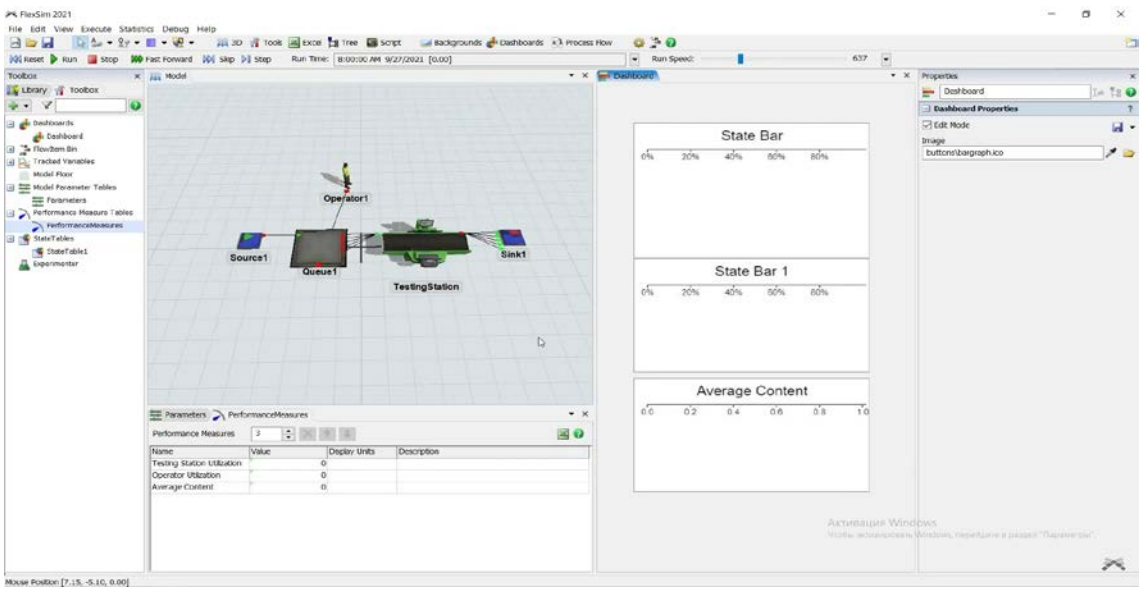


Рис. 4. Рабочий интерфейс Flexsim

Для сравнения инструментальных средств предложены ключевые параметры моделирования информационной системы автоматизации бизнес-процессов аэропорта. Результаты сравнения приведены в таблице 1.

ТАБЛИЦА 1. Результаты сравнения инструментальных средств моделирования

Инструмент	Поддерживаемые ОС	Сторонние приложения	Поддержка вывода анализа	Просмотр в реальном времени	3D - анимация	Бесплатные версии
AnyLogic	Windows, Mac,Linux	Exel,база данных, любая библиотека java	Отчеты, графики, вывод в строенную БД или любое хранилище данных	Да	Да	Free AnyLogic Personal Learning Edition
Arena	Windows	OptQuest	Arena Output Analyzer и Process Analyzer	Да	Да	Доступна бесплатная версия

Инструмент	Поддерживаемые ОС	Сторонние приложения	Поддержка вывода анализа	Просмотр в реальном времени	3D - анимация	Бесплатные версии
Witness	Windows	Н/Д	Н/Д	Да	Да	Доступна бесплатная версия
FlexSim	Windows	Exel, любая база данных, приложения на C++	Exel и полный набор графиков и диаграм	Да	Да	От бесплатной до 100$

Ключевыми параметрами являются: поддерживаемые операционные системы, поддержка сторонних приложений, поддержка вывода анализа, просмотр модели в режиме реального времени, поддержка 3D-анимации и наличие бесплатных версий [7]. На основе выведенных параметров было проведено сравнение инструментальных средств моделирования бизнес-процессов.

На основе сравнения был сделан вывод, что для моделирования информационной системы автоматизации бизнес-процессов аэропорта лучше всего подходит инструментальное средство AnyLogic. Оно работает на всех актуальных ОС и имеет полную поддержку сторонних приложений, вывода результатов анализа, просмотра в реальном времени и 3D-анимации. Кроме того, у него есть бесплатная версия.

Список используемых источников

1. Транспорт России. «Умный аэропорт»: будущее, которое стучится в дверь. URL: https://transportrussia.ru/razdely/vozdushnyj-transport/6850-umnyj-aeroport-budushchee-kotoroe-stuchitsya-v-dver.html (дата обращения: 12.02.2022).

2. Informs. Simulation Software Survey. URL: https://www.informs.org/ORMS-Today/OR-MS-Today-Software-Surveys/Simulation-Software-Survey (дата обращения: 10.02.2022).

3. Witness simulation moddeling software. URL: https://www.lanner.com/en-gb/technology/witness-simulation-software.html (дата обращения: 11.02.2022).

4. AnyLogic. URL: https://www.anylogic.ru/ (дата обращения: 11.02.2022).

5. Arena simulation software. URL: https://www.rockwellautomation.com/ru-ru.html (дата обращения: 11.02.2022).

6. FlexSim. URL: https://www.flexsim.com/ (дата обращения: 11.02.2022).

7. Simulation Software Comparison. URL: https://www.anylogic.com/resources/white-papers/simulation-software-comparison/ (дата обращения 12.02.2022).

УДК 519.876.5
ГРНТИ 49.33.29

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ УПРАВЛЕНИЯ НАДЕЖНОСТЬЮ СЛОЖНЫХ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ С ПРИМЕНЕНИЕМ ЦИФРОВЫХ ДВОЙНИКОВ

Е. А. Логвинова, А. В. Никитин, А. В. Пачин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современная техносфера все более насыщается различными устройствами, имеющими в составе средства для сбора и обработки данных, воздействия на другие объекты и окружающую среду. Кроме того, объединение этих устройств в сети позволило сформулировать концепцию интернета вещей, как разнесенной сложной системы, элементы которой способны обмениваться данными и функционировать без участия человека. Такие системы внедряются в самые сложные промышленные линии производства, системы управления безопасностью, в сферу освоения космоса, медицину и иные отрасли деятельности человека. Их применение играет все более существенную роль, а нарушение работоспособности такой системы в результате отказа техники, может привести к значительным потерям, как финансовым, так и репутационным. Следовательно, задача управления надежностью сложных систем интернета вещей имеет значительную актуальность.

Одним из современных подходов обеспечения требуемо надежности технических комплексов является проактивное управление, осуществляемое с использованием цифровых двойников.

В статье рассматриваются основы проактивного подхода к управлению надежностью сложной системы интернета вещей – киберфизической системы, с использованием цифровых двойников. Вводится показатель эффективности системы управления и обосновываются возможные направления решения поставленной задачи.

киберфизическая система, цифровой двойник, интернет вещей, аналитика.

Переход к Industry 4.0 определяет повсеместное использование устройств, способных обмениваться большими объемами данных, выполнять анализ информации и взаимодействовать, в том числе и без участия человека, в рамках Интернета вещей (Internet of Things – IoT).

Использование вещей IoT обеспечивает целый ряд преимуществ, вследствие чего подобные системы нашли применение и за пределами производственных линий, в таких областях человеческой деятельности как транспорт, медицина, «умные города», космическая деятельность и безопасность. Сложность систем постоянно возрастает, как и круг решаемых ими задач. При этом, к сожалению, возрастает и риск, связанный с их применением. Существенное увеличение устройств в системе ведет к повышению

числа отказов, а последствиями таких отказов могут стать существенные финансовые или репутационные потери, в некоторых случаях может быть нанесен ущерб человеку или окружающей среде. Таким образом, управления надежностью систем IoT различного назначения является весьма актуальной.

Наиболее перспективным направлением для решения этой задачи является использование киберфизических систем. **Киберфизическая система (КФС)** – сочетание информационно и логически взаимосвязанных объекта (технической системы как множества элементов, принадлежащих IoT), его цифрового двойника и средств проактивного управления. Основной задачей КФС является повышение эффективности функционирования объекта путем повышения результативности при заданных ограничениях на ресурсы, либо путем сокращения затрат при обеспечении требуемого результата. Для решения этой задачи необходимо структурно и логически увязать работу всех компонентов.

Системы в Интернете вещей

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и, в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен. IoT-устройства функционируют самостоятельно, хотя люди могут настраивать их или предоставлять доступ к данным [1].

Наиболее важными отличиями Интернета вещей от существующего интернета людей являются:

– фокус на вещах, а не на человеке;

– существенно большее число подключенных объектов;

– существенно меньшие размеры объектов и невысокие скорости передачи данных;

– фокус на считывании информации, а не на коммуникациях;

– необходимость создания новой инфраструктуры и альтернативных стандартов.

Главным преимуществом IoT является способность коммуникации устройства с устройством в автоматическом режиме. Необходимость человеку наблюдать и контактировать с устройством становится менее актуальной, так как интернет вещь способна сама получать, обрабатывать и передавать информацию. Это помогает продлить работоспособность устройства, исключением возможности повредить устройство персоналом, а также снизить трудозатраты работников, в следствии чего снижение расхода материальных и энергоресурсов.

Интеллектуальные системы IoT позволяют быстро создавать новые продукты, динамически реагировать на требования к продуктам и оптимизировать производственную цепочку и сеть цепей поставок в режиме реального времени с помощью сетевого оборудования, датчиков и систем управления [2].

Цифровой двойник

Цифровой двойник – программно реализованная модель управляемого (исследуемого) объекта, связанная с ним цифровыми каналами, обеспечивающими синхронизацию физического и цифрового состояний с требуемой периодичностью.

Цифровой двойник включает максимально полный набор измеряемых в реальном масштабе времени характеристик и параметров объекта в виде специальной структуры данных, а также средства обработки и визуализации [3].

Рис. 1. Цифровой двойник с визуализацией

Подсистема проактивного управления

В качестве инструментов для управления надежностью объектов в состав КФС включаются различные средства для поддержки принятия решений человеком, или же интеллектуальные управляющие системы.

Это различные модели (в том числе имитационные), позволяющие исследовать поведение объекта при изменении внешних и внутренних условий. А также системы искусственного интеллекта, позволяющие на основе баз знаний и моделей ситуаций формировать необходимые управляющие воздействия.

Цель **проактивного** управления с применением цифровых двойников – увеличение эффективности функционирования технической системы IoT путем повышения ее надежности.

В качестве целевого показателя при управлении надежностью может быть использован комплексный показатель надежности - коэффициент технического использования [2]

$$К_{ТИ} = \frac{T_о}{T_о + T_В + T_{ТО}}$$

Пути повышения $К_{ТИ}$:

1. Сокращение времени восстановления работоспособного состояния;
2. Сокращение суммарного времени проведения плановых работ по техническому обслуживанию.

1. Время восстановления $T_В$ зависит от:

– времени диагностирования неисправности (локализация отказавшего элемента, определение характера и причин отказа);

– времени доставки запасной части из ЗИП (со склада, с завода).

2. Суммарное время выполнения плановых работ по техническому обслуживанию $T_{ТО}$ может быть сокращено за счет применения стратегии тех. обслуживания по фактическому состоянию.

Комплексное сочетание первого и второго подходов позволит повысить надежность технической системы без увеличения расходов на ее функционирование, либо обеспечить требуемую надежность (эффективность) при рациональных затратах. Однако при этом необходимо учитывать расходы, связанные с созданием и функционированием инструментария КФС.

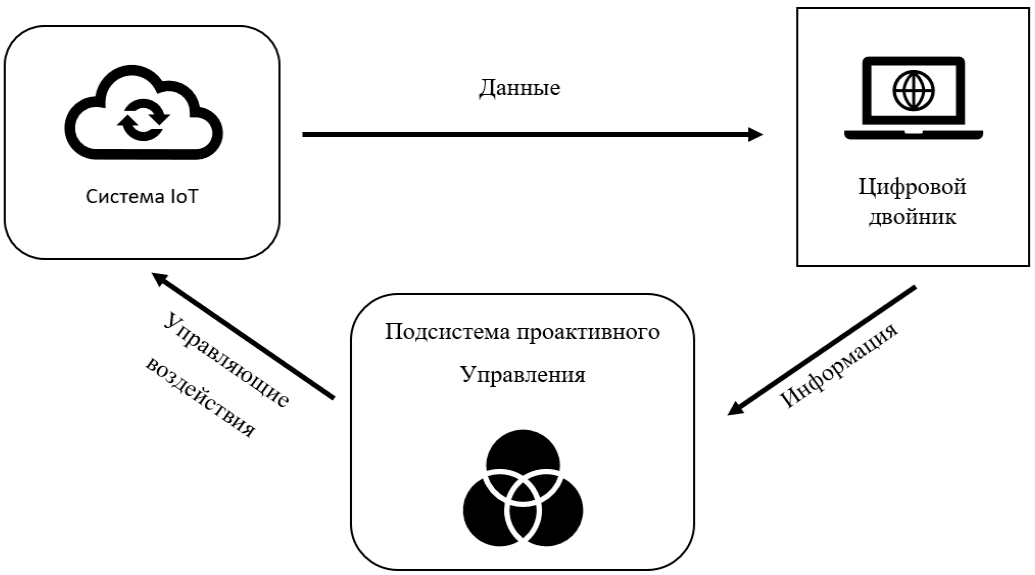


Рис. 2. Схема киберфизической системы

В данной схеме представлены три основных элемента, образующие киберфизическую систему:

Система IoT:

- Физический объект.
- Сенсоры и исполнительные устройства.

Цифровой двойник:

- Образ вещи (thing shape).
- Свойства (properties).
- События (events).
- Действия (services).

Подсистема проактивного управления в составе КФС решает следующие задачи:

- Анализ.
- Прогнозирование.
- Обоснование вариантов решений.
- Подготовка результирующих команд для формирования управляющих воздействий.

Заключение

Киберфизические системы, построенные на основе технологий IoT и цифровых двойников, являются перспективным инструментом для управления эффективностью сложных технических систем, в первую очередь различных объектов промышленного назначения. Они помогут значительно облегчить работу со сложным оборудованием и автоматизировать контроль его параметров для сокращения числа отказов и минимизации их негативных последствий. Применяемые в КФС методологии предиктивной аналитики и управления знаниями позволят обеспечить требуемую надежность технических систем, что приведет к повышению их результативности и сокращению затрат на их обслуживание и восстановление. Таким образом, задача построения и использования КФС в современной техносфере является весьма актуальной.

Список используемых источников

1. Росляков А. В., Ваняшин С. В., Гребешков А. Ю. Интернет Вещей: учебное пособие. Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015.

2. Цветков В. Я. Интернет вещей как глобальная инфраструктура для информационного общества // Современные технологии управления. 2017. № 6 (78).

3. ISO/IEC JTC 1/SC 41. Internet of Things and Digital Twin. Secretariat: KATS (Korea, Republic of).

4. ГОСТ Р 27.102-2021, п. 109. Надежность в технике. Надежность выполнения задания и управление непрерывностью деятельности, 2021.

УДК 519.6
ГРНТИ 28.19.27

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПРОИЗВЕДЕНИЙ ТВОРЧЕСТВА

Л. М. Макаров, С. В. Протасеня

Санкт-Петербургский государственный университете телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большое количество наблюдений за проявлением природных процессов создает представление о наличии определенных закономерностей, проявляющихся в совершенно непохожих по форме и содержанию явлениях и объектах, столь массово представленных в реальном пространстве событий, исследование которых проводится посредством физико-математических формализмов.

энтропия, информационная энтропия, количество информации.

Рассматривая процесс творчества достаточно широко и оперируя понятиями динамического потока событий, отождествляемого с физическими представлениями о эволюции материального мира выделим наиболее типичные направления:

– природное творчество, выраженное в терминах классической физики;

– природное творчество, выраженное в литературных произведениях;

– природное творчество, выраженное в уникальных наборах нуклеотидов живых организмов.

В общем перечне направлений реально наблюдаемых событий выделяется понятие сложной системы, демонстрирующей наличие непрерывного потока смены состояний. Оценка сложности потока смены состояний создается на классических постулатах термодинамики, в частности информационной энтропии.

В физике термин энтропия характеризует степень, или иначе говоря, уровень «хаоса» частиц, образующих систему или объект. Беспорядочность элементов системы оценивается показателем вероятности обнаружения истинного положения. Формализм этого понятия установлен в виде математического выражения:

$$H(X) = -\sum_x P(x) log_2\big(P(x)\big),$$

$H(X)$ – количество информации (биты); $P(x)$ – значение вероятности того факта, что выбранное значение принадлежит массиву X. Принимая это за

основу можно оценить совместную энтропию нескольких переменных по выражению:

$$H(X_1, X_2, \dots . X_n) = -\sum_{x_1} \dots \dots \sum_{x_n} P(x_1, \dots x_n) log_2 (P(x_1, .. x_n).$$

Следует признать, что все объекты Природы являются сложными объектами, для которых характерно:

– наличие большого количества разнообразных элементов;
– отчетливое проявление свойств недетерминированности;
– наличие обратных связей;
– наличие свойств эмерджентности;
– инициализация мульти параметрического эволюционного процесса.

Свет обладает электромагнитную природу. То, что свет является электромагнитной волной, позволило значительно расширить базовые представления о материальных объектах, в том числе таких которые очень удалены от наблюдателя. Скорость электромагнитных волн в вакууме, как и света, оказалась одинаковой и равной величине $3{,}1 \cdot 10^8$ м/с; – электромагнитные и оптические волны имеют поперечную структуру.

Оптические волны на высоких частотах имеют фундаментальные ограничения, обусловленные квантовой природой лучистого потока. В квантовой теории электромагнитное излучение существует в виде «порций» энергии (квантов). Энергия кванта излучения лучистого потока связана с частотой излучения. Этот постулат создает фундаментальные предпосылки для формулировки физического понятия энтропии, определяемой в терминах энергетического спектра.

Действительно, принимая дуализм определения светового потока, где отмечаем реальную физическую возможность увеличения частоты излучения, постулируем невозможность существования квантов с бесконечно большой энергией.

В таком случае взаимная связь энергии излучения сферического физического источника, связанная с определением энтропии, определяется из выражения:

$$L_p = a(2.28\left(1 - \frac{(b-1)}{a}\right)^{1.308} + 4),$$

где $a = b = 1$ – параметры сферы.

Для лучистого потока с круговой поляризацией имеем: $L_0 = 2\pi$, что соответствует состоянию точечного источника излучения при физической температуре $-273{,}15$ C^0.

Расширяя это, определение констатируем, что информационная энтропия вычисляется по выражению (1) и измеряется в битах:

$$H(X)_L = \frac{L_p}{L_0}. \quad (1)$$

Типичными объектами в физике являются атомарные конструкции химических элементов. Проведем расчет информационной энтропии для некоторых химических элементов [5]. Результаты представим в таблице 1.

ТАБЛИЦА 1. Набор химических элементов

	Химический элемент				
	Литий	Бериллий	Бор	Углерод	Азот
	Li	**Be**	**B**	**C**	**N**
Атомный номер	3	4	5	6	7
Атомная масса	7	9	11	12	14
Протоны	4	5	6	6	7
Нейтроны	3	4	5	6	7
	Информационная энтропия $H(X)_L$, бит				
	17.49	21.39	25.31	24.00	28.00

Представленные расчетные значения информационной энтропии позволяют оценить возрастающую степень сложности атомарных конструкций.

Рассмотрим примеры литературных произведений [1]. Результаты представим в таблицах 2 и 3.

ТАБЛИЦА 2. Литературный стиль

Фрагмент анализируемого текста	$H(X)_L$, бит
Н. Лесков. Проза «Зимний день»	
Зимний, северный день с небольшою оттепелью. Два часа. Рассвет не успел оглядеться, и опять смеркается. В гостиной второй руки сидят за столом хозяйка и гостья.	Количество символов: 96251 Количество слов: 16141 $H(X)_L$= 72659.5129

ТАБЛИЦА 3. Поэтический стиль

Фрагмент анализируемого текста	$H(X)_L$, бит
А. Блок. Стихотворение – «Авиатор»	
Летун отпущен на свободу. Качнув две лопасти свои, Как чудище морское в воду, Скользнул в воздушные струи. Его винты поют, как струны... Смотри: недрогнувший пилот К слепому солнцу над трибуной	Количество символов: 1331 Количество слов: 203 $H(X)_L$= 1035.3106

Фрагмент анализируемого текста	$H(X)_L$, бит
А. Блок. Стихотворение – «Авиатор»	
Стремит свой винтовой полет... Уж в вышине недостижимой Сияет двигателя медь... Там, еле слышный и незримый, Пропеллер продолжает петь...	

Рассмотрим нуклеотидные наборы, составляющие генетические конструкции разных организмов. В качестве примера рассмотрим нуклеотидный набор из аденина (A), гуанина (G), тимина (T) и цитозина (C) – фрагмент вируса Abaca Bunchu [4, 5]. Результаты представим в таблице 4.

ТАБЛИЦА 4. Генетический код

	Фрагмент анализируемого кода	$H(X)_L$, бит
1.	G	
2.	A	Количество символов: 14
3.	A	Количество словоформ –
4.	G	парных сочетаний: 8
5.	T	
6.	T	$H(X)_L$= 4.4563
7.	T	
8.	C	
9.	C	
10.	A	
11.	C	
12.	A	
13.	C	
14.	A	

Понятие энергии и энтропии источника составляют фундаментальное определение базовых понятий современной физики, математической лингвистики и теории сигналов. Рассматривая окружность, как модель сложной системы, обладающей бесконечным и счетным количеством разнообразных форм состояний, устанавливается алгоритм вычисления информационной энтропии, представленный в терминах алгебраической геометрии с использованием иррационального числа π.

Наличие строгих, с точки зрения физики и биофизики представлений о возможности сопоставления описаний различных по своей природе систем и объектов реализуется на понятии лучистого потока, для которого формально выделяются два состояния с единичным значением и бесконечно большим значением информационной энтропии. Формализм оценки состояния сложной природной системы, самостоятельно реализующей некоторый творческий процесс, оценивается значением энтропии, выраженной в угловых единицах – радианах, а информационной энтропии в битах.

Сохраняя общность постулатов физической теории оценки состояния сложных систем, показана возможность вычисления информационного показателя энтропии [4], выраженного в битах, для разных объектов, в том числе и результатов творчества в эпистолярном жанре.

Список используемых источников

1. Макаров Л. М., Поздняков А. В., Протасеня С. В. Эргодическая модель атомарных конструкций // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 74–84.
2. Lit-classic.ru. Русская классическая литература. URL: https://litclassic.ru/index.php?fid=1&sid=6
3. NCBI информационный ресурс. URL: https://www.ncbi.nlm.nih.gov/nuccore.
4. Макаров Л. М. Информационная энтропия. International scientific review of the problems and prospects of modern science and education. Collection of scientific articles LXVII International correspondence scientific and practical conference. 2020. С. 7–12.
5. Макаров Л. М., Поздняков А. В., Протасеня С. В. Агрессивность коронавируса // Инновационные технологии современной научной деятельности: стратегия, задачи, внедрение. Сборник статей по итогам Международной научно-практической конференции. 2020. С. 11–16.

УДК 004.491
ГРНТИ 81.93.29

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ОСУЩЕСТВЛЕНИЯ КИБЕРАТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье приводится анализ результатов воздействий на информационные ресурсы Российской Федерации, технических возможностей инструментальных средств. Предложены рекомендации по совершенствованию системы защиты информационных систем и состав комплекса первоочередных мер по реагированию на компьютерные инциденты.

компьютерный инцидент, критическая информационная инфраструктура, атака.

В первой половине февраля 2022 года на многочисленные информационные ресурсы Российской Федерации были осуществлены компьютерные

атаки, результатом которых стала модификация программного обеспечения (ПО) веб-сайтов. Однако в ряде случаев на работоспособности сайтов это явным образом не отразилось, другие стали недоступны или работали с ошибками. Позже после начала специальной военной операции России на Украине значительно возросло количество компьютерных атак на критическую информационную инфраструктуру РФ. В первую очередь осуществлялись *DDoS*-атаки, как наиболее доступные для реализации и не требующие сложной реализации, а также осуществлялись атаки, направленные на подмену содержания веб-ресурсов, модификацию ПО, сбор информации, распространение недостоверных сведений.

Анализ последствий компьютерных инцидентов, выявленных до начала специальной военной операции, позволяет сделать однозначный вывод о том, что первая волна компьютерных атак являлась подготовкой для создания инструментальной базы, используемой в дальнейших волнах кибератак.

В результате одной из методик реализации компьютерной атаки первой волны взломов сайтов осуществлялись следующие воздействия.

На первом этапе осуществлялось предварительное сканирование информационной системы на предмет наличия уязвимостей (разведка – 1-й этап реализации *APT*-угроз согласно матрицы *MITRE ATT&CK – https://mitre.ptsecurity.com*) с последующей подготовкой средств воздействия.

Далее осуществлялось получение первичного доступа средствами имеющихся эксплойтов с выполнением следующих операций:

Модификация точки входа сайта за счет изменения файла *.htaccess,* а также добавления файлов *.htaccess* в каталоги, доступные для записи. Примеры вариантов содержания модифицированного файла приведены ниже:

Вариант 1. Замена или определение точки входа сайта.

```
DirectoryIndex index.php
```

Вариант 2. Разрешение исполнения заданных типов файлов.

```
<FilesMatch
".(py|exe|phtml|php|PHP|Php|PHp|pHp|pHP|phP|PhP|php5|suspected
)$">
Order Allow,Deny
Deny from all
</FilesMatch>
```

Загрузка веб-шеллов – сценариев, исполняемых интерпретатором веб-сервера. Наименование файлов с кодом веб-шеллов – сформированно псев-

дослучайным образом. Код веб-шелла защищен от обнаружения обфускацией. Размер подгружаемых веб-шеллов варьировался от нескольких сотен байт до сотен килобайт.

Примеры веб-шеллов показаны ниже

Вариант 1. Фрагмент обфусцированного сценария вредоносного кода.

```
<?php /* tjwlltii akhmhcij
*/error_reporting(0);ini_set("display_errors",
0);if(!defined('lmhelqpg')){define('lmhelqpg',__FILE__);if(!fu
nction_exists(""гЧ©$ЉаЕуц")){func-
tion  ИљБЃХМіЧ($Т-Ъњвфsћц){globa……
```

Вариант 2. Закодированные данные.

```
Lm51dHJpdGlvbmZvcmNlLmluaw==|NTAwLm51dHJpdGlvbmZvcmNlLmluaw==
```

Вариант 3. Закодированные данные.

```
MDUyOWxmLnR4dHxsMDMwOS0xLnR4dHwwNTI5bGYudHh0fGtrMTA-
wOC50eHR8MDUyOWxmLnR4dA==-M2luZGV4LnBocHxvbGQtaW5kZXgucGh-
wfHdwLWNvbnRlbnQvbXUtcGx1Z2lucy1vbGQvaW5kZXgucGhwfHdwL-
WFkbWluLnBocHxhZG1pbi5waHA=
```

Вариант 4. Фрагмент обфусцированного сценария фредоносного кода.

```
<?php
 $uoeq967= "O)sl 2Te4x-
+gazAbuK_6qrjH0RZt*N3mLcVFEWvh;inySJC91oMfYXId5Up.(GP7D,Bw/kQ8
";$vpna644='JGNoID0gY3VybF9pbml0KCdodHRwOi8vYmFua3N';$vpna645=
…
```

Обфускация программного кода в общем случае является необратимой [1]. Однако существуют подходы, позволяющие получить фактически исполняемых интерпретируемый код, соответственно, получить возможность восстановить алгоритм веб-шелла [2]. При декодировании кода некоторых веб-шеллов был обнаружен код, представленный на рис. 1.

```
$code = "http://".$_GET["php"];
//если $code пуст или неопределен or !находит первое вх
if (empty($code) or !stristr($code, "http"))
      {
            exit;
      }
else
      {
            //получить либо, если это веб-страница, то
            $php=file_get_contents($code);
            //парсит страницу php + eval($php) -> вызыв
            if (empty($php))
                  {
                        $php = curl($code);
                  }
            $php=str_replace("<?php", "", $php);
            $php=str_replace("?>", "", $php);
            eval($php);
```

Рис. 1 Деобфусцированный код веб-шелла

Представленный деобфусцированный код способен получать полезную нагрузку через *HTTP*-запрос методом *GET* (посредством извлечения данных из пакета *$_GET["php"]*, а затем исполнять его с помощью функции *eval($php)*.

Поскольку данные сайт получает извне, то фактически реализована возможность исполнения произвольного кода.

В 2016 году работе [3, 4] рассматривался подход построения анонимной устойчивой сети, построенной на подобном коде, с указанием угроз и возможностей, которые он дает, исследовалась устойчивость построенной сети. А в работе [5] продемонстрирована возможность использования сети для распределённого анонимного тестирования защищенности веб-ресурсов, которые, при другой целевой установки носят характер целенаправленных компьютерных атак.

Схема доступа посредством сети скомпрометированных информационных систем с последующей реализацией компьютерной атаки показана на рис. 2.

Особенность такого подхода заключается в использовании скомпрометированных сайтов как перевалочных пунктов передачи пакетов данных, содержащих деструктивный код, что с одной стороны маскирует источник атаки, а с другой за счет механизма исполнения переданных данных (активных данных [6]), позволяет не хранить в скомпрометированных системах полезную нагрузку, а передавать ее.

В качестве средств своевременного обнаружения, реагирования на компьютерные инциденты, устранения последствий может использовать достаточно большой перечень средств защиты. Обобщенная схема возможных СЗИ, которые могут применяться на стороне защищаемой информационной системы показана на рис. 3.

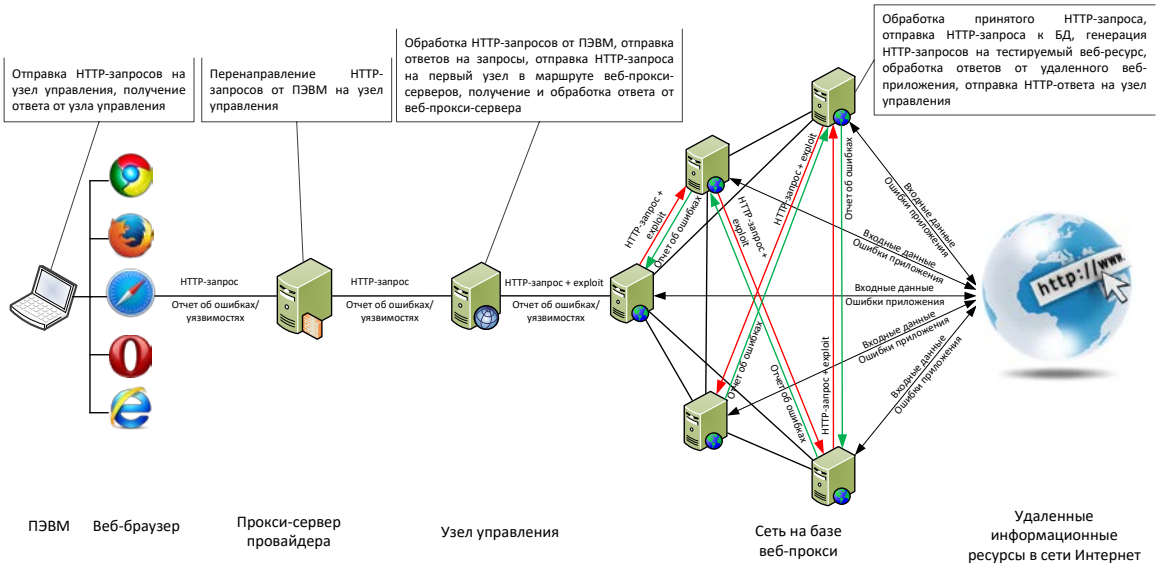


Рис. 2. Схема компьютерной атаки с использованием сети веб-прокси серверов

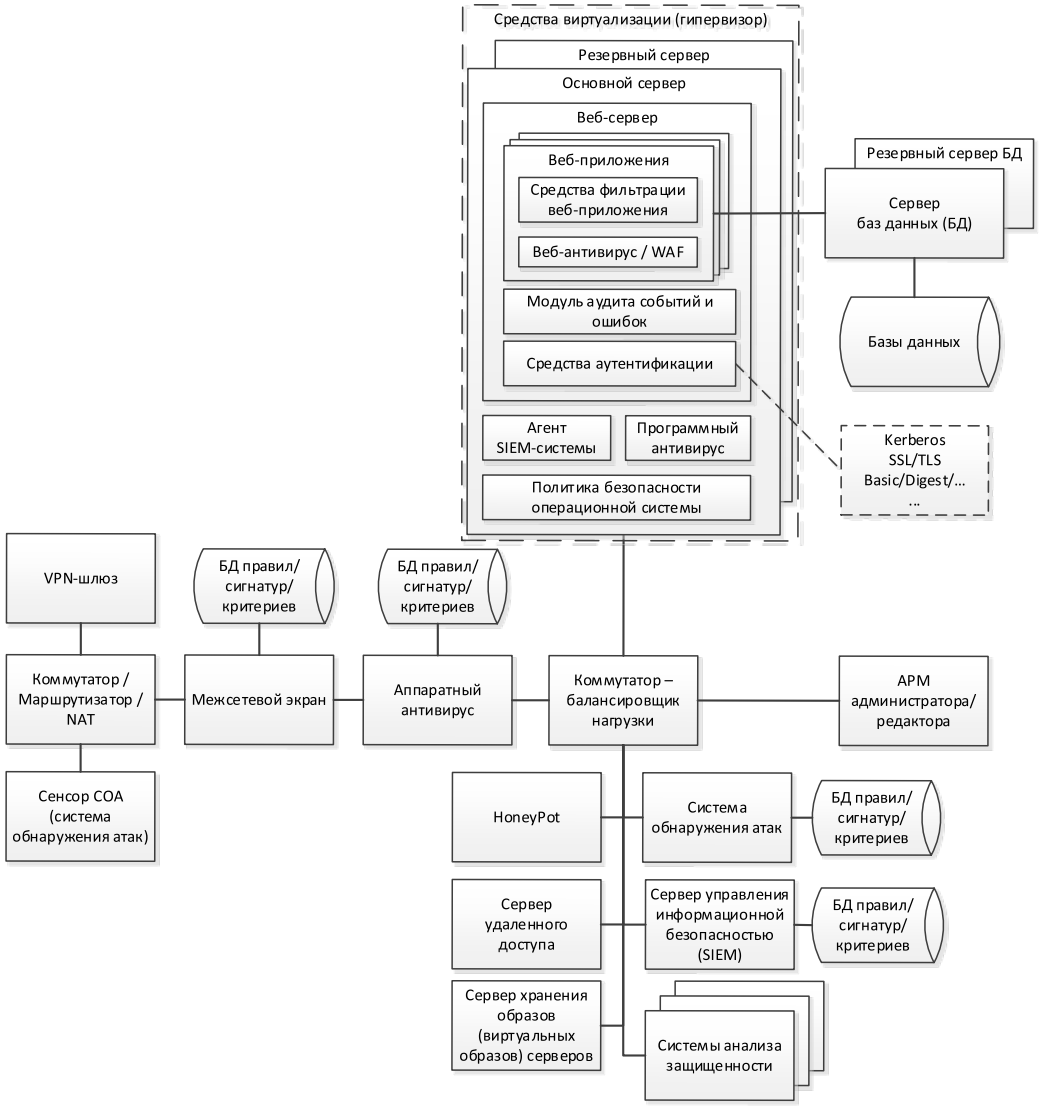


Рис. 3. Средства защиты информационных систем

Для противодействия рассмотренному классу компьютерных атак в первую очередь необходимо использовать средства межсетевого экранирования, особенно *WAF* – межсетевые экраны уровня веб-приложений. В государственном реестре сертифицированных средств защиты (СЗИ) ФСТЭК России (*https://fstec.ru*) в настоящее время (по состоянию на март 2022 года) средств, относящихся к *WAF* (тип «Г»), сравнительно немного:

1. Система защиты приложений от несанкционированного доступа *Positive Technologies Application Firewall* (сертификат соответствия № 3455) от ООО «Прорывные технологии».

2. Средство защиты информации "Континент *WAF*" (сертификат соответствия № 4044) от ООО «Код безопасности».

3. Программный комплекс "*InfoWatch Attack Killer*" (сертификат соответствия № 4255) от АО «ИнфоВотч».

Таким образом, анализ возможностей инструментальных средств, примененных для кибератак на критическую информационную инфраструктуру РФ, показал, что

- сценарий рассмотренного класса атак – многоэтапный;
- в качестве непосредственных средств реализации атак используются скомпрометированные информационные ресурсы на территории России;
- современная система безопасности сети связи общего пользования, управление которой в настоящее время возложена на Роскомнадзор (согласно Постановлению Правительства РФ от 12.02.2020 № 127), требует серьезной адаптации к актуальным угрозам.

Список используемых источников

1. Маркин Д. О., Рыков Д. А. Методы и средства обфускации и деобфускации исходных текстов веб-приложений на языке Javascript // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. Санкт-Петербург: СПбГУТ, 2020. Т. 2. 748 с. С. 520–524.

2. Маркин Д. О., Звягинцев С. А., Павлов Д. И. Методы и средства анализа программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. Санкт-Петербург: СПбГУТ, 2019. Т. 2. 603 с. С. 293–298.

3. Маркин Д. О., Архипов П. А., Галкин А. С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21–28. DOI: 10.21681/2311-3456-2016-2-21-28.

4. Маркин Д. О., Галкин А. С., Архипов П. А. Организация анонимного доступа с помощью веб-прокси // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8, № 5. С. 44–49.

5. Маркин Д. О., Галкин А. С., Архипов П. А. Алгоритм распределенного тестирования веб-приложений на основе технологий веб-прокси и активных данных // Информационные системы и технологии. 2018. № 1 (105). С. 93–101.

6. Кулешов С. В., Цветков О. В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы. 2014. № 6. С. 12–19.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЭВМ НА ОСНОВЕ ПРОЦЕССОРОВ С АРХИТЕКТУРОЙ ARM

Д. О. Маркин, А. С. Мищенко, Ч. Т. Хо

Академия Федеральной службы охраны Российской Федерации

В статье приводится подход по исследованию на предмет наличия потенциально опасных объектов встроенного программного обеспечения ЭВМ на основе процессоров с архитектурой ARM (трастлетов). Описаны модель трастлета, структурная схема средства анализа, алгоритм кластеризации бинарных файлов трастлетов. Целью работы является совершенствование инструментальных средств по анализу встроенного программного обеспечения на предмет выявления уязвимостей и недекларированных возможностей в них. Представлена оценка эффективности разработанного подхода при анализе трастлетов, свидетельствующая об увеличении полноты информации об объектах анализа.

трастлет, TrustZone, ARM, уязвимости, недекларированные возможности.

Безопасность множества современных мобильных устройств основывается на использовании доверенных сред исполнения (ДСИ). Считается, что ДСИ имеют высокую степень защищенности, и технология *TrustZone*, в частности, применяется повсеместно [1].

Технология *TrustZone* реализуется каждым производителем со своими особенностями и программными решениями. Приложения ДСИ, функционирующие в защищенном мире и обрабатывающие критически важную информацию на устройствах, называются трастлетами [2]. Для анализа на наличие уязвимостей были выбраны приложения ДСИ от нескольких производителей: *Qualcomm*, *Trustonic*, *Linaro*. У каждого производителя исполняемые файлы имеют свою структуру. Разработаная схема средства анализа трастлетов показана на рис. 1.

Извлечение объектов производилось несколькими способами: из устройства напрямую при подключении к нему ЭВМ посредством *ADB Plugin* или извлечением системных директорий из образов встроенного программного обеспечения с помощью специализированных утилит из пакета *Android ROM Tool*.

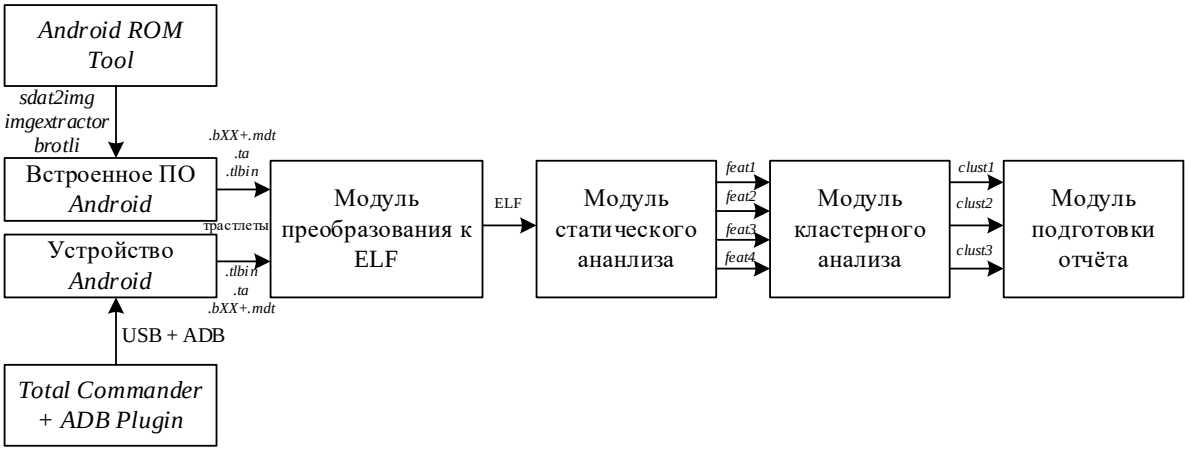


Рис. 1. Схема исследования трастлетов

Трастлеты от *Qualcomm* имеют *ELF* формат, расширенный сегментом с хеш-суммами. Однако на устройстве они хранятся как несколько файлов расширения *.bXX* и один файл *.mdt*. В дополнительный сегмент включаются: заголовок хеш-таблицы, хеш-сумма *ELF* заголовка и заголовка блока данных, хеш-сумма каждого из сегментов *.bXX*, подпись и цепочку сертификатов (рис. 2) [3]. Формирование файла происходит во время выполнения по информации о заголовках, представленной в файле *.mdt*.

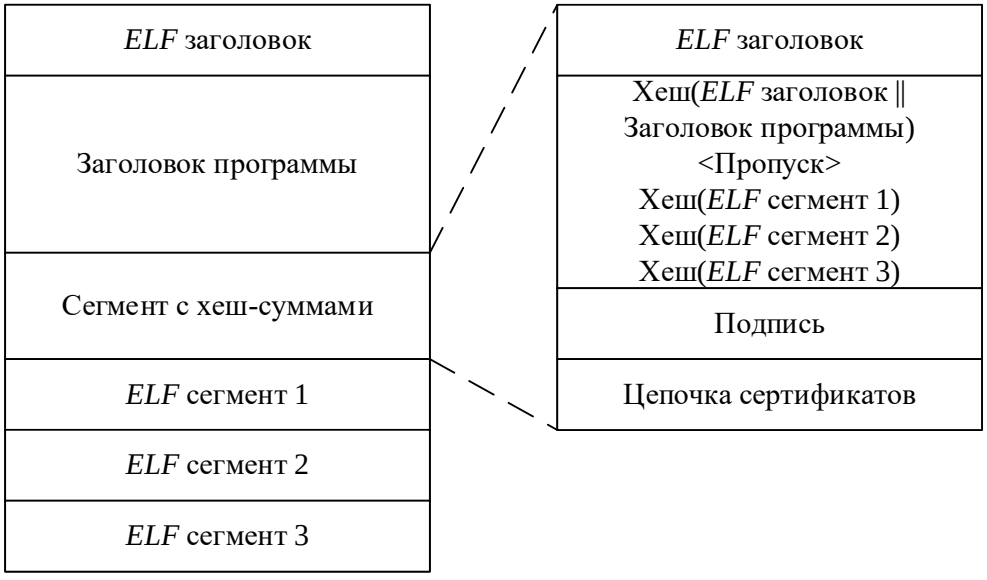


Рис. 2. Структура трастлета от производителя *Qualcomm*

Трастлеты от производителя *Trustonic* имеют формат *MobiCore Load Format*. Описание заголовка присутствует в открытых источниках [4] и позволяет проанализировать реальную структуру файла (рис. 3). Затем, зная конкретные адреса памяти, можно реализовать искусственное преобразование формат *MCLF* к формату *ELF* для последующего анализа в качестве обычного исполняемого файла.

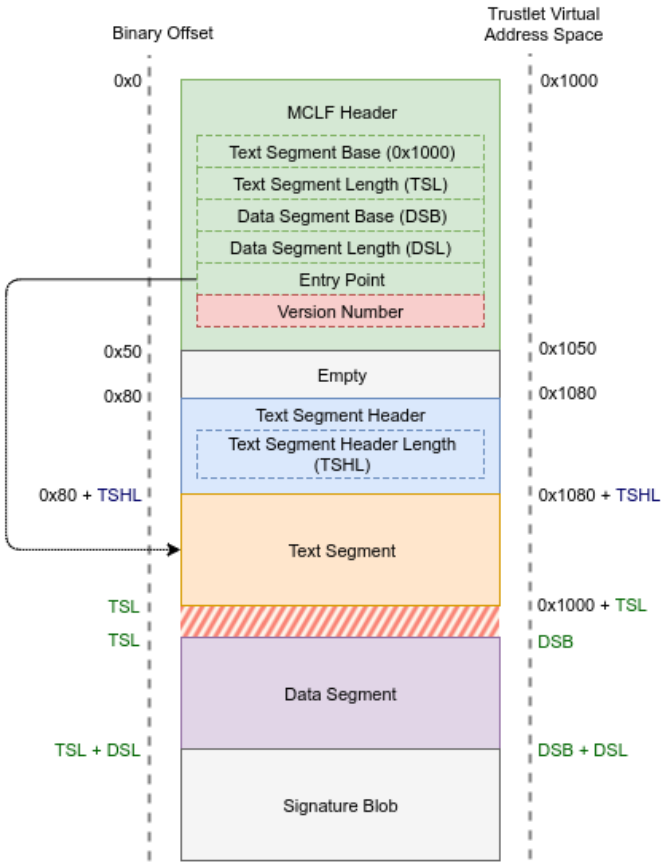


Рис. 3. Структура трастлета формата *MCLF*

Трастлеты от производителя *Linaro* имеют формат *HSTO*. Это *stripped ELF* формат с добавленным заголовком (рис. 4).

Чтобы верно проанализировать данный формат исполняемого файла, достаточно передать часть зачищенного *ELF*.

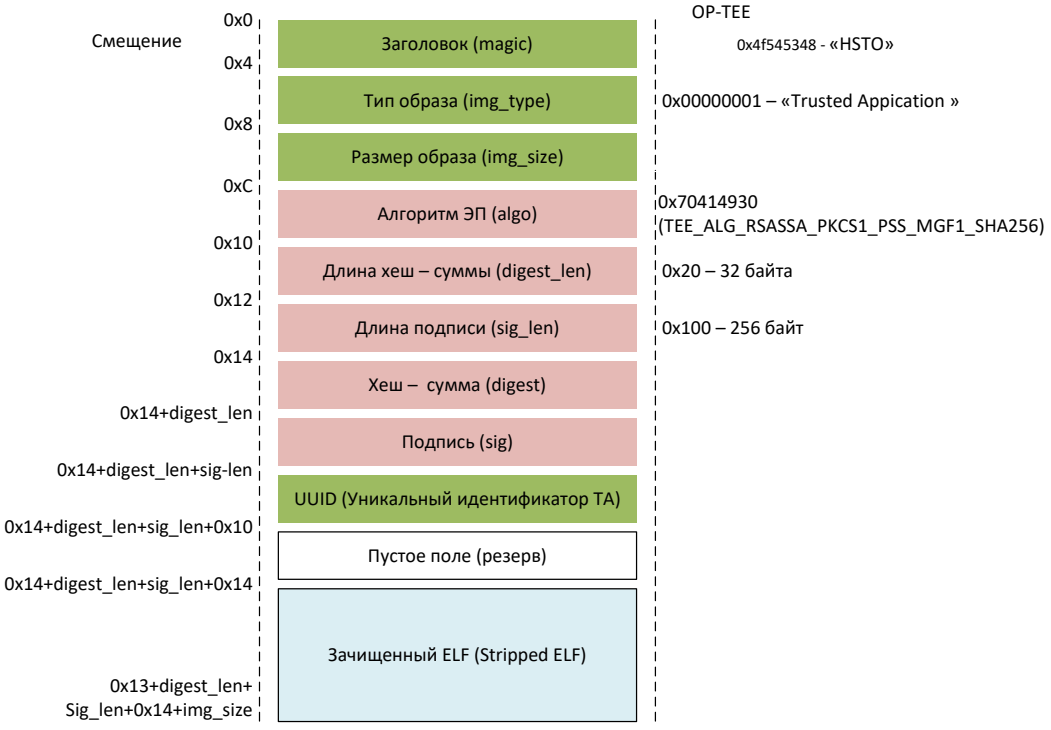


Рис. 4. Структура трастлета формата *HSTO*

После искусственного приведения файлов к *ELF*-подобному формату произведен статический анализ этих файлов на предмет наличия потенциально опасных функциональных объектов, а также выделения критически важных признаков для последующего определения степени угрозы безопасности обрабатываемой информации.

Были получены общие данные об исполняемом файле из заголовка, например, тип файла, язык программирования, на котором был написан, компилятор, с помощью которого был собран, и другие. Также была получена статистика вызова различных команд в программе. Были проанализированы все функциональные объекты и построен граф на основе связей между ними. Были исследованы вызовы системных и библиотечных функций, а также точки входа и выхода.

Для анализа большого объема исполняемых файлов и выделения из них потенциально опасных применен алгоритм машинного обучения без учителя. Для разделения приложений по степени угрозы безопасности обрабатываемой информации выбран алгоритм кластеризации *k*-средних. Действие алгоритма заключается в минимизации суммарного квадратичного отклонения объектов кластера от центров данных кластеров.

В эксперименте для трастлетов формата *HSTO* в качестве критически важных признаков было выделено количество точек входа (*IN*), выхода (*OUT*), а также вызовы системных (*SYSCALL*) и библиотечных (*LIB*) функций. После применения алгоритма кластеризации по данным признакам было получено три группы со схожими расстояниями до центров кластеров. Результаты анализа файлов *HSTO* выборочно приведены в таблице 1. Каждому файлу присваивается своя метка, обозначающая номер кластера.

Для трастлетов двух других форматов более репрезентативным признаком является статистика появления команд в файле. На основе этого признака была также произведена кластеризация данных и получены три множества со схожими признаками. Результат анализа частично приведен в таблице 2.

Результат работы заключается в возможности распределения исследуемых объектов по уровню угроз безопасности потенциально опасных функциональных объектов из однородного множества. Также в возможности по детальному анализу одного экземпляра из каждого кластера судить всей группе и автоматизации процесса исследования встроенного программного обеспечения для ЭВМ на основе процессоров с архитектурой *ARM*.

ТАБЛИЦА 1. Результаты кластерного анализа формата *HSTO*

Файл	***IN***	***OUT***	***SYSCALL***	***LIB***	**Кластер**
5b9e0e40-2636-11e1-ad9e-0002a5d5c51b.ta	0	0	12	12	0
873bcd08-c2c3-11e6-a937-d0bf9c45c61c.ta	2	2	13	7	0
e6a33ed4-562b-463a-bb7e-ff5e15a493c8.ta	0	0	15	0	0
e13010e0-2ae1-11e5-896a-0002a5d5c51b.ta	0	0	56	2	1
614789f2-39c0-4ebf-b235-92b32ac107ed.ta	0	0	47	0	1
484d4143-2d53-4841-3120-4a6f636b6542.ta	0	0	55	1	1
ffd2bded-ab7d-4988-95ee-e4962fff7154.ta	2	2	57	56	2

ТАБЛИЦА 2. Результаты кластерного анализа формата *MCLF*

Файл	***mov***	***str***	***ldr***	***cmp***	***b***	***add***	***movs***	**Клас-тер**
ffffffff000000000000000000000060.tlbin	152	81	135	28	29	35	133	0
ffffffffd00000000000000000000016.tlbin	177	97	278	62	88	68	136	0
ffffffff000000000000000000000041.tlbin	146	116	157	105	67	27	2286	1
ffffffffd0000000000000000000000e.tlbin	483	143	446	144	148	83	318	2
ffffffffd00000000000000000000017.tlbin	420	121	369	135	121	55	263	2
ffffffff000000000000000000000000f.tlbin	252	128	282	102	107	76	434	2

Список используемых источников

1. Маркин Д. О., Чунг Х. Т. Исследование уязвимостей доверенной среды исполнения в приложении на основе технологии TrustZone // Известия ТулГУ. Технические науки. 2020. № 9. С. 316–328.
2. TrustZone: Доверенная ОС и ее приложения. URL: https://www.aladdin-rd.ru/company/pressroom/articles/trustzone-doverennaa-os-i-ee-prilozenia (дата обращения: 10.03.2022).
3. Trust Issues: Exploiting TrustZone TEEs. URL: https://googleprojectzero.blogspot.com/2017/07/trust-issues-exploiting-trustzone-tees.html (дата обращения: 10.03.2022).
4. Android user space components for the Trustonic Trusted Execution Environment. URL: https://github.com/Trustonic/trustonic-tee-user-space/blob/master/common/MobiCore/inc/mcLoadFormat.h (дата обращения: 10.03.2022).

УДК 004.491
ГРНТИ 81.93.29

СРЕДСТВО ОБЕСПЕЧЕНИЯ РАЗВЕДЗАЩИЩЕННОСТИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Д. О. Маркин, Н. Н. Молчанов, А. В. Щукин

Академия Федеральной службы охраны Российской Федерации

В статье приводится описание технологии обеспечения разведзащищенности средств тестирования на проникновения, основанной на использовании цепочки веб-прокси серверов. Приводится анализ современных средств тестирования на проникновение, а также технологий анонимизации. Показано, что для передачи сетевых пакетов через цепочку веб-прокси серверов необходима реализация вспомогательных средств трансляции сетевых пакетов в сценарии активных данных на интерпретируемых языках программирования. Представлена структурная схема системы обеспечения разведзащищенности. Предложены дополнительные меры защиты от компрометации узлов сети веб-прокси серверов.

тестирование на проникновение, веб-прокси, активные данные, анализ защищенности.

Современные системы безопасности информационных систем могут обладать эшелонированной системой защиты, построенной на базе средств фильтрации – межсетевых экранов, антивирусной защиты, средств предупреждения (*IPS*) и обнаружения вторжений (*IDS*), средств управления инцидентами информационной безопасности (*SIEM*), средств реализации ловушек и дезинформирования (*HoneyPot*, *Deception*). При необходимости исследования потенциальных уязвимостей информационных систем, защи-

щенных средствами из указанного перечня, возникает объективная потребность исследования возможности повышение эффективности средств анализа уязвимостей, средств анализа защищенности (САЗ) и средств тестирования на проникновение. Одним из показателей эффективности указанных средств является разведзащищенность, который может выражаться в вероятности идентификации источника, реализующего тестирование на проникновения, с целью его последующей блокировки.

К современным средствам тестирования на проникновения относятся:

– *Metasploit* от *Rapid 7* (США);

– *RedCheck* от АО Алтекс-Софт (Россия, сертификат соответствия ФСТЭК России № 3172);

– *MaxPatrol* от ООО "Прорывные технологии" (Россия, сертификат соответствия ФСТЭК России № 2922);

– утилиты *Kali Linux* от *Offensive Security* (США);

– *Core Impact* от *Core Security* (США);

– *Burp Suite* от *PostSwigger* (Великобритания);

– «Ревизор Сети» от ФГУП «НПП Гамма» (Россия, сертификат соответствия ФСТЭК России № 845/2);

– «Сканер-ВС» от АО «НПП «Эшелон» (Россия, сертификат соответствия ФСТЭК России № 2204).

Классический подход повышения разведзащищенности построены на основе применения цепочек прокси-серверов. Например, широко известное средство анализа защищенности *nMap* позволяет использоваться утилиту *proxychains* либо ее более современный аналог *ProxyChains-NG* – средство, перенаправляющее трафик через цепочку предопределенных прокси-серверов различных типов (*socks5, http, socks4* и др.). К аналогам данного средства относятся утилиты *SocksCap*, *CacheGuard-OS*. *tsocks* и ряд других.

Еще один способ повышения разведзащищенности заключается в использовании сети, создаваемой *tor*-браузером, в качестве транспорта запросов. Считается, что *tor*-браузер позволяет обеспечить анонимность (хотя, хорошо известно, что данные проект спонсируется силовыми ведомствами США, соответственно, доверие к реальному обеспечению анонимности нет). Для перенаправления сетевого трафика через создаваемую *tor*-браузером сеть используются такие утилиты как:

- o*rjail* – создает сетевое окружение для запускаемой программы);
- *torctl* – использует комбинацию средств *Tor* и *iptables*;
- *AnonSurf* – перенаправляет сетевой трафик и *DNS*-запросы через сеть *Tor*;
- *Nipe* – создает в качестве шлюза по умолчанию сеть *Tor*;
- *Tor Router* – использует сеть *Tor* как прозрачный прокси, перенаправляя в него сетевой трафик и *DNS*-запросы;

• *TorIpTables2* – средство настройки *Tor* и *iptables* для перенаправления сетевого трафика через них.

Третий вариант основ на использовании известных *VPN*-сервисов, для формирования логических каналов на их основе. К утилитам, позволяющим использовать (псевдо)случайный *VPN*-сервер относится средство *autovpn*.

В данной работе предлагается в качестве цепочки прокси-серверов использовать объединенные в управляемую программную сеть на базе веб-серверов и виртуальных узлов, содержащих интерпретируемые сценарии, реализующие функционал веб-прокси-сервера.

Принцип, лежащий в основе управляемой сети, заключается в использовании инструкций интерпретируемых языков программирования (*PHP*, *Python*, *Perl* и др.), позволяющих исполнять переданный им параметра. Пример такого кода показан на рисунке 1.

На рисунке данные из *HTTP*-запроса, переданные методом *GET*, передаются для исполнения в функцию *eval()*, реализуя таким образом технологию исполнения активных данных, описанную в работах [1–3]. Учитывая, что переданный код, может инициировать новое соединение в отдельном потоке, то может быть построена бесконечно длинная цепочка, которая помимо передачи запросов далее по цепочке, может исполнять и некоторую полезную нагрузку. Эффективность такого подхода была проверена и результаты представлены в работах [2–4].

```
$code = "http://".$_GET["php"];
//если $code пуст или неопределен or !находит первое вх
if (empty($code) or !stristr($code, "http"))
	{
		exit;
	}
else
	{
		//получить либо, если это веб-страница, то
		$php=file_get_contents($code);
		//парсит страницу php + eval($php) -> вызыв
		if (empty($php))
			{
				$php = curl($code);
			}
		$php=str_replace("<?php", "", $php);
		$php=str_replace("?>", "", $php);
		eval($php);
```

Рис. 1. Сценарий исполнения активных данных

Пример построения цепочки последовательной передачи активных данных с исполнением полезной нагрузки показан на рис. 2.

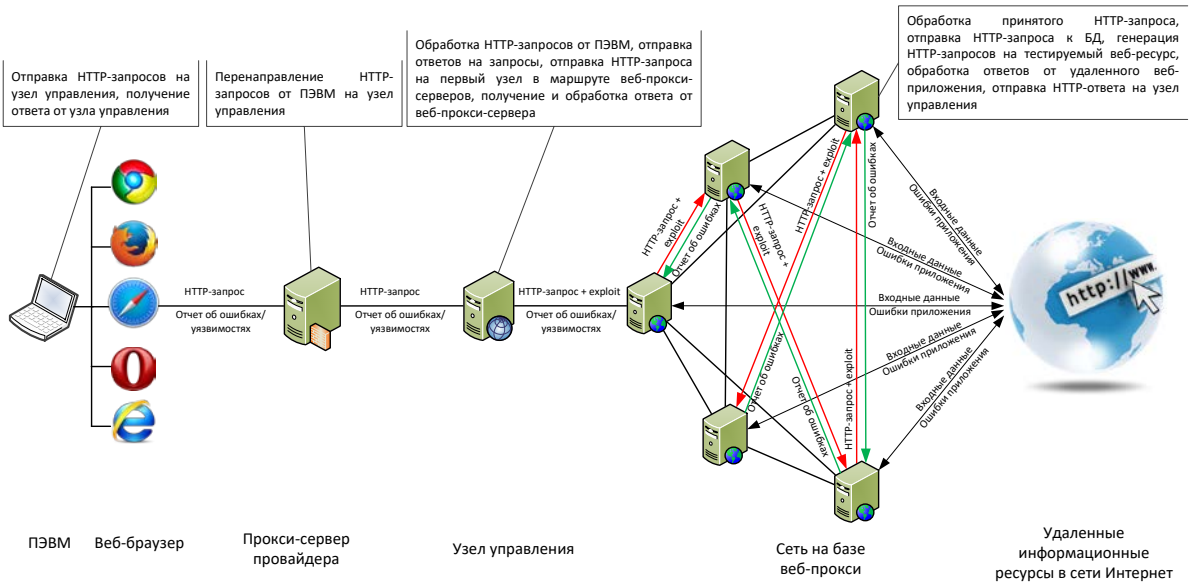


Рис. 2. Схема передачи активных данных по цепочке веб-прокси серверов

Для использования цепочки на основе веб-прокси серверов необходимо решить задачу построения интерфейса между САЗ или средства тестирования на проникновения и точкой входа в сеть веб-прокси-серверов. Иными словами, сетевой трафик, передаваемый от САЗ или средства тестирования на проникновение необходимо транслировать в активные данные – сценарий на интерпретируемом языке программирования, который будет исполняться на узлах цепочки веб-прокси-серверов. Схема трансляции выглядит так, как показано на рис. 3.

Рис. 3 Структура системы обеспечения разведзащищенности анализа защищенности и тестирования на проникновения

Порядок функционирования представленной системы следующий:

4. Защищаемые САЗ и/или средства тестирования на проникновение инициируют последовательность сетевых пакетов.

5. Передаваемые сетевые пакеты захватываются программным прокси-сервером и передаются транслятору.

6. Транслятор осуществляет синтаксический анализ полученных сетевых пакетов и формирует сценарий на заданном интерпретируемом языке программирования, который при исполнении отправит идентичный сетевой пакет, полученный транслятором от прокси-сервера.

7. Сформированный сценарий передаются средству подготовки активных данных, который упаковывается в сценарий активных данных, содержащий функциональные возможности по интеллектуальному построению псевдослучайного маршрута передачи через цепочку прокси-серверов и ряд других необходимых функций.

8. Сформированный пакет активных данных передаются в сеть веб-прокси серверов, в которых осуществляется продвижение пакета по заданному псевдослучайному маршруту, в конце которого исполняется сценарий, формирующий и передающий целевой информационной системе сетевой пакет, полученный от САЗ и/или средства тестирования на проникновение.

9. После получения ответа или иной реакции целевой информационной системы, формируется сценарий активных данных, который передается по обратной цепочке веб-прокси серверов к источнику.

10. Из полученного сценария активных данных извлекается сведения об ответе целевой информационной системе, которые передаются их первоначальному источнику – САЗ и/или средству тестирования на проникновение.

Представленная система обеспечения разведзащищенности позволяет использовать вместо дорогостоящих *VPN*-сервисов и/или недоверенных общедоступных прокси-серверов или систем анонимизаций типа *Tor* сеть виртуальных узлов, которые значительно доступнее и проще в настройках.

В целях обеспечения дополнительной защиты данных узлов могут использоваться методы обфускации сценариев [5], реализующих функции веб-прокси, в том числе с использованием защиты на основе несимметричных криптографических ключей.

Список используемых источников

1. Кулешов С. В., Цветков О. В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы. 2014. № 6. С.12–19.

2. Маркин Д. О., Архипов П. А., Галкин А. С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21–28. DOI: 10.21681/2311-3456-2016-2-21-28.

3. Маркин Д. О., Галкин А. С., Архипов П. А. Организация анонимного доступа с помощью веб-прокси // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8, № 5. С. 44–49.

4. Маркин Д. О., Галкин А. С., Архипов П. А. Алгоритм распределенного тестирования веб-приложений на основе технологий веб-прокси и активных данных // Информационные системы и технологии. 2018. № 1 (105). С. 93–101.

5. Маркин Д. О., Макеев С. М., Вихарев А. Н. Комплекс алгоритмов защищенных туманных вычислений на основе технологии активных данных // Известия Тульского государственного университета. Технические науки. 2019. Вып. 3. С. 263–269.

УДК 004.491.42
ГРНТИ 81.93.29

АЛГОРИТМ ИДЕНТИФИКАЦИИ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИХ АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Д. О. Маркин, Д. О. Некрасов

Академия Федеральной службы охраны Российской Федерации

Статья посвящена исследованию подходов по идентификации автоматизированных средств (ботов), осуществляющих анализ информационных систем. Представлены результаты сравнительного анализа известных средств автоматизированного анализа информационных систем. Предложена модель автоматизированного средства и алгоритм ее распознавания. Разработан алгоритм идентификации.

бот, средство анализа, информационная система, идентификация.

Информационные технологии постоянно совершенствуются. Увеличение доли использования веб-ресурсов для предоставления большого спектра услуг, включая государственные, обуславливают необходимость обеспечения их информационной безопасности. Как показывают отчеты компаний, предоставляющих услуги аудита и обеспечения защитного программного обеспечения (ПО), количество взломов, выведения из строя и компрометации сайтов постоянно растет. Из отчетов видно, что почти все атаки начинаются с разведки, а именно – сбора информации о потенциальном объекте атаки, используемых ресурсах, пользователях и прочих сведений. Доступных и очевидным средством разведки являются автоматизированные средств – веб-боты (боты) [1], позволяющие проводить анализ *HTML*-кода, подгружаемые скрипты, ответы сайта на специально сформированные запросы.

Под веб-ботом понимается специальная программа, выполняющая автоматически действия на веб-ресурсах через интерфейсы, предназначенные для людей. Соответственно для обеспечения комплексной информационной безопасности возникает необходимость обнаружения ботов. На данный момент существуют средства идентификации ботов, используемых крупными компаниями. Но эти средства являются проприетарными и недоступными для большинства веб-сайтов. Следовательно, всё большую актуальность приобретают задача разработки собственных средств, осуществляющих идентификацию этих ботов для повышения защищенности информационной системы.

Одним из эффективных способов решения данной задачи является анализ трафика веб-приложений [2], поведенческий анализ пользователей. Метод анализа веб-трафика заключается в проверке поступающих веб-сайту запросов и отправляемых им ответов по критериям полей. Поведенческий анализ пользователей заключается в исследовании, как он использует мышь, скорость ввода информации в поля, частота запросов и использование ссылок и т. д.

Для решения задачи идентификации необходимо провести классификацию веб-ботов. Пример такой классификации представлен в таблице 1 [3–4].

ТАБЛИЦА 1. Классификация веб-ботов

Название	**Описание**	**Примеры**
Краулеры	Веб-боты, собирающие веб-страницы	*SemrushBot, 360Spider, Heritix*
Социальные сети	Веб-боты различных социальных сетей	*LinkedInBot, WhatsApp Bot, Facebook Bot*
RSS-ридеры	Веб-боты, собирающие информацию с помощью RSS	*Feedfetcher, Feed Reader, SimplePie*
Поисковые движки	Веб-боты поисковых движков	*GoogleBot, BingBot, YandexBot*
Утилиты	Веб-боты, использующие различные библиотеки и утилиты для автоматизации	*Curl, Wget, python-requests, scarpy*
Веб-боты	Общая категория	
Неизвестные	Такие сессии, для которых не была известна разметка или значение поля *User-Agent* было пустым/отсутствовало	

Для решения задачи идентификации веб-ботов необходимо определить средства их обнаружения. В целом, все системы можно отнести либо к классу систем, работающих в режиме реального времени, либо к классу систем, работающих после завершения сессии. Оба класса могут использовать большинство известных методов обнаружения веб-ботов, таких как

анализ *IP*-адреса, анализ значения *HTTP/HTTPS*-заголовка *User-Agent* и др. Но, количество методов, доступных только для класса систем, работающих в режиме реального времени, как правило, больше количества методов, доступных для обоих классов. Также обнаружение ботов в режиме реального времени является более оперативным и дает больше времени для применения ответных мер. Наиболее полными и эффективными мерами обнаружения ботов являются: анализ полей *HTTP/HTTPS* пакета, значения полей веб-браузера пользователя, выявление особенностей поведения, не присущих человеку, использование «ловушек» для ботов.

В полях *HTTP/HTTPS* пакетов наибольший интерес представляет *IP*-адрес источника, то есть откуда был послан запрос. Для проверки *IP*-адреса используются черные списки адресов. Урезанные версии выкладываются некоторыми антивирусными компаниями. Черный *IP*-адрес – это адрес, который использовался злоумышленниками в качестве пункта управления для бот-фермы или адреса, на который присылается необходимая информация.

Так как значения полей *HTTP/HTTPS* можно подделать, то можно использовать данные о веб-браузере, полученные с помощью *JavaScript* (в дальнейшем *js*). Это позволяет увеличить вероятность обнаружить попытку подделать значения полей, а также получить больше данных для анализа и обнаружения бота. Так, можно проверять значения поля *Automated,* которое появляется у автоматизированных веб-браузеров, сравнивать размеры окна веб-браузера со стандартными размерами браузера, открываемого ботом, сравнивать значение *User-Agent* со значением из сетевых пакетов данной сессии.

Анализ поведения пользователя позволяет обнаружить черты, не присущие поведению на веб-сайте человека. Так, человек не сможет постоянно передвигать курсор с одинаковой скоростью, переходить по ссылке не нажав на неё, безошибочно печатать текст с большой скоростью или с большой скоростью заполнять поля без интервалов смены выделения поля. Такие черты поведения на веб-сайте позволяют утверждать, что действует бот.

Использование ловушек для ботов позволяет однозначно идентифицировать пользователя как бота. Данный метод можно отнести к поведенческому анализу, но с некоторыми особенностями. Ярким примером ловушки является размещение на веб-сайте невидимых ссылок или ссылок с нулевыми размерами. Так, человек не сможет перейти на неё, однако бот, сканирующий все элементы веб-страницы, сможет перейти на данную ссылку. Это является однозначным признаком бота.

Так как через веб-сервер проходит большой объем трафика, который предстоит анализировать, а любой из критериев проверки можно, как правило, легко подделать, то вытекает необходимость анализа по комплексу критериев, чтобы уменьшить вероятность ошибки первого рода. Так же

стоит учесть последовательность применения методов. Так, снятие отпечатков подключаемого устройства в начале сессии может дать информацию, однозначно определяющую бота, что позволяет либо прекратить дальнейший анализ, либо дальше изучать поведение уже определенного бота.

На основе вышеуказанных фактов можно составить алгоритм модуля идентификации автоматизированных средств анализа. Он должна включать несколько методов обнаружения средств анализа, выполняемых в определенной последовательности с учетом их специфики. Схема представлена на рисунке.

Так как поведение, теги *User-Agent HTTP/HTTPS*-заголовка и прочие атрибуты у всех ботов разные, то эта схема не является универсальной и требует доработки в зависимости от типа ботов, против которых она должна быть применена. Для создания более всеохватной схемы потребуется использование большего количества критериев, а также создание более сложных отдельных систем, например, нейронных сетей. С другой стороны, нужно учитывать ограниченность ресурсов сервера, так как увеличение количества принимаемых во внимание критериев увеличивает количество обрабатываемой информации, а для этого требуется большее количество ресурсов.

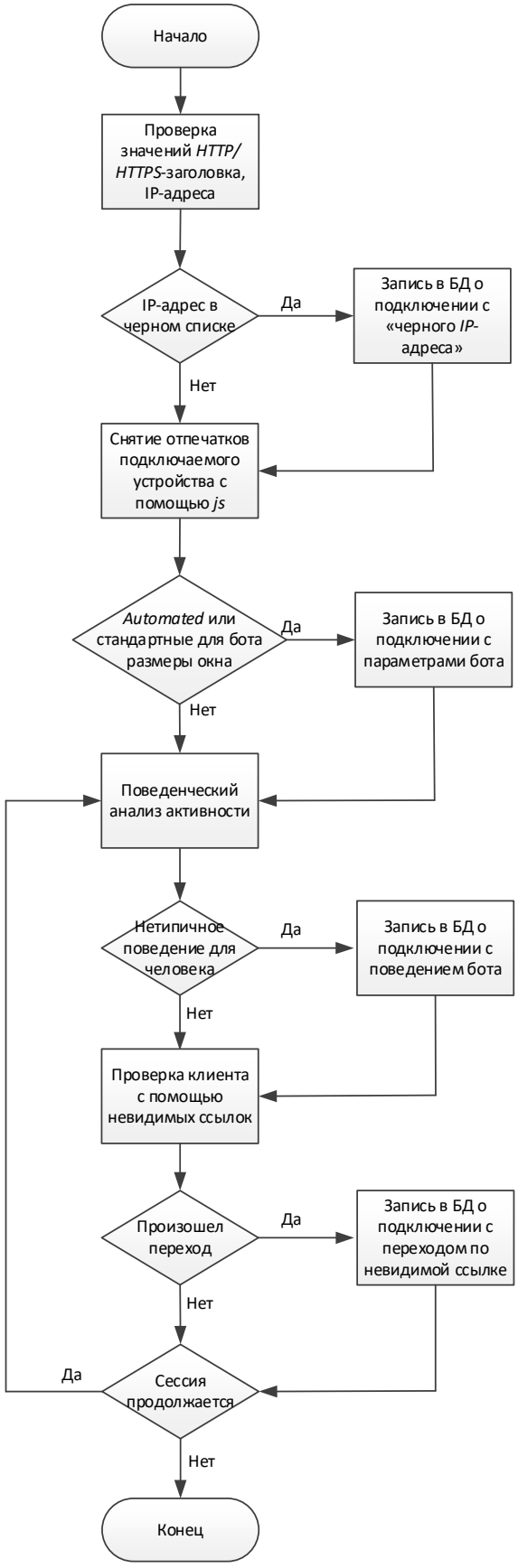


Рисунок. Алгоритм модуля идентификации автоматизированных средств анализа

Список используемых источников

1. Маркин Д. О., Зверев А. А., Макеев С. М. Алгоритм распознавания точек входа обфусцированных веб-приложений методом динамического анализа // Известия Тульского государственного университета. Технические науки. 2020. Вып. 9. С. 28–40.

2. Маркин Д. О., Архипов П. А., Галкин А. С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21–28.

3. Один подход к обнаружению веб-ботов, или Как мы использовали машинное обучение для классификации ботов. URL: https://www.securitylab.ru/blog/company/pt/349258.php (дата обращения: 10.03.2022).

4. Маркин Д. О., Некрасов Д. О. Анализ моделей автоматизированных средств, осуществляющих анализ информационной системы // Информационная безопасность и защита персональных данных: Проблемы и пути их решения : материалы XIII Межрегиональной научно-практической конференции / под ред. М. Ю. Рытова. Брянск: БГТУ, 2021. 283 с. С. 175–178. URL: http://mark.lib.tu-bryansk.ru/marcweb2/Found.asp (дата обращения: 10.03.2022).

УДК 004.056.52
ГРНТИ 81.93.29

СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ ВЕБ-САЙТА НА ОСНОВЕ ТЕХНОЛОГИИ HASP

Д. О. Маркин, Е. А. Никифорова, М. С. Шульгин

Академия Федеральной службы охраны Российской Федерации

В работе перечислены и дана краткая характеристика модулей системы защиты от несанкционированного использования информационной системы, доступ к которой осуществляется удаленно. Описана структурная схема системы и особенности реализации ограничения доступа к информационной системе на основе использования USB-ключа JaCarta и подсистемы перехвата системных вызовов с последующей фильтрацией доступа и защитой данных.

USB-токен, HASP, перехват системных вызовов, LD_PRELOAD.

Для решения задачи защиты авторских прав программного обеспечения (ПО) наряду с законодательными мерами широкое применения нашли технические средства защиты. Вместе с тем развитие цифровой экономики и предоставление услуг с использованием информационных систем (ИС), как частных, так и государственных, предъявило аналогичные требования по защите от несанкционированного использования уже в отношении веб-

сайтов и сложных ИС, доступ к которым предоставляется удаленно. Особенности реализации ИС и растущая сложность применяемых информационных технология требует применения новых подходов к реализации защиты от их несанкционированного использования таким образом, чтобы доступ к ИС предоставлялся только в случае ее правомерного использования, соблюдения авторских прав и лицензионного соглашения с правообладателем ИС.

При использовании ПО, которое имеет в своем составе средство защиты от несанкционированного использования (защита авторских прав), могут применяться следующие ограничения:

− ограничение числа скачиваний, установок и запусков программы;

− ограничение доступа за счет использования контрольных фраз или паролей;

− применение экземпляров ПО, которые требуют обязательного спустя определенное время;

− требование предъявления электронной почты пользователя с последующей рассылкой рекламных сообщений;

− требование предъявления электронной подписи пользователя;

− необходимость применения пары электронных ключей;

− навязчивые рекламные сообщения и напоминания о необходимости приобретения лицензии;

− напоминание об авторских правах (как способ психологического воздействия).

Вышеперечисленные методы осуществляются с помощью программных, программно-аппаратных средств и аппаратных средств защиты ИС и ПО от неавторизированного использования.

Особенности современной реализации технологии HASP

Технология *HASP* (англ. *Hardware Against Software Piracy*) [1] заключается в специальным образом настроенных аппаратных идентификаторов – токенов (*USB*-ключей) или *HASP*-ключей, без применения которых доступ к защищаемому экземпляру ПО или ИС ограничен. Принципиальная особенность *HASP* заключается в реализации основных сервисов безопасности (идентификация и аутентификация, шифрование, разграничение доступа) средствами программного обеспечения (как правило, апплетов) самого *HASP*-ключа (токена).

Технология реализуется следующим образом. Аппаратный токен используется совместно с заранее подготовленными и подключенными библиотеками, которые реализуют определенные разработчиком функции. В них входят такие функции как кодирование, декодирование информации, контроль лицензии, контрольное суммирование, чтение и запись из памяти ключа, мониторинг работы и в сети и т.д. [2]. Данный способ может быть

ненадежен при наличии известных способов обхода функционала, заложенного в применяемые библиотечные функции, отключение защиты осуществляется сравнительно оперативно.

Для устранения этого недостатка предлагается использовать системные библиотеки и системные вызовы, а именно настроить системные библиотеки таким образом, чтобы при проверке подключения *HASP*-ключа происходило обращение к системной функции из библиотеки. И при несовпадении заранее прописанной идентификационной информации с токена и базы данных, где хранятся разрешенные к использованию ключи, происходило действие, обнаруживающее неавторизированное использование программы [3]. При отсутствии *HASP*-ключа действия модуля защиты программы будет аналогичным.

HASP-ключ выполняет функции аппаратного идентификатора для обеспечения авторизованного использования ПО ИС и средством криптографической защиты информационных ресурсов защищаемой информационной системы для обеспечения защиты данных ресурсов от несанкционированного копирования [4].

Система защиты от неавторизированного использования на основе технологии HASP

Программная часть системы защиты состоит из модулей (подсистем), каждый из которых несет свою функциональную нагрузку. Состав системы следующий:

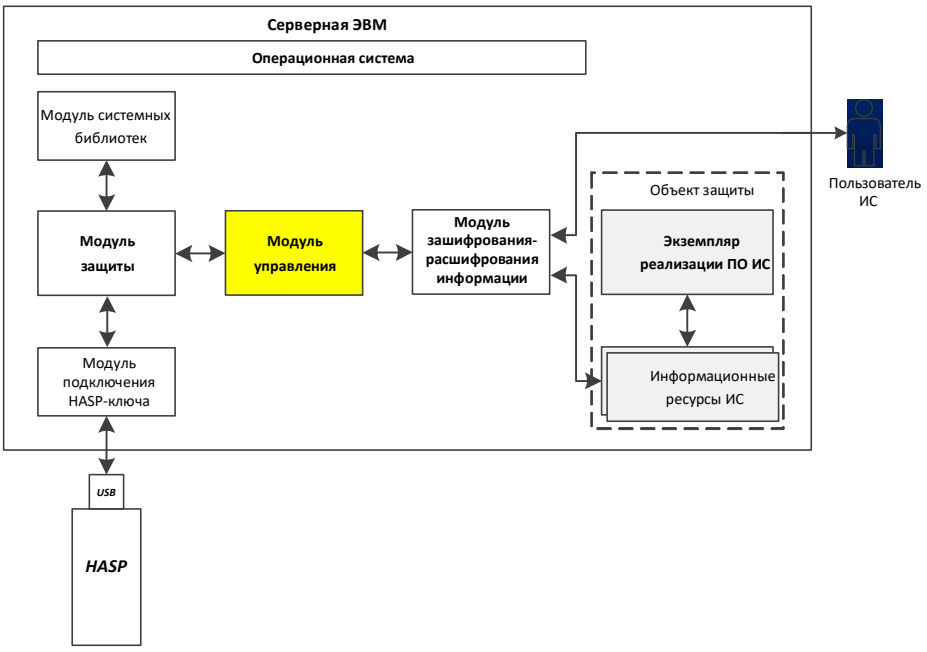


Рисунок. Система защиты от неавторизированного использования на основе технологии HASP

Модуль управления.
Модуль защиты.
Модуль системных библиотек.
Модуль подключения *HASP*-ключа.
Модуль зашифрования-расшифрования информации.
Структурная схема системы показана на рисунке (см. выше).

Модуль управления

Главная задача данной части программы- обеспечение доступа к ИС, контроль взаимодействия пользователя и программы, а также периодическое соединение с модулем защиты ИС для предоставления пользования системой только для авторизированных пользователей. Также одной из функций данного модуля является корректная подача команд на расшифрования и зашифрование информации на соответствующем модуле.

Модуль защиты

Главная часть ПО, следит за подключениями к *USB*-порту, сравнивает идентификационную информацию на токене с базой данных(БД), хранит значение установления соединения с *HASP*-ключом, взаимодействует с стандартными библиотеками, при необходимости использует переменную окружения *LD_PRELOAD* для загрузки измененной библиотеки до загрузки остальных.

Модуль системных библиотек

Хранит измененную библиотеку, где заранее условлен порядок действий при неавторизированном использовании ПО, путем перехвата системного вызова.

В основе перехвата системных вызовов для разных операционных систем могут использоваться такие функции как *SetWindowsHook* – для ОС семейства *Windows* либо специальный параметр вызова программ *LD_PRELOAD* – для ОС семейства *UNIX*.

Модуль подключения HASP-ключа

Сканирует порты на наличие подключенных устройств, считывает с них информацию, которую затем передает модулю защиты. Также для временного хранения состояния токена примеряется переменная, которая по таймеру запрашивает, произведено ли подключение. Это позволяет экономить ресурсы системы и сокращать по времени процедуру проверки подключения *HASP*-ключа.

Модуль зашифрования-расшифрования информации

Для обеспечения защиты от копирования информация в БД информационной системы хранится в зашифрованном виде. Для ее получения пользователю необходимо предъявить токен, пройти процесс идентификации, аутентификации и авторизации и на ключе, записанном внутри *HASP*-устройства, расшифровать информацию из БД. Необходимо обратить внимание, что процесс зашифрования и расшифрования информации происходит на самом *HASP*. Это сделано с целью недопущения передачи секретной последовательности в ПО. Модуль зависит от модуля защиты и модуля управления ИС, а также предоставляет доступ к базе данных.

Выводы

Хранение информации в БД в открытом виде и ПО в форме исходных текстов позволяют предоставлять доступ к информационным системам лицам, не имеющим на это право. Для сохранения авторских прав необходимо использовать специально подобранную и правильно настроенную систему их защиты. Одной из наиболее эффективных технологий защиты от несанкционированного использования в настоящее время является технология *HASP*.

Таким образом, в защите ИС и ПО от несанкционированного копирования и неавторизированного использования, существует множество направлений, которые необходимо учитывать специалисту по информационной безопасности для обеспечения комплексной и оптимальной защиты.

Список используемых источников

1. Ананченко И. В., Мусаев А. А. Защита приложений, выполняемых торговым терминалом Metatrader, ключами Sentinel HASP // Труды СПИИРАН. 2013. № 3 (26). С. 69–78.

2. Жданова И. В., Быков Д. В. Варианты построения системы защиты электронных документов от копирования // Инженерный вестник Дона. 2012. № 8 (68). С. 490–492.

3. Маркин Д. О., Звягинцев С. А., Павлов Д. И. Методы и средства анализа программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании: VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. Санкт-Петербург: СПбГУТ, 2019. Т. 2. 603 с. С. 293–298.

4. Федорук И. В., Миловзорова Ю. С. Защита авторских прав на компьютерную программу: от законодательства к использованию технических средств // Сборник работ 69-й научной конференции студентов и аспирантов Белорусского государственного университета, 14–17 мая 2012 г., Минск. В 3 ч. Ч. 2. Минск, 2013. С. 374–377.

УДК 004.05
ГРНТИ 20.15.05

АНАЛИЗ ПРИМЕНЕНИЯ СИСТЕМ ОБРАБОТКИ ОБРАЩЕНИЙ ГРАЖДАН

Д. С. Медведев, И. В. Пинегина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире важна открытая и оперативная коммуникация между государственными структурами и гражданами. В статье приведено актуальное состояние систем обработки обращений граждан. Выявлены наиболее значительные проблемы процесса цифровизации деятельности учреждений, взаимодействующих с гражданами. Отмечены возможные эффекты внедрения системы обработки обращений. Предложены перспективы развития подобных систем.

система обработки обращений, граждане, государственные структуры, цифровизация.

Налаживание эффективных механизмов взаимодействия органов власти и населения на государственном и на местном уровнях оказалось одной из ключевых задач текущего дня. Взаимодействие государства и населения – понятие весьма широкое и многогранное. Если гражданин решает вступить во взаимоотношения с одним из институтов государства, он, в действительности, включается в контакт, непосредственно, с самим государством.

Для адаптации этого взаимодействия – государство начало переход от «электронного правительства» к «цифровому правительству». Переход осуществляется от технологий для поддержания процессов в органах власти к применению инструментов для создания ощутимого результата государственного управления. В предложенных условиях формируется «единое окно», по которому планируется поступление обращений граждан. Цифровое правительство выступит связующим звеном в этой цепочке. Реализация основных мероприятий по цифровизации государственного управления сформулирована в рамках федерального проекта «Цифровое государственное управление» [1]. Главной целью этого проекта является: интегрирование платформенных решений и цифровых технологий в сферах оказания государственных услуг и государственного управления, в том числе, в интересах людей и субъектов малого и среднего предпринимательства.

Все эти изменения идут на упрощение коммуникации между гражданами и государством. Одной из весомых проблем в этом симбиозе можно

указать то, что некоторая часть населения России придерживается достаточно консервативных взглядов, и люди не склонны к освоению новых знаний и технологий ввиду различных причин. Тем не менее, текущая эпидемиологическая ситуация вынуждает граждан чаще использовать информационные системы для решения повседневных задач. На сегодняшний момент сервисом «ГосУслуги» пользуется свыше 90 млн пользователей [2]. Доля граждан от общей численности населения РФ, пользующихся порталом «ГосУслуги» в процентном соотношении по годам представлена на рис. 1.

Рис. 1. Процент граждан, пользующихся порталом «ГосУслуги»

Появляется огромное количество сервисов, позволяющих гражданам Российской Федерации сообщать об окружающих их проблемах [3]. Зачастую смежные программные реализации сопровождаются сложной архитектурой построения сервисов и неинтуитивным интерфейсом пользователей.

Рассмотрим город Санкт-Петербург, в нём реализованы проекты «Наш Санкт-Петербург» [4] и «Решаем вместе» [5], которые направлены на оперативное взаимодействие жителей города с представителями органов власти Санкт-Петербурга. Системы включают в себя: вход в учетную запись, статистику проблем по каждому району, добавление нового сообщения о проблеме и общую базу сообщений всех пользователей. Интерфейсы систем представлен на рис. 2, 3.

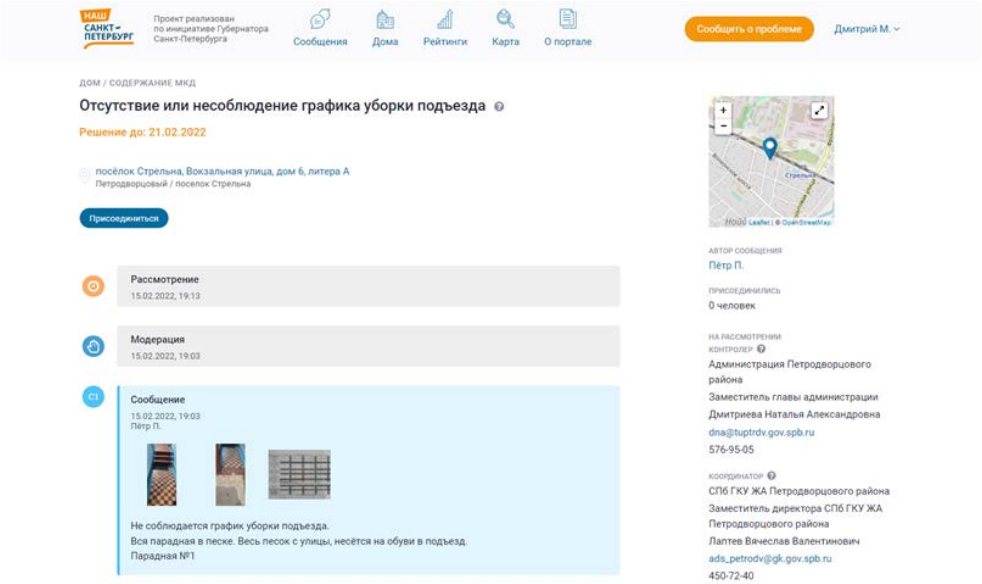


Рис. 2. Интерфейс системы «Наш Санкт-Петербург»

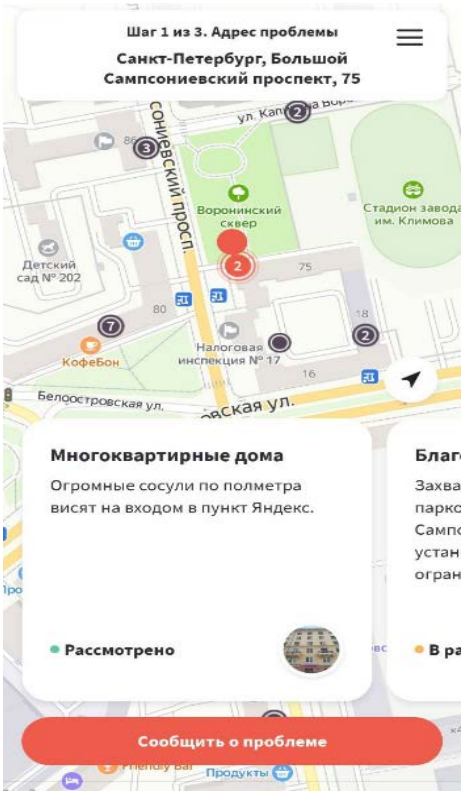


Рис. 3. Интерфейс системы «Решаем вместе»

При добавлении нового обращения предлагается выбрать категорию, указать место и подробно описать волнующий аспект, после чего можно увидеть сроки выполнения, человека, курирующего этот процесс, и инстанцию, исполняющую заявку по этой проблеме. Все обращения, которые поступают, можно увидеть на интерактивной карте с возможностью детального рассмотрения. Ежедневно публикуется огромное количество новых проблем, что подтверждает актуальность данных систем. Как правило, они носят бытовой характер, но встречаются и более крупные проблемы. Типовой процесс организации обработки обращений граждан представлен на рис. 4.

Рис. 4. Типовой процесс организации обработки обращений граждан

Выявлены следующие недостатки рассмотренных систем:

– работа выполняется не в полном объёме (для отчётности);

– отсутствует возможность оценить проделанную работу с комментариями;

– отсутствует функционал для анонимной отправки сообщений;

– отсутствуют некоторые категории проблем, в связи с чем многие обращения отклоняются;

– шаблонные ответы на обращения без возможности продолжить диалог;

– срок обработки сообщений может достигать 30 дней.

Предложены возможные улучшения:

– расширить функционал операторов с возможностью корректировки категорий обращений на валидные;

– добавить возможность создания новых категорий;

– расширить штат операторов и закрепить их за районами, в которых они проживают для действительного понимания о проблемах на рабочей территории;

– ввести категорию предложений и идей;

– добавить возможность коллективных сообщений и кооперации жителей по решению проблем.

Современным системам обработки обращений граждан необходимы существенная доработка и более комплексный подход к решению проблем. Людям сложно перестроиться на новый формат взаимодействия. Для эффективного перехода на цифровую платформу государственного управления целесообразен системный подход по каждому направлению цифрового правительства, включая внесение изменений в административные внутриведомственные процессы, обновление законодательного поля, повышение компьютерной грамотности и адаптивной подготовки граждан к переходу.

Большая часть публичных услуг уже переведена в цифровой формат. Нужна поддержка государства для тех, кто не имеет возможности получить доступ к цифровым сервисам и создавать новые каналы связи, с помощью которых каждый сможет оперативно решить свою проблему.

Список используемых источников

1. Национальная программа «Цифровая экономика Российской Федерации» от 28 июля 2017 г. № 1632-р // Сайт Правительства Российской Федерации. URL: http://government.ru/docs/28653/ (дата обращения: 26.01.2022).

2. ГосУслуги // Портал государственных услуг Российской Федерации. URL: https://www.gosuslugi.ru/ (дата обращения: 01.02.2022).

3. Дрожжинов В. И. Построение информационных систем, обеспечивающих соответствие требованиям федеральных законов России о доступе граждан к информации о деятельности государственных органов и органов местного самоуправления и о персональных данных. М. : Федеральное агентство по информационным технологиям, 2009. 191с.

4. Наш Санкт-Петербург // Система обработки обращений граждан в городе Санкт-Петербург. URL: https://gorod.gov.spb.ru/ (дата обращения: 03.02.2022).

5. ГосУслуги. Решаем вместе // Система обработки обращений граждан в городе Санкт-Петербург. URL: https://pos.gosuslugi.ru/form/ (дата обращения: 03.02.2022).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.657
ГРНТИ 47.63.29

ИСПОЛЬЗОВАНИЕ СЕМАНТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ СОСТАВЛЕНИЯ ТЕХНИЧЕСКОГО ЗАДАНИЯ К РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Г. А. Михаль, Г. Н. Смородин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проведен краткий анализ подходов к составлению технического задания и подготовке документации для разработки программного обеспечения. Представлены преимущества семантического подхода к формированию требований для стадии эскизного проектирования и составления технического задания. Приведён пример применения семантической модели на первых стадиях жизненного цикла проекта разработки приложения.

эскизное моделирование, семантическая модель, формализация технического задания.

В век информационных технологий разработка программного обеспечения (ПО) является одной из важнейших и передовых областей инженерной мысли. Для создания качественного ПО необходим тщательный предварительный анализ предметной области и подробное документирование и описание всех процессов, элементов, закономерностей, входящих в данную предметную область. Некачественно составленное техническое задание (ТЗ) может образовать противоречивую картину у разработчиков о разрабатываемой ими системе, затормозить процесс разработки, и привести к фатальным ошибкам.

В ходе работы над статьёй были проанализированы основные существующие стандарты и методологии где упоминается ТЗ программного обеспечения: ГОСТ 34, ГОСТ 19, IEEE STD 830-1998, ISO/IEC/ IEEE 29148-2011, RUP, SWEBOK, BABOK. Как правило каждый из этих стандартов включает в себя следующие разделы: Назначение, термины и определения, ссылки, функциональные требования, требования к программно-техническим средствам, требования к графическому интерфейсу, обзор вариантов использования [1].

Техническое задание – это документ, в основе которого лежат требования, сформулированные на понятном (обычном, привычном) для Заказчика языке. При этом может и должна использоваться отраслевая терминология, понятная Заказчику [2].

Разработка ТЗ чаще всего происходит в виде поэтапного накопления информации о системе и бизнес-процессах, которые она обслуживает. Сущности тщательно описываются в рамках задач конкретного раздела, над которым происходит работа. Разделы между собой связаны лишь формально, в рамках предметной области, которую они описывают. Такой подход может привести к тому, что информация в последних разделах ТЗ может вступать в противоречие с информацией, описанной ранее. Также возможны последующие корректировки ТЗ, которые могут только усилить противоречия. Такой подход не позволяет выявить как существующие, так и возможные противоречия описываемых объектов и процессов на этапе определения бизнес требований [3]. Для повышения объективности положений ТЗ требуется формализация его содержания, при этом одним из возможных подходов может быть семантическое моделирование.

Использование семантической модели (СМ) для составления ТЗ поможет качественно структурировать информацию, формализовать этап документирования процессов и явлений, выявить неочевидные зависимости между элементами разрабатываемой системы, подготовить базу знаний для документирования и использования на более поздних этапах разработки [4].

Использование СМ при составлении документации заставляет разработчика ТЗ придерживаться определённых правил и порядка действий, что

в свою очередь позволяет провести более подробное описание документируемых процессов и явлений.

Существует несколько способов представления СМ: графическое представление, математическая запись, лингвистическая запись. В данной работе будут использоваться лингвистическая запись и графическое представление. Данные формы представления позволят эффективно использовать собранную информацию, быстро ориентироваться среди разделов и понятий ТЗ. Тип отношений данной СМ является неоднородным, так как элементы, представленные в ТЗ имеют различные взаимные отношения. При использовании в ТЗ *N* различных сущностей (элементов), каждый элемент может обладать *N-1* связями с другими элементами.

Главной сущностью разрабатываемой информационной системы (ИС) или программного обеспечения является сама ее программная реализация (приложение). Перед разработкой архитектор системы должен выявить основные задачи, которые будет решать разрабатываемое ПО. Приложение, как правило, ориентировано на решение ряда задач и связано с каждой из них отношением «предназначено для».

ИС имеет требования к технологической платформе, на которой будет развёрнута

Приложение и технические требования связаны отношением «требуется». В ТЗ могут указываться ссылки на различные источники информации, связанные с разрабатываемой системой или её предметной областью, приложение и ссылки связаны отношением «ссылается на».

Любая система состоит из различных функциональных модулей, в каждом из которых реализована значительная часть функционала, отражающего определённую область в бизнес процессах, каждый модуль имеет своё графическое представление в системе в виде набора различных графических элементов.

Каждый графический элемент необходим для решения определённой поставленной задачи. Семантических подход позволяет формализовать действия разработчика, ориентируя его для достижения цели на совершения ряда простейших операций с определённым графическими элементами.

ТЗ включает ряд определений в рамках предметной области, которые способствуют более глубокому пониманию описываемого объекта.

Каждый модуль имеет различные ограничения на использования определённого функционала для конкретной группы лиц объединённой одной ролью. Каждая роль характеризует возможности использования различных инструментов системы для пользователя. Пример реализации технического задания с использованием семантической сети приведен на рисунке.

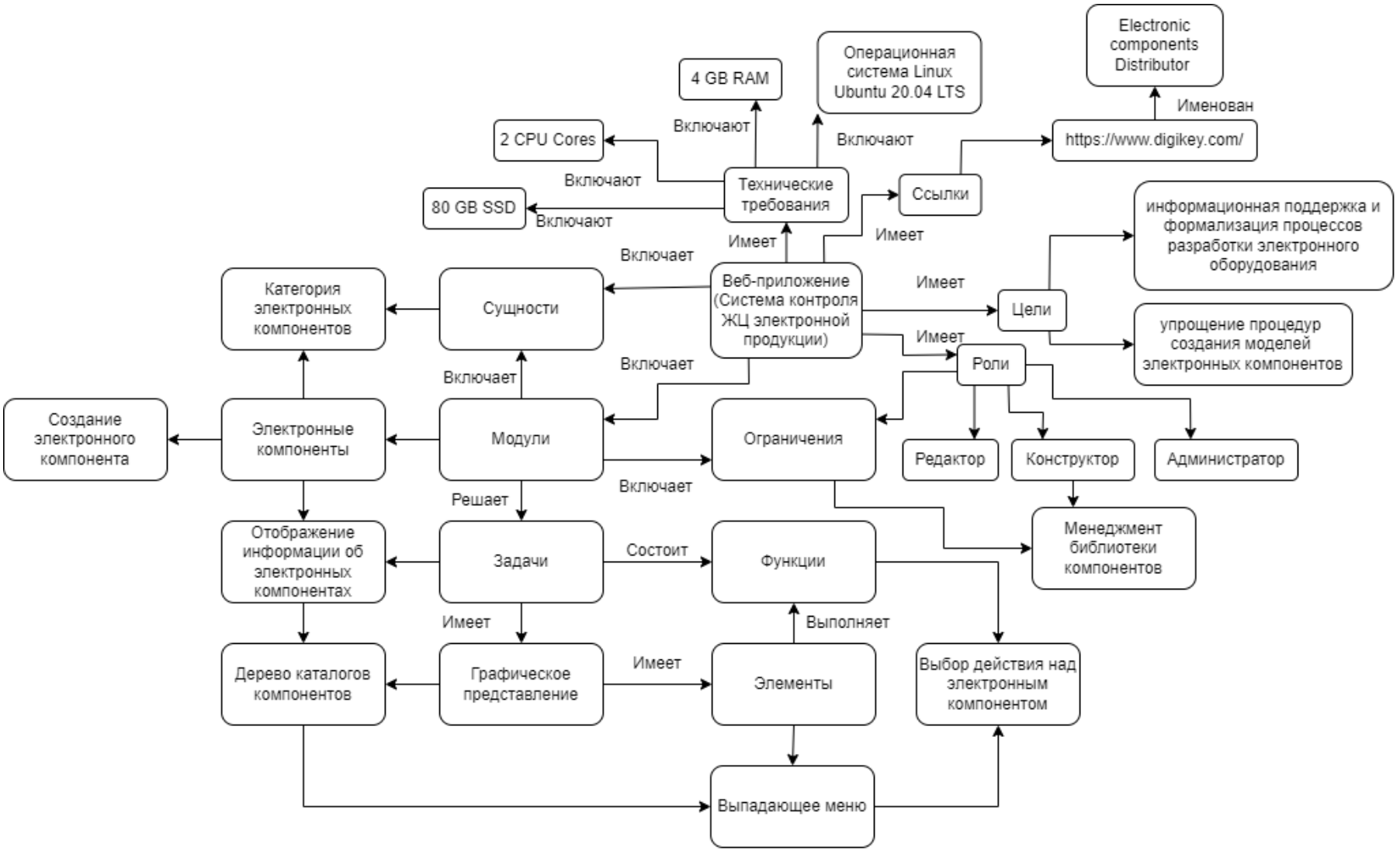


Рисунок. Пример семантической сети технического задания

Дальнейшая детализация технического задания требует формирования семантического словаря – тезауруса предметной области и использования профессиональных инструментов семантического моделирования.

Таким образом, семантическая модель позволяет представить последовательную формализацию требований к разрабатываемой информационной системе. Данный подход в целом должен способствовать повышению объективности положений технического задания и тем самым снизить риски появления погрешностей и ошибок, выявляемых на последующих фазах жизненного цикла разработки программных систем.

Список используемых источников

1. ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению.
2. Макконнелл С. Совершённый код. Санкт-Петербург: Русская редакция/БХВ, 2017. 896 с.
3. Ми Р., Фаулер М., Райс Д., Фоммел М., Хайет Э., Стаффорд Р. Шаблоны корпоративных приложений. М.: Диалектика, 2018. 544 с.
4. Горшков С. Введение в онтологическое моделирование. 2016. URL: https://trinidata.ru/files/SemanticIntro.pdf

УДК 004.514
ГРНТИ 50.41.29

КРИТЕРИИ МАРКЕРОВ КАЧЕСТВЕННОГО РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Т. В. Мусаева, А. В. Ураго

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При построении сцен в дополненной реальности на мобильных устройствах, основным средством получения данных об окружающем мире является оптическое распознавание ключевых объектов реального мира через основную камеру устройства. Одним из наиболее распространённых способов определения ключевых точек в пространстве является использование маркеров-изображений. От скорости и качества распознавания данных маркеров зависит качество проецируемой дополненной реальности на экране мобильного устройства. Целью данной работы является определение ключевых критериев изображений-маркеров, влияющих на скорость и качество распознавания в среде дополненной реальности на примере программной библиотеки Vuforia.

дополненная реальность, маркеры, пользовательский интерфейс, Vuforia, визуализация.

На сегодняшний день активно развиваются и продвигаются технологии дополненной реальности в различных сферах. Это могут быть полноценные очкои, способные отслеживать окружение и точно позиционировать компоненты дополненной реальности в реальном пространстве с использованием специализированных сенсоров, также, как и бюджетные решения, использующие мобильные устройства с камерой и технологии компьютерного зрения для распознавания окружения.

Современные технологии уже позволяют внедрить технологии дополненной реальности в современные интерфейсы [1]. Это позволит разнообразить инструментарий при создании интерфейса, а также дополнить системы уникальными интерактивными компонентами, способными взаимодействовать с реальным миром. Данные средства могут значительно повысить гибкость и функциональность создаваемых пользовательских интерфейсов.

Учитывая наибольшую распространённость и массовость носимых мобильных устройств, применение технологий дополненной реальности на их основе наиболее удобно ввиду большего охвата доступной технической базы и большей привычности для конечного пользователя. Но основной проблемой при внедрении на их основе может оказаться невысокая устойчивость работы дополненной реальности, даже при использовании маркерного позиционирования [2].

В данной статье планируется выявить основные критерии, влияющие на качество позиционирования дополненной реальности при использовании маркерного позиционирования.

В качестве маркеров будут рассматриваться плоские изображения.

Данный подход является классическим для реализации дополненной реальности на мобильных устройствах на основе маркерного позиционирования [3].

Предлагается исследовать критерии эффективности распознавания визуальных маркеров на примере библиотеки дополненной реальности Vuforia.

Принцип идентификации визуальных маркеров данной библиотеки определяется на основе поиска ключевых точек, привязанных к уникальному рисунку изображения (рис. 1) [4].

На основе уникальности расположения облака точек идентифицируется визуальная мишень и определяется его положение в пространстве, а именно положение в трёхмерной системе координат, а также поворот по трём основным осям.

В общем случае, чем больше найдено ключевых точек, и чем более уникально они расположены, тем проще приложению распознать данный маркер.

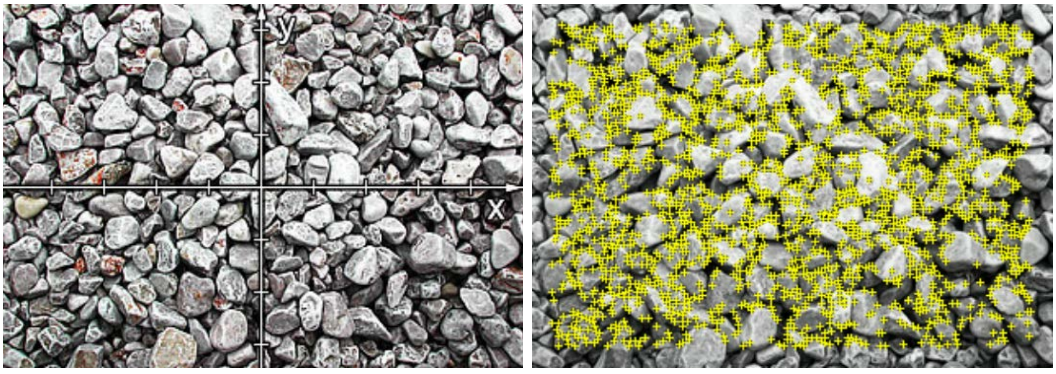


Рис. 1. Изображение маркер и его ключевые точки

Для идентификации ключевых точек в Vuforia используется модификация алгоритма FAST (Featured from Accelerated Segment Test) [5].

Алгоритм FAST нацелен на поиск особых точек на растровом изображении и позволяет детектировать угловые точки.

Работа алгоритма заключается в следующем. При проходе пикселей кандидатов вокруг точек рассматривается окружность из 16 пикселей вокруг точки кандидата P. Точка является угловой если для текущей рассматриваемой точки P существует N смежных пикселей на окружности, интенсивности которых больше интенсивности опорной точки плюс пороговая величина, или интенсивности которых меньше интенсивности опорной точки минус пороговая величина [6].

На начальном этапе сравнивается интенсивность на вертикальных и горизонтальных точках (1, 5, 9, 13) (рис. 2) с интенсивностью в точке P. Если для трёх из четырёх точек выполняется условие превышения или занижения интенсивности выше пороговой величины, то проводится полный обход всех 16 точек. Данный подход позволяет быстрее отсечь ложные точки и повысить производительность.

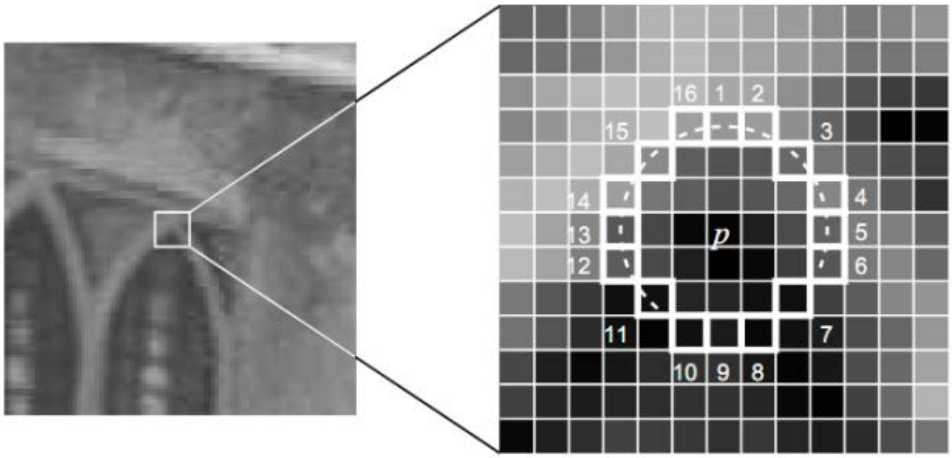


Рис. 2. Определение точки кандидата в алгоритме FAST

В данном алгоритме можно выделить следующие параметры, изменение которых может влиять на результат:

1) Количество N точек на окружности, при котором точка считается угловой;

2) Пороговая величина границы интенсивности.

Интенсивность – это величина насыщенности пикселя в изображении, приведённом к формату градаций серого.

Эксперименты показывают, что наименьшее значение N, при котором особые точки начинают стабильно обнаруживаться равно N = 9.

На основании логики идентификации мишеней по ключевым точкам, и работы алгоритма детектирования точек при распознавании мишеней изображений в библиотеке Vuforia, можно выделить следующие критерии для изображений, которые могут повлиять на скорость и качество распознавания в дополненной реальности:

1) В изображении должно встречаться много углов или областей с большим перепадом контраста;

2) Углы или области большого контраста должны встречаться хаотично и давать уникальное расположение точек;

3) Отсутствие шаблонности, повторяемости или ритмичности узоров на изображении;

4) Стремление к большей контрастности изображения;

5) Контраст по цвету не учитывается, оценивается контраст интенсивности в градациях серого.

На основании выведенных критериев были сформированы следующие тестовые группы изображений для подтверждения гипотез:

1) Изображения с угольными примитивами

2) Изображения с круглыми примитивами

3) Изображения с ритмичными и шаблонными образами

4) Изображения с разными значениями контраста

Тестирование изображений производилось средствами сервиса оценки качества изображений мишеней Vuforia в личном кабинете разработчика в разделе Vuforia Target Manager [7], а также практическими тестами с использованием приложения в дополненной реальности, работающего на библиотеке Vuforia. Тесты проводились с учётом постоянства освещённости в рабочей зоне распознавания. Оценка проводилась в диапазоне от 0 до 5, где 5 – это наилучший результат.

При тестировании групп изображений выводились следующие значения:

1) Количество найденных ключевых точек на каждой тестовой группе изображений,

2) Оценка качества средствами сервиса Vuforia,

3) Оценка качества практическими тестами.

Результаты тестирования представлены в таблицах 1, 2 и 3.

ТАБЛИЦА 1. Результаты тестирования угольных и округлых примитивов

Тип фигур на изображении	Кол-во фигур			Оценка качества (0-5)					
	6	12	45	6 фигур		12 фигуре		45 фигур	
	ключевые точки			Vuforia	тест	Vuforia	Тест	Vuforia	Тест
Треугольники	13	14	72	1	1	1	1	5	5
окружности	21	38	77	1	0	2	1	3	2

ТАБЛИЦА 2. Результат тестирования ритмичных изображений

Тип изображения	Ключевые точки	Оценка качества (0-5)	
		Vuforia	тест
ритмичные фигуры	316	0	0
ритмичные образы с уникальными деталями	326	5	2

ТАБЛИЦА 3. Результат тестирования изображения с разным контрастом

Тип изображения	Ключевые точки	Оценка качества (0-5)	
		Vuforia	Тест
изображение с низким контрастом	120	3	3
контрастное изображение	480	5	5

Стоит обратить внимание на результаты группы изображений с окружностями. В данном тесте было обнаружено большее число ключевых точек чем при тесте с треугольными композициями. Это может быть связано особенностями работы алгоритма Vuforia. При этом не смотря на количество точек, общее качество распознавания как в теоретических, так и в практических тестах оказывается значительно хуже, чем в группе с треугольными композициями, что подтверждает изначальную гипотезу.

По полученным результатам видно, что выведенные гипотезы подтверждаются на практике. Алгоритм с большей точностью распознаёт композиции, имеющие чётко выраженные углы, количество углов напрямую влияет на качество распознавания. В тесте с ритмичными формами, не смотря на большое число найденных ключевых точек, общее качество распознавания оказалось неудовлетворительным как в теоретических, так и в практических тестах. Увеличение числа уникальных деталей в повторяющихся фигурах повышает точность распознавания, но на практических тестах результат оказался всё ещё неудовлетворительным. При тестировании контраста, использовалось одно и то же изображение, но с разным контрастом. В результате при низком контрасте число зафиксированных ключевых точек было закономерно ниже, также пропорционально падало качество распознавания.

Полученные результаты показывают, что выведенные критерии для изображений-маркеров являются верными, обосновываются особенностями работы алгоритмов распознавания изображений в библиотеке дополненной реальности Vuforia, а также доказываются практическими тестами.

Соблюдение выведенных критериев позволит повысить качество работы приложений дополненной реальности, использующие библиотеку Vuforia, повысить точность позиционирования дополненной реальности, а также снизить эффект «дрожания» картинки, что положительно скажется удобстве и пользовательском опыте. Это также позволит открыть возможность внедрения дополненной реальности в сферы технического проектирования и производственные системы [8].

Список использованных источников

1. Славин О. А., Гринь Е. С. Обзор технологий виртуальной и дополненной реальности // Труды института системного анализа Российской академии наук. 2019. Т. 69. № 3. С. 42–54.

2. Аблякимова А. Н., Абляев М. Р. Критерии оценки качества приложений с дополненной реальностью // Информационно-компьютерные технологии в экономике, образовании и социальной сфере. 2020. № 1 (27). С. 129–138.

3. Yunqiang C. An overview of augmented reality technology // Journal of Physics: Conference Series. Volume 1237. 2019.

4. Vuforia. Best. Best Practices for Designing and Developing Image-Based Targets. URL: https://library.vuforia.com/features/images/image-targets/best-practices-for-designing-and-developing-image-based-targets.html

5. Rudy S., Indra R. Augmented reality using features accelerated segment test for property catalogue // TELKOMNIKA Telecommunication, Computing, Electronics and Control. Vol. 18, No. 1. 2020. pp. 140–147.

6. OpenCV. FAST Algorithm for Corner Detection. URL: https://docs.opencv.org/3.4/df/d0c/tutorial_py_fast.html

7. Vuforia Target Manager. URL: https://library.vuforia.com/articles/Training/Getting-Started-with-the-Vuforia-Target-Manager.html

8. Муссаева Т. В., Ураго А. В. Дополненная реальность в проведении занятий по инженерным техническим дисциплинам проектирования // Геометрия и Графика. 2021. Том 9, № 2. С. 46–55.

УДК 528;004.9
ГРНТИ 20.23.27

ГЕОИНФОРМАЦИОННОЕ УПРАВЛЕНИЕ РИСКАМИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ РАЙОНОВ В РЕСПУБЛИКЕ БУРУНДИ

Ндикумана Элиас

Российский государственный гидрометеорологический университет

Данная работа посвящена проблемам, с которыми сталкивается сельскохозяйственный сектор в Бурунди. Также в ней будут проанализированы возможные решения для снижения воздействия, преследующего этот сектор, с целью увеличения национальной экономики, которая почти полностью основана на сельскохозяйственном секторе.

геоинформатика, разработка геоинформационную систему управления рисками сельскохозяйственных районов в Республике Бурунди.

Бурунди – это государство в Восточной Африке, не имеющее выхода к морю. Государство расположено на плато, спускающемся на юго-западе к озеру Танганьика. Средняя высота плато от 1 525 до 2 000 м. На западе расположена ориентированная по меридиану горная цепь, с наивысшей точкой 2 760 метров. Около озера Танганьика находится и самая низкая точка страны – 772 метра. Озеро Танганьика и впадающая в него пограничная река Рузизи лежат на расширяющейся к северу равнине с плодородными почвами. В центре страны и на востоке расположены равнины, окружённые горами и болотами.

Климат Бурунди в основном тропический со значительными дневными амплитудами температур, которые значительно варьируются в зависимости от высоты рельефа. Осадки очень нерегулярны и максимальны на северо-западе страны. Выделяются четыре сезона в зависимости от выпадения осадков:

- длинный сухой сезон (июнь – август),
- короткий влажный сезон (сентябрь – ноябрь),
- короткий сухой сезон (декабрь – январь),
- длинный влажный сезон (февраль – май).

По данным Межправительственной группы экспертов по изменению климата [1] изменение климата в целом негативно повлияет на сельское хозяйство, лесоводство и рыболовство в большинстве районов Бурунди. Согласно данным метеорологических наблюдений в последние десятилетия

в Бурунди наблюдается частое изменение погоды, особенно во время длительного влажного сезона и в начале сухого сезона. Результатом этого являются наводнения в разных частях страны, что плохо сказывается на сельском хозяйстве, на уровне жизни населения, а, следовательно, и на уровне развития страны. В связи с этим, возникает необходимость разработки геоинформационную систему управления рисками сельскохозяйственных районов в Республике Бурунди.

Население Бурунди преимущественно сельское и получает средства к существованию от сельского хозяйства. Однако на сельскохозяйственный сектор приходится менее половины годового богатства страны (ВВП). Это связано с низкой продуктивностью сельского хозяйства в результате деградации почв, неправильных методов ведения сельского хозяйства и, прежде всего, климатических угроз (повышение температуры, снижение доступности воды, внезапное изменение количества, выпавших осадков и внезапное появление отсутствия ливневых осадков во времени сезона дожди, наводнения, а также потеря биоразнообразия и деградация экосистем).

В Бурунди сельскохозяйственный сектор является основанием роста национальной экономики. Она является гарантом продовольственной безопасности населения. По данным Министерства сельского хозяйства, сельским хозяйством традиционно и занимаются около 90% населения на очень маленьких фермах (в среднем 0,5 га на домохозяйство).

Сельское хозяйство Бурунди остается очень уязвимым к климатическим угрозам. Показательным примером является феномен Эль-Ниньо 2017 года. Было уничтожено около 30 000 гектаров фермерских хозяйств. В результате по всей стране возник дефицит продовольствия, что привело к экспоненциальному росту цен на продукты питания на рынке. В 2017 году уровень инфляции достиг 16 %. [1]

Уязвимость к изменению климата – это степень, в которой системы (регионы, население, экосистемы и т. д.) подвержены влиянию последствий изменения климата. Это функция как воздействия, которому подвергается рассматриваемая система, так и чувствительности этой системы и ее способности к адаптации:

•Воздействие – это скорость и величина изменчивости и изменения климата (например, изменение температуры/осадков, появление града/ливней/штормов и т. д.). Поэтому оценка воздействия включает в себя оценку масштабов изменчивости климата, с которой столкнется данная территория, а также вероятности возникновения такой изменчивости климата.

•Чувствительность к изменению климата – это степень, в которой система, подверженная изменению климата, вероятно, будет затронута положительно или отрицательно в результате этого изменения. Он описывает природную или физическую среду территории и зависит от множества па-

раметров, таких как плотность населения, демографический профиль, землепользование, развитие территории и т. д. Подверженность и чувствительность - это потенциальное воздействие изменения климата, которое происходит независимо от способности местного населения адаптироваться к последствиям.

•Адаптация к изменению климата будет заключаться в снижении чувствительности системы и, следовательно, уменьшении ее уязвимости. Он описывает социальную среду системы, такую как финансовые ресурсы людей, доступ к технологии и информации, доступ к институтам и группам, местные знания и т.д., которые позволяют ей адаптироваться [1, 2].

Основные вредные воздействия сельскохозяйственного сектора включают эрозию почвы, паводки. Они формируют общее потенциальное воздействие на сектор, которое происходит в случае отсутствия способности к адаптации: изменение сельскохозяйственного производства [2, 3].

Для увеличения сельскохозяйственного производства и смягчения дефицита продовольствия, вызванного стихийными бедствиями (наводнениями, непогодой, пожарами в кустарниках, эрозией, градом), необходимо использовать новые технологии, учитывающие географические данные в поиске рационального решения, способного предсказать риски стихийных бедствий и обеспечить принятие решений.

В сельскохозяйственной области географические информационные системы интересны тем, что почвенные переменные могут быть пространственно представлены с помощью различных методов интерполяции. Их преимущество заключается в пространственном расположении данных на картографической основе с привязкой к местности. Фермер, хорошо информированный о содержании компонентов в своей почве, может наметить участки для обработки с помощью GPS. Это будет огромным преимуществом, поскольку он будет инвестировать только в точные места; последствия: экономия времени, снижение затрат, сохранение окружающей среды от загрязняющих веществ и т. д. [4].

Сельское хозяйство с использованием ГИС может позволить:

– адаптация методов ведения сельского хозяйства к неоднородным характеристикам участка (обработка почвы, орошение, посев);

– точное нацеливание на обрабатываемые участки;

– -лучшее управление производственными затратами (удобрения, семена, фунгициды, гербициды и т.д.);

– ограничение вымывания избытка удобрений в грунт;

– принятие решений по борьбе со стихийными бедствиями;

– повышение урожайности в сельскохозяйственном секторе.

Заключение

Для устранения рисков, преследующих сельскохозяйственный сектор, необходимо:

- Внедрить географическую информационную систему, учитывающую рельеф Бурунди и позволяющую визуализировать влияние всех факторов, связанных с изменением климата, на сельское хозяйство.
- Разработать модель, способную прогнозировать риски, которые могут вызвать проблемы для сельскохозяйственной отрасли.
- Принимая во внимание прогноз риска, необходимо принять меры по снижению потерь.

Список используемых источников

1. Dr. Stefan Liersch, Rocio Rivas, Kerstin Fritzsche. Rapport sur le changement climatique au Burundi. URL: https://www.adelphi.de/de/system/files/ mediathek/bilder/changement_climatique_au_burundi_r%C3%A9sum%C3%A9_fr_1.pdf (дата обращения: 03.03.2022).

2. Вагизов М. Р., Истомин Е. П., Колобин О. Н., Присяжнюк С. П., Соколов А. Г., Яготинцева Н. В. Введение в геоинформационное управление // Геоинформатика. № 3. 2021. С.4–11.

3. Соколов А.Г ., Истомин Е. П., Кирсанов С. А., Колбина О. Н. Феномен геоинформационного управления и принципы его реализации // Вестник СП6ГУ. Серия 7. Геология. География. СПОГУ, 2014. № 4. С.180–182.

4. Соколов А. Г., Истомин Е.П., Слесарева Л. С., Зоринова Е. М., Геоинформационные аспекты управления рисками устойчивого развития приморской рекреационной территории // Известия ЮФУ. Технические науки. 2013. № 9. С. 233–239.

Статья представлена научным руководителем,
доктором технических наук, профессором Е. П. Истоминым.

УДК 608.3
ГРНТИ 50.49.02; 50.49.29; 50.43.31

АНАЛИЗ УРОВНЯ ТЕХНИЧЕСКИХ РЕШЕНИЙ ДЛЯ СИТУАЦИОННЫХ ЦЕНТРОВ

А. А. Нестеров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На основе анализа информационного потока патентных документов Российской Федерации и программного обеспечения, включенного в Единый реестр российских программ для электронных вычислительных машин и баз данных, рассмотрены основные технические решения для ситуационных центров различного уровня и назначения. Представлена динамика активности регистрации объектов интеллектуальной собственности, а также проведена оценка уровня технических решений. Выявлены основные направления развития технических решений для функциональных задач системы поддержки принятия решений широкого класса.

ситуационный центр; технический уровень; поддержка принятия решений.

Одним из важнейших элементов в системах управления различного уровня являются ситуационные центры. В [1] используется следующее определение ситуационного центра: это совокупность программно-технических средств, научно-математических методов и инженерных решений для автоматизации процессов отображения, моделирования, анализа ситуаций и управления. При этом в [2] ситуационный центр по своему назначению определяется как организационно-технический комплекс, предназначенный для информационно-аналитического обеспечения решения задач управления в органах государственной власти, на крупных предприятиях, в отраслях экономики или при развитии кризисных ситуаций.

Существующие тенденции развития и внедрения информационных и коммуникационных технологий в системе ситуационных центров (СЦ) различного уровня и назначения приводят к росту многообразия системотехнических решений по их построению и проблемам информационно-технического сопряжения при создании единого информационного поля. Несомненно, актуальными являются исследования, направленные на систематический сбор, обработку и анализ уровня технических решений ситуационных центров.

Результаты исследования информационного потока патентных документов Российской Федерации, которые были проведены по базам данных

Роспатента с глубиной в 10 лет, показывают достаточно активную регистрацию технических решений для ситуационных центров, что представлено в таблице 1 и на рис. 1.

ТАБЛИЦА 1. Статистические данные регистрируемых объектов интеллектуальной собственности в сфере ситуационных центров

Наименование объекта	Количество регистрируемых объектов									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Программы для ЭВМ для СЦ	0	15	10	14	16	12	27	13	22	12
Базы данных для ЭВМ для СЦ	0	1	2	1	1	0	0	0	0	0
Изобретения для СЦ	2	0	1	1	0	2	2	0	0	0
Полезные модели	1	3	0	1	3	1	0	0	0	0

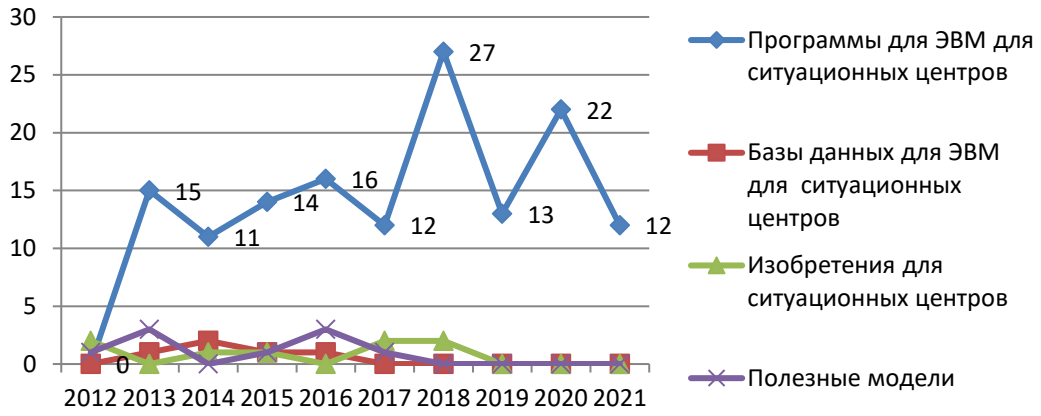


Рис. 1. Статистические данные регистрируемых объектов интеллектуальной собственности в сфере ситуационных центров

Результаты исследования информации, содержащейся в Едином реестре российских программ для электронных вычислительных машин и баз данных, представленные на рисунке 2, показывают значительно меньшие темпы регистрации – с даты его создания 01.01.2016 и по 2021 год включительно в реестр введены всего 16 решений от 14 правообладателей. Это количество сравнимо со среднегодовыми объемами регистрации программ в сфере ситуационных центров для ЭВМ в Роспатенте.

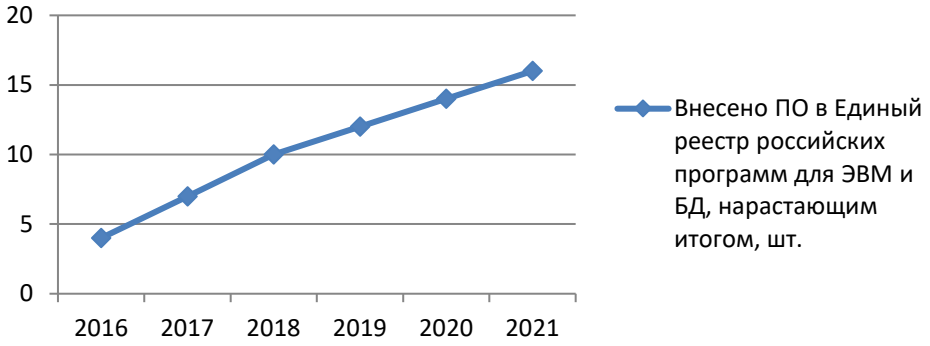


Рис. 2. Данные нарастающим итогом
по программному обеспечению ситуационных центров, внесенные в 2016–2021 годах
в Единый реестр российских программ для ЭВМ и БД

Анализ решений для ситуационных центров, представленных в базах патентных документов Российской Федерации и в Едином реестре российских программ для электронных вычислительных машин и баз данных показывает, что уровень этих решений отличается по многим параметрам и их заявленным функциональным возможностям. В ходе исследования был рассмотрен уровень и направления развития технических решений, которые в наибольшей степени связаны с реализацией функциональных задач систем поддержки принятия решений широкого класса. Из определения СЦ [1] следует, что в нем должен быть реализован функционал автоматизации процессов отображения, моделирования, анализа ситуаций, управления. Однако современные решения, запатентованные в течение трех последних лет (2019–2021) предоставляют пользователям систем гораздо более широкий функционал. Представленные в патентных базах сведения показывают, что чаще всего это возможность использования встроенных подсистем визуализации, прогнозирования, поддержки принятия решений, геоинформационных подсистем (или интеграции с существующими геоинформационными системами), а также возможность использовать решение мобильным пользователям.

Была проведена оценка выявленного множества запатентованных решений с применением положений ГОСТ Р ИСО/МЭК 25010-2015 по модели качества системы/программного продукта. В качестве характеристик, по которым проводилась оценка, были использованы функциональная пригодность (заявлены ли в продукте соответствующие функциональные подхарактеристики) и переносимость (наличие мобильной версии продукта, которая доступна для мобильного телефона и/или планшета). Использованные подхарактеристики, а также результаты оценки, сведены в таблицу 2.

ТАБЛИЦА 2. Оценка регистрируемых объектов интеллектуальной собственности в сфере ситуационных центров по модели качества программного продукта

	Запатентованных решений в 2012–2021 гг.	В том числе запатентованных в 2019–2021 гг.	% запатентованных в 2019–2021 гг. от 2012–2021
всего запатентованных решений	142	47	33,1
в том числе имеющим по параметру «Функциональная пригодность»:			
функционал прогнозирования	29	10	34,5
функционал визуализации	26	16	61,5
функционал поддержки принятия решений	30	13	43,3
интеграцию и/или наличие в функционале модуля геоинформационной подсистемы	10	5	50,0
в том числе имеющим по параметру «Переносимость»:			
наличие мобильной версии	13	9	69,2

Заявляемые возможности патентуемых в последние годы объектов, как правило, превышают те минимальные требования, которые считаются «классическими» и используются в определении ситуационных центров. Любопытно, что единственным запатентованным решением, в чьем составе оказались все анализируемые параметры, оказалось система [3], дата регистрации которой 08.12.2021 и при этом предыдущая версия этой же программы, зарегистрированная ранее в 2021 году, не имела в своем составе функционала мобильной версии. Очевидно, что технические решения ситуационных центров эволюционируют быстрыми темпами, при выявленных примерно постоянных темпах регистрации патентных документов уровень решений за три последних года вырос. Показателен пример решений с наличием мобильной версии – за последние три года их запатентовано 69% от общего числа. Это говорит о том, что для востребованности в ближайшем будущем решения для СЦ высокого уровня, как правило, должны будут иметь все рассмотренные в данной статье подхарактеристики по модели качества, и более того, в них будут появляться новые возможности (в том числе интеграционные) и функционал.

Список используемых источников

1. Княжев В. Б. и др. Ситуационное управление в деятельности органов внутренних дел: курс лекций. М.: Академия управления МВД России, 2020. 80 с. ISBN 978-5-907187-31-3.

2. Шестаков А. В., Фролова К. А., Плетнев Я. А. Геоинформационные системы в управлении и мониторинге техногенных объектов. Схемы и QR-ссылки: учебное пособие. СПб.: Любавич, 2021. - 100 с. ISBN 978-5-907440-62-3.

3. Удальцов Иван Александрович (RU), Пиманенко Алексей Владимирович (RU), Нечаев Денис Сергеевич (RU), Тябин Илья Витальевич (RU). Название программы для ЭВМ: «Информационно-аналитическая система Ситуационного центра Губернатора Саратовской области, версия 2021».

Статья представлена научным руководителем, доктором технических наук, с.н.с. А. В. Шестаковым.

УДК 004.056
ГРНТИ 81.96.29

СПОСОБЫ ЭКСФИЛЬТРАЦИИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

А. А. Нестерова, А. А. Полков

Академия Федеральной службы охраны Российской Федерации

В работе перечислены основные типы APT-атак и распространенные способы эксфильтрации. Приведена их краткая характеристика и способы защиты, предупреждения и нивелирования последствий атак злоумышленника на автоматизированную систему. Атаки киберпреступников случаются все чаще, и компаниям необходимо прорабатывать систему защиты таким образом, чтобы предотвратить максимальное количество возможных инцидентов.

утечка данных, эксфильтрация данных, защита конфиденциальности, трафик.

Более половины утечек информации имеют случайный характер. Другая половина – это тщательно спланированные махинации киберпреступников, работников организации или ее поставщиков. Все чаще появляются сведения о краже служебной информации, например, в отчете Tadviser [1] за 2022 год приведены данные об утечках информации в госсекторе, медицинских учреждениях, соцсетях. Такие кражи наносят вред не только в масштабах государства, но и гражданам в том числе: утечка данных авиакомпании British Airways, файлы с более чем 8 миллиардами паролей, адреса кошельков, данные домашних маршрутизаторов и IoT-устройств.

Согласно отчету Positive Technologies за 2019 год [2], массовые атаки отошли на второй план, а целенаправленные успешно идут вперед. Основная цель всех киберпреступлений – это кража информации. Потеря такой

информации может принести вред как в финансовом плане, так и конфиденциальности пользователей.

Анализ реально существующих APT-атак позволил компании MITRE составить матрицу тактик, которые киберпреступники применяют для их реализации. Эта матрица называется ATT&CK [3] и состоит из 12 основных тактик, указанных на рис. 1.

Первоначальный доступ в систему (*Initial access*)	Выполнение кода или команды (*Execution*)	Закрепление (*Persistence*)
Повышение привилегий в системе (*Privilege escalation*)	Предотвращение обнаружения средствами защиты (*Defense evasion*)	Получение учетных данных (*Credential access*)
Разведка (*Discovery*)	Перемещение внутри периметра (*Lateral movement*)	Сбор данных (*Collection*)
Управление и контроль (*Command and control*)	Эксфильтрация данных (*Exfiltration*)	Воздействие (*Impact*)

Рис. 1. Матрица тактик APT-атак

Эксфильтрация данных – этап проведения тестирования на проникновение, в котором атакующая сторона пытается осуществить скрытную загрузку файлов из системы за периметр организации, оставаясь не замеченной.

Матрица MITRE ATT&CK выделяет девять техник, которые используют злоумышленники, представленных на рис. 2.

Автоматизированная эксфильтрация	Сжатие данных	Шифрование данных
Ограничение размера передаваемых данных	Эксфильтрация через альтернативный протокол	Эксфильтрация через командный сервер
Эксфильтрация через альтернативный канал связи	Физическая эксфильтрация	Передача по расписанию

Рис. 2. Основные техники эксфильтрации

Автоматизированная эксфильтрация: злоумышленники могут извлекать данные при помощи автоматизированной обработки после их сбора и во время сбора. Собранная информация с помощью автоматизированных сценариев или зеркалирования трафика через скомпрометированную сетевую инфраструктуру передается злоумышленнику.

Дублирование трафика является подвидом автоматизированной эксфильтрации. Злоумышленники могут использовать зеркалирование трафика для автоматизации кражи данных через скомпрометированную сетевую инфраструктуру. Зеркальное отображение трафика является встроенной функцией некоторых сетевых устройств и используется для анализа сети, и может быть настроено для дублирования трафика и пересылки в одно или несколько мест назначения для анализа анализатором сети или другим устройством мониторинга [3].

Ограничения размера передаваемых данных: злоумышленник извлекает данные фрагментами фиксированного размера вместо целых файлов или ограничивает размеры пакетов ниже определенных пороговых значений. Этот подход можно использовать, чтобы избежать срабатывания предупреждений о пороговых значениях передачи данных по сети.

Эксфильтрация через альтернативный протокол: злоумышленники могут украсть данные путем их эксфильтрации по протоколу, отличному от протокола существующего канала управления и контроля. Данные также могут быть отправлены в альтернативное место в сети с главного сервера управления и контроля.

Эксфильтрация по каналу C2. Злоумышленники могут украсть данные, передав их по существующему каналу управления и контроля. Украденные данные кодируются в обычный канал связи с использованием того же протокола, что и для командной и управляющей связи.

Физическая эксфильтрация. Злоумышленники могут попытаться эксфильтровать данные через другую сетевую среду, отличную от канала управления и контроля. Если сеть управления и контроля представляет собой проводное подключение к Интернету, эксфильтрация может происходить, например, через соединение Wi-Fi, модем, сотовое соединение для передачи данных, Bluetooth или другой радиочастотный (РЧ) канал.

Эксфильтрация через физический носитель Злоумышленники могут попытаться эксфильтровать данные через физический носитель, например съемный диск. В определенных обстоятельствах, таких как компрометация сети с воздушным зазором, эксфильтрация может происходить через физический носитель или устройство, введенное пользователем. Таким носителем может быть внешний жесткий диск, USB-накопитель, сотовый телефон, MP3-плеер или другое съемное устройство хранения и обработки. Физический носитель или устройство можно использовать в качестве конечной

точки эксфильтрации или для перехода между другими отключенными системами.

Сжатие данных. Злоумышленники сжимают обнаруженные в компьютерной сети данные перед их передачей, для минимизации трафика, передающегося в сеть. Сжатие происходит либо при помощи специальных программ, либо с использованием утилит, поддерживающих наиболее распространенные форматы сжатия, такие как 7Z, RAR или ZIP [4].

Шифрование данных. Злоумышленник может зашифровать данные перед эксфильтрацией, чтобы избежать защиты, основанной на анализе содержимого файлов или сделать утечку менее очевидной на фоне других сетевых событий. Шифрование файлов, не зависящее от протокола передачи данных, не позволит средствам защиты определять тип передаваемой информации. Использование широко известных форматов архивации с применением шифрования, таких как RAR и ZIP, позволит атакующей стороне замаскировать вывод данных под легитимную передачу сжатых файлов.

Эксфильтрация через командный сервер. Эксфильтрация производится через командный сервер при помощи того же протокола, который применяется для администрирования сбора данных, например через электронную почту или созданные лазейки.

Предотвращение сетевых вторжений на уровне сети осуществляется путем использования системы обнаружения и предотвращения сетевых вторжений, которые по сигнатурам определяют трафик, типичный для ВПО. Сигнатуры являются уникальными для протокола и основываются на определенных методах обфускации, характерных для конкретного злоумышленника или инструмента. Сигнатуры взаимодействия с командным сервером могут меняться, а злоумышленники – изобретать новые способы обмана средств защиты.

Эксфильтрация через альтернативный канал связи. Чтобы украсть данные, злоумышленник может использовать канал, отличный от канала C&C. К примеру, в случае если управление производится через проводное подключение к интернету, проникновение может проводиться через Wi-Fi-сети, модемную, сотовую связь, Bluetooth или радиочастотные каналы. Эти альтернативные каналы будут использоваться, когда они небезопасны или когда уровень безопасности ниже, чем у других каналов в сетевой среде. При использовании таких методов проникновения злоумышленник должен иметь соответствующий доступ к устройствам Wi-Fi или радиопередатчикам.

Запланированная передача. Утечка данных может быть осуществлена в определенное время или через определенные промежутки времени. Этот метод позволяет злоумышленникам скрывать свои действия в контексте стандартных рабочих процессов. К примеру, передача данных осуществляется

только с 10 утра до 15 часов дня по будням. В это время большинство сотрудников используют Интернет для отправки писем и документов через Интернет.

Чтобы обнаружить существование злоумышленника до того, как он нанесет ущерб компании, необходимо постоянно следить за безопасностью инфраструктуры, быстро реагировать на подозрительные инциденты, устанавливать предположения об утечке и проверять их в инфраструктуре. Подозрительными необходимо считать необычные процессы или скрипты, сканирующие файловую систему посредством обращения к каталогам высшего уровня, и отправляющие данные в сеть. Распространенные приложения для шифрования, установленные в системе или загруженные злоумышленниками, можно обнаружить, отслеживая соответствующие процессы и известные аргументы, использующиеся при запуске утилит из командной строки. Для защиты на уровне сети используются системы обнаружения и предотвращения сетевых вторжений, которые по сигнатурам могут определить трафик, типичный для вредоносного программного обеспечения и командного сервера.

Список используемых источников

1. Утечки данных // Ресурс о корпоративной информатизации. Tadviser, 2022. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных (дата обращения: 27.02.2022)

2. Актуальные киберугрозы // Ресурс о разработке инновационных решений в сфере информационной безопасности. Positive Technologies, 2019. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/ (дата обращения: 01.03.2022)

3. Enterprise Matrix // База знаний о тактиках, приемах и методах коберпреступников. Mitre Att&ck, 2021. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 17.02.2022)

4. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: ДИАЛОГ-МИФИ, 2002. 384 с.

УДК 004.56
ГРНТИ 50.43.19

НЕКОТОРЫЕ АСПЕКТЫ ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ ИНФРАСТРУКТУР

С. Б. Ногин

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В статье рассмотрены вопросы организации мониторинга функционирования вычислительных сетей, приведены основные контролируемые параметры мониторинга объектов. Рассмотрены подходы к построению систем мониторинга функционирования вычислительных инфраструктур.

мониторинг функционирования, система мониторинга функционирования, параметры мониторинга.

Качество работы любого комплекса средств автоматизации (КСА) напрямую зависит от скорости, доступности и стабильности работы всех его компонентов. Под КСА понимается совокупность взаимосогласованных компонентов и комплексов программного, технического и информационного обеспечений, разрабатываемая, изготовляемая и поставляемая как продукция производственно-технического назначения, принадлежащая одному объекту и предназначенная для автоматизированного выполнения заданных функций управления на объекте. Как правило, с точки зрения технического обеспечения КСА представляет собой совокупность серверного оборудования, автоматизированных рабочих мест должностных лиц, периферийного оборудования связанных в вычислительную сеть с помощью коммуникационного оборудования.

Мониторинг представляет собой непрерывный процесс сбора, обработки, оценки информации о техническом состоянии отдельных составляющих КСА и КСА в целом и подготовки решений, направленных на обеспечение его корректного функционирования [1].

В узком смысле термином «мониторинг функционирования сети» называют работу системы, которая выполняет постоянное наблюдение за вычислительной сетью в поисках медленных или неисправных систем (элементов) и которая при обнаружении проблем сообщает о них соответствующему должностному лицу с помощью средств оповещения. Эти задачи являются подмножеством задач управления сетью.

В настоящее время мониторинг сети подразделяется на несколько отдельных подсистем, например:

– система обнаружения вторжений;

– система мониторинга производительности сети;

– система поиска проблем, вызванных отказавшими серверами, другими устройствами или сетевыми соединениями.

Мониторинг позволяет выявить потенциальные проблемы на этапе их зарождения и избежать опасных последствий.

Как правило, системы мониторинга строятся по технологии «клиент-сервер».

Система мониторинга функционирования КСА включает в себя:

– сервер мониторинга;

– система управления базами данных и базы данных с информацией, необходимой для обеспечения мониторинга;

– автоматизированное рабочее место администратора системы;

– автоматизированное рабочее место оператора системы;

– клиенты системы мониторинга;

– агенты (программы сбора данных).

К наиболее распространенным методам мониторинга технического состояния КСА обычно относят проверки (тесты), на основании которых получают дифференциальные и комплексные оценки, которые затем закладываются в основу формируемых решений.

Мониторинг производительности осуществляется по следующим ключевым показателям:

– фактическая пропускная способность коммутаторов и маршрутизаторов;

– загруженность памяти и процессоров сетевых устройств;

– периоды непрерывной работы серверов;

– время отклика сервисов и приложений;

– качество сетевых соединений (потери, задержки пакетов и т. д.);

– использование существующего пространства для хранения данных на серверах, дисковых массивах и других накопителях;

– метрики, заданные пользователями.

Для конкретных объектов могут задаваться дополнительные параметры.

Параметры отслеживания при мониторинге сайта: доступность по ICMP; доступность домена; скорость загрузки; нагрузка на сайт (действия на сайте, поиск слова и др.).

Параметры отслеживания при мониторинге серверов: доступность по IP (ping, потери, задержки); службы по портам (RDP, HTTP, FTP и т. д.); службы внутри системы (RDP, HTTP, FTP, сервисы, наличие в логах какого-

то текста, параметры диска, загрузка канала, центрального процессора, оперативного запоминающего устройства).

Мониторинг сетевого оборудования.

Параметры отслеживания при мониторинге сетевого оборудования: доступность по SNMP/ICMP; мониторинг параметров (трафик на порту, BGP сессия, статус порта, нагрузка на центральном процессоре).

Параметры отслеживания при мониторинге источника бесперебойного питания: доступность по протоколу SNMP/ICMP; нагрузка, заряд батарей, напряжение тока и др.

Доступность сервисов при мониторинге вычислительной сети.

Наблюдение сервером баз данных выполняется с целью оценки производительности сервера. Эффективное наблюдение подразумевает регулярное создание моментальных снимков текущей производительности для обнаружения процессов, вызывающих неполадки, и постоянный сбор данных для отслеживания тенденций роста или изменения производительности.

Как правило, производительность сервера и мониторинг активности оценивается либо средствами операционной системы и внешних программ, либо с использованием хранилища запросов или выполнением задач наблюдения с трассировкой SQL (запуск трассировки, фильтрация событий, анализ результатов).

Исходными данными для построения системы мониторинга функционирования КСА являются:

1) Вычислительная инфраструктура, для которой создается система мониторинга;

2) Цели мониторинга функционирования;

3) Объекты мониторинга:

4) Состав КСА (технические и программные средства) [2]: вычислительные средства (оборудование, операционные системы, приложения); коммуникационное оборудование (оборудование коммутаторы, маршрутизаторы), операционные системы маршрутизаторов); системы хранения (накопители на жестких дисках, дисковые массивы, системы хранения, сети хранения); виртуальную инфраструктуру (виртуальные сети, виртуальные машины, используемые операционные системы, приложения);

5) Организация информационного процесса в вычислительной системе;

6) Объем диагностических функций для элементов и их агрегаций;

7) Требуемый объем мониторинга:

8) Объем параметров для диагностики отдельных единиц оборудования;

9) Объем параметров для диагностики групп оборудования;

10) Объем параметров для диагностики комплекса средств автоматизации в целом;

11) Виды технических состояний;

12) Ограничения и границы значений параметров технических состояний компонентов КСА;

13) Методы и алгоритмы получения технических диагнозов и прогнозов.

Возможны два основных варианта построения систем мониторинга функционирования КСА [3]: использование готовых систем мониторинга или разработка новой системы под собственные нужды.

Использование готовых систем мониторинга.

Достоинства:

– система уже разработана, требуется лишь ее установка и настройка;

– вполне развиты средства визуализации технического состояния элементов КСА (как правило, вариант «семафор» - зеленый, желтый, красный);

– имеются развитые средства оповещения о контролируемых событиях.

Недостатки:

– набор контролируемых типовых компонентов КСА как правило задан и нет возможности его изменить;

– набор контролируемых параметров задан, и не всегда имеется возможность ее изменить;

– как правило, отсутствует возможность прогноза развития ситуации при выходе параметров из «зеленой» зоны;

– как правило, отсутствует агрегация контролируемых элементов в функциональные модули;

– как правило не контролируют процесс обработки информации (загруженность серверов, нагрузку на сеть, нагрузку виртуальной инфраструктуры и т. д.);

– имеются ограничения по установке программ-клиентов на контролируемые элементы КСА.

Разработка новой системы мониторинга.

Достоинства:

– набор контролируемых типовых компонентов КСА полностью соответствует целям мониторинга, включая вертикальную схему агрегации элементов (по результатам предварительного анализа объекта, который подвергается мониторингу), кроме того должна быть предусмотрена возможности его изменения по мере необходимости;

– набор контролируемых параметров задан и соответствует целям мониторинга, (по результатам предварительного анализа объекта, который подвергается мониторингу), кроме того должна быть предусмотрена возможности его изменения по мере необходимости;

– предусмотрена возможность прогноза развития ситуации при выходе параметров из «зеленой» зоны;

– возможен вариант построения комбинированной системы учета технических средств (для нужд технического обеспечения: серийные номера, год выпуска, межремонтные сроки, наработка и т. д.) и мониторинга технического состояния КСА;

– может быть реализована как в виде «desktop» приложения, так и в виде «Web»-приложения.

Недостатки:

– требует самостоятельной разработки, при этом необходим большой аналитический объем работ, связанный с определением перечня контролируемых элементов (в том числе и обобщенных: функциональных модулей, КСА в целом), их технических состояний, параметров технических состояний, правил их контроля, задания ограничений и исключений на значения параметров, моделей и расчетных формул для прогноза поведения соответствующих контролируемых параметров и т. д.);

– требует разработки ресурсно-сервисных моделей ИТ-услуг, т. е. структуры взаимосвязей между ИТ-услугой и элементами ИТ-инфраструктуры, обеспечивающими ее работоспособность;

– требует разработки собственных программ клиентов и программ контроля состояния;

– требует разработки собственной системы оповещения должностных лиц.

С точки зрения использования системы мониторинга для КСА второй вариант представляется более предпочтительным, так как дает возможность построить более универсальную систему мониторинга (для различных вычислительных систем), более полно охватить процесс обработки информации (с учетом специфики ее обработки в рамках соответствующих вычислительных систем), дать прогноз развития ситуации и выдать соответствующие рекомендации должностному лицу.

Однако в данном случае существенным является ресурсный вопрос (время, кадры, финансы).

Общий подход к построению системы мониторинга может быть представлен в виде следующей последовательности действий [4]:

1. Определение функционала (объема диагностических функций) проектируемой системы.

2. Определение требуемого объема мониторинга средств автоматизации:

2.1.Определение объема параметров для диагностики отдельных единиц оборудования.

2.2.Определение объема параметров для диагностики групп оборудования.

2.3.Определение объема параметров для диагностики комплекса средств автоматизации в целом.

3. Определение видов и архитектуры технических состояний КСА.

4. Выбор методов и разработка алгоритмов получения технических диагнозов и прогнозов.

5. Определение границ фиксации отклонений.

6. Определение состава и структуры программно-технических средств для построения системы мониторинга.

Список используемых источников

1. Новые информационные и сетевые технологии в системах управления военного назначения. Ч. 2 Новые информационные технологии в системах военного назначения / под редакцией И. Б. Саенко. СПб.: ВАС, 2017. 518 с.

2. Олифер Виктор, Олифер Наталья. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. СПб.: Питер, 2020. 1008 с.

3. Семенов. В. Ю. Исследование и анализ средств и методов мониторинга вычислительных сетей // Решетневские чтения. Материалы XVIII Междунар. науч. конф., посвящ. 90-летию со дня рождения генер. конструктора ракет.-космич. систем акад. М. Ф. Решетнева (11–14 нояб. 2014, г. Красноярск) : в 3 ч. / под общ. ред. Ю. Ю. Логинова ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2014. Ч. 1. 530 с.

4. Бувалый Г. Е., Завершинский В. С. Методы построения систем мониторинга и диагностики оборудования и средств автоматизации газовых промыслов с учетом требований нормативной документации ПАО «Газпром». Газовая промышленность. № 31749. 2017 г.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛИ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ АГЕНТОВ

А. Р. Окладников, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Показана значимость интеллектуальных информационных агентов для внедрения систем искусственного интеллекта в информационные инфраструктуры различных масштабов в условиях развития цифровой экономики. Описаны особенности функционирования интеллектуальных информационных агентов в гетерогенных сетях. Рассмотрены различные подходы к построению моделей процессов функционирования интеллектуальных информационных агентов в гетерогенных сетях. Выделены преимущества расширенных объектно-ориентированных моделей интеллектуальных информационных агентов. Предложена методика построения расширенных объектно-ориентированных моделей интеллектуальных информационных агентов для

исследования влияния характеристик цифровых трактов связи на их динамический профиль.

искусственный интеллект, информационный агент, модель, сеть, расширение, моделирование.

Информационное общество характеризуется стремительным развитием техносферы, обеспечивающей погружение различных видов жизнедеятельности в информационную инфраструктуру. Повышение качества выполняемых в информационной инфраструктуре работ связывается с использованием средств и систем искусственного интеллекта. В условиях развития цифровой экономики непрерывно разрастается масштабность информационной инфраструктуры, обуславливающей возрастание востребованности интеллектуальных информационных агентов для решения задач управления инфраструктурой и решения прикладных задач, связанных с обработкой и генерацией информации и знаний.

В научном направлении по искусственному интеллекту агент позиционируется как носитель вычислительного интеллекта, способного решать задачи воспроизведения способностей человека и задачи обеспечения рациональности. Решение подобных задач интеллектуальными агентами в информационных инфраструктурах, развернутых в гетерогенных сетях, характеризуется представительным использованием разнообразных цифровых трактов связи, оказывающих непосредственное влияние на временные характеристики процессов их функционирования.

В методологии жизненного цикла интеллектуальных информационных агентов временные затраты на передачу информации по цифровым трактам учитываются в неявной форме [1–5], что не позволяет проанализировать их влияние на показатели и критерии качества их функционирования. В связи с этим предлагается модификация модельного ряда интеллектуальных информационных агентов, выделяющая отображение временных затрат на передачу информацию по цифровым трактам на временную развертку их функциональности.

В соответствии с [1, 2] ситуация достижения цели в крупномасштабной гетерогенной сети с помощью интеллектуального информационного агента описывается кортежем

$$\mathbf{S}_v = \langle \mathbf{V}, \mathbf{f}^s(\mathbf{k}_0^s), \mathbf{f}^f(\mathbf{k}_0^f), \mathbf{C}, \mathbf{P}_I, \mathbf{F}_A, \mathbf{F}_B, \mathbf{F}_N, \mathbf{F}_O, \mathbf{N}_O \rangle,$$

где $\mathbf{V}$ – вектор отображения цели;

$\mathbf{f}^s(\mathbf{k}_0^s)$ – вектор плотностей распределения вероятностей $\mathbf{k}_0^s$ дискретного времени успешного выполнения запросов информационного агента;

$\mathbf{f}^{f}(\mathbf{k}_0^f)$ – вектор плотностей распределения вероятностей $\mathbf{k}_0^f$ дискретного времени неуспешного выполнения запросов информационного агента;

C – матрица инциденций, представляющая вырожденный граф объектно-ориентированной модели параллельных действий информационного агента;

$\mathbf{P}_I$ – множество матриц вероятностей переходов, характеризующих последовательные действия в параллельных профилях информационного агента;

$\mathbf{F}_A$ – вектор функций объединения последовательно выполняемых действий информационного агента;

$\mathbf{F}_B$ – вектор функций разветвления последовательно выполняемых действий информационного агента;

$\mathbf{F}_N$ – вектор априорно неопределённых функций объединения распараллеленных действий информационного агента;

$\mathbf{F}_O$ – вектор функций распараллеливания действий информационного агента;

$\mathbf{N}_O$ – нотация объектно-ориентированного моделирования.

Процесс достижения интеллектуальным информационным агентом моделируется с помощью расширенных объектно-ориентированных моделей в классе диаграмм деятельности. Основным преимуществом расширенного объектно-ориентированного моделирования интеллектуального информационного агента является сквозная связность моделей, представляющих его системообразующие подпроцессы, обуславливающая возможность аналитического определения показателей и критериев качества его функционирования.

С целью отображения временных затрат на передачу информацию по цифровым трактам связи предлагается расширение модели запроса интеллектуального агента к информационному источнику.

В предлагаемом расширении процесс запроса интеллектуального агента к информационному источнику описывается в виде логической модели, представляемой ориентированным графом с двумя неузловыми вершинами и двумя последовательными подпроцессами, соответствующими успешному и неуспешному запросам. Каждой неузловой вершине ставится в соответствие фрагмент кода программы, который

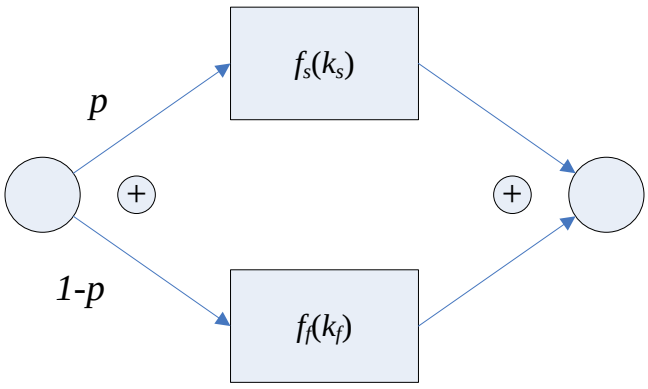


Рисунок. Модель запроса интеллектуального агента к информационному источнику

выполняется последовательно. Разделение и объединение последовательных подпроцессов представляется логической функцией ⊕ – «Исключающее ИЛИ» (рис.). Случайное время выполнения последовательного подпроцесса, соответствующего успешному запросу, описывается плотностью распределения вероятностей $f_s(k_s)$. Случайное время реализации последовательного подпроцесса, связанного с неуспешным запросом, представляется плотностью распределения вероятностей $f_f(k_f)$.

Плотность распределения вероятностей $f_s(k_s)$ успешного выполнения запроса, переданного по цифровому тракту, определяется следующим выражением

$$f_s(k_s) = \sum_{k_{dt}} f_{dt}(k_{dt})\, f_{as}(k_s - k_{dt}),$$
$$k_s = \min(k_{dt} + k_{as}),\ldots,\max(k_{dt} + k_{as}),$$
$$k_{dt} = 1,2,\ldots,K_{dt};\ \ k_{as} = 1,2,\ldots,K_{as},$$

где $f_{dt}(k_{dt})$ плотность распределения вероятностей k_{dt} дискретного времени передачи запроса по цифровому тракту;

$f_{as}(k_{as})$ – плотность распределения вероятностей k_{as} дискретного времени успешной обработки запроса интеллектуального агента к информационному ресурсу.

Плотность распределения вероятностей $f_f(k_f)$ неуспешного выполнения запроса, переданного по цифровому тракту, находится по формуле:

$$f_f(k_f) = \sum_{k_{dt}} f_{dt}(k_{dt})\, f_{af}(k_f - k_{dt}),$$
$$k_f = \min(k_{dt} + k_{af}),\ldots,\max(k_{dt} + k_{af}),$$
$$k_{dt} = 1,2,\ldots,K_{dt};\ \ k_{af} = 1,2,\ldots,K_{af},$$

где $f_{af}(k_{af})$ – плотность распределения вероятностей k_{af} дискретного времени неуспешной обработки запроса интеллектуального агента к информационному ресурсу.

Представленный на рис. 1 процесс запроса интеллектуального агента к информационному источнику относится к разряду последовательных. Он описывается некоторым распределением вероятностей времени извлечения информации $f(k_0)$, где $k_0 = \min(k_s,k_f),\ldots,\max(k_s,k_f)$. Для распределения $f(k_0)$ должно выполняться следующее условие:

$$\sum_{k_0} f(k_0) = 1,\ k_0 = \min(k_s,\ k_f),...,\max(k_s, k_f).$$

Проведем анализ предлагаемой модели запроса к одному информационному источнику с целью определения времени извлечения информации. Для анализа воспользуемся явным методом свертки. В соответствии с построенной моделью:

$$f(k_0) = pf_s(k_s = k_0) + (1-p)\, f_f(k_f = k_0);$$
$$k_0 \ = \ \min(k_s, k_f),...,\max(k_s, k_f).$$

Для проверки подставим последнее выражение в предшествующее соотношение:

$$\sum_{k_0} f(k_0) = p * \sum_{k_0} f_s(k_s) + (1-p) * \sum_{k_0} f_f(k_f) = p + (1-p) = 1.$$

Проверка подтверждает корректность представленной модели запроса интеллектуального агента к информационному ресурсу, учитывающая временные затраты на передачу информации по цифровому тракту.

Модель запроса интеллектуального агента к информационному ресурсу, учитывающая временные затраты на передачу информации по цифровому тракту, входит в кортеж описания ситуации достижения агентом цели в крупномасштабной гетерогенной сети. В связи с этим весь последующий методологический базис агентных технологий, представленный в [1–5], обеспечивается обновлением исходного модельного ряда. При этом реализуется отображение временных затрат на передачу информации по цифровом трактам на показатели и критерии качества функционирования интеллектуальных информационных агентов при различных стратегиях их поведения в гетерогенных сетях.

Введение предложенного расширения процесса запроса интеллектуального агента к информационному источнику приводит к обновлению математического обеспечения модельно-аналитического интеллекта агентных систем. Благодаря подобному обновлению предоставляется возможность проанализировать влияние характеристик цифровых трактов связи на показатели и критерии качества достижения интеллектуальным информационным агентом поставленной цели.

Список используемых источников

1. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 1. С. 50–55.

2. Птицын А. В., Птицына Л. К. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146–154.

3. Птицына Л. К., Лебедева А. А. Методика формирования динамических характеристик интеллектуальных информационных агентов в условиях активной инфокоммуникационной среды // Информация и космос. 2017. № 1. С.105–111.

4. Птицына Л. К., Лебедева А. А. Математическое обеспечение системы приобретения знаний о влиянии активности инфраструктуры на качество функционирования интеллектуальных информационных агентов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 466–470.

5. Дымченко А. В., Птицына Л. К. Модельно-аналитический интеллект мультиагентных систем раннего предупреждения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX-я Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб.: СПбГУТ, 2020. С. 291–294.

УДК 004.428
ГРНТИ 50.41.25

АРХИТЕКТУРА ПРОГРАММЫ-ЭМУЛЯТОРА СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

А. А. Олимпиев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описаны актуальные проблемы создания интегрированной автоматизированной системы управления жизненным циклом, связанные с гетерогенностью ее подсистем. Рассмотрены особенности реализации программных изделий, предназначенных для организации стыков между этими подсистемами. Отмечена особая сложность разработки программных модулей, взаимодействующих с подсистемой управления технологическими процессами. Предложена архитектура программы-эмулятора, которая может ускорить процесс разработки подобных модулей.

автоматизация управления жизненным циклом, разработка программного обеспечения, интеграция автоматизированных систем.

Современный подход к созданию автоматизированной системы управления жизненным циклом продукции (АСУ ЖЦ) опирается на ряд типовых принципов, применяемых организациями, которые стремятся обеспечить максимальный охват всех операций, выполняемых на при проектировании, на производстве, в процессе эксплуатации и утилизации, с помощью интегрированного комплекса средств автоматизации.

В соответствии с данным подходом интегрированная АСУ ЖЦ должна включать в себя следующие основные подсистемы [1]:

– подсистема управления данными об изделии (PDM);

– подсистема управления производственными ресурсами и мощностями (MES);

– подсистема управления жизненным циклом (PLM).

Подсистемы интегрируются друг с другом с помощью технологий автоматизации ведения справочных технологических и эксплуатационных информационных руководств (IETM и IETP) и электронных дел изделия (EPD) [2]. Ожидается, что в результате совместного применения этих технологий может быть получена единая информационная среда предприятия, повышающая эффективность управления процессами жизненного цикла.

Однако, данное комплексное решение не всегда можно сконструировать быстро и качественно по причине того, что применяемые в конкретной АСУ ЖЦ прикладные компоненты редко разрабатываются одной организацией. Чаще всего, эффективные для конкретного процесса предложения по автоматизации относятся к компетенции разных поставщиков. В результате разворачиваемая АСУ ЖЦ обладает достаточно высокой степенью гетерогенности элементов.

Несмотря на то, что для решения описанной проблемы разработан стандарт STEP-технологий [3], данный стандарт каждым производителем либо реализуется не в полной мере, либо адаптирован под нужды предприятия, либо не применяется совсем, что существенно снижает качество конкретных систем в части их совместимости с системами конкурентов. По этой причине для интеграции прикладных компонентов разрабатывается «стыковочное» СПО, позволяющее обеспечить унифицированный доступ к полному описанию данных об изделии и бесшовной автоматизации управления процессами жизненного цикла.

В условиях рыночной экономики, порождающей высокую конкуренцию между производителями программного обеспечения, а также сверх интенсивного развития информационных технологий, разработка «стыковочного» СПО является фактически единственным «быстрым» и «дешевым» способом обеспечения полной интеграции комплекса средств автоматизации управления жизненным циклом изделия. Однако, применение этого способа интеграции приводит к появлению ряда проблем, среди которых:

– отсутствие типовых шаблонов проектирования средств «бесшовной» интеграции приводит к достаточно большому разнообразию решений, которые в конечном итоге нужно сопровождать;

– уникальность каждого из стыков, образованных прикладными компонентами АСУ ЖЦ, приводит к необходимости привлекать разные команды разработчиков (для ускорения разработки), что увеличивает общее разнообразие функциональных модулей.

В свою очередь, разработчики, которые привлекаются для разработки стыковочного СПО также оказываются в достаточно трудной ситуации: отсутствие «под рукой» реальной системы, для которой они должны разработать «стыковочный» модуль. Эта ситуация вызвана тем, что разрабатываемое СПО уникально и с высокой вероятностью не будет больше нигде применяться, поэтому средства на покупку реальных модулей автоматизации и развертывание макета производства не выделяются.

Как правило (но далеко не всегда по различным причинам), разработчикам для работы предоставляется ограниченный доступ к системе через выделенный канал связи, но это решение является не достаточно эффективным и приводит к частым сбоям в их работе. Очевидно, что в этих условиях разработка интегрирующих модулей существенно замедляется, а при коротких сроках приводит к созданию СПО низкого качества.

Другим способом выхода из сложившегося положения является создания программы эмулятора интерфейса, которая имеет тот же API, что и система-оригинал. Как правило, такой эмулятор выдает фиксированный набор «правдоподобных» значений, не связанных между собой, то есть отсутствует реальная эмуляция.

Описанная задача приобретает особую сложность в тех ситуациях, когда необходимо осуществить интеграцию с подсистемами управления технологическими процессами. Для реализации эмулятора работы таких подсистем может быть использовано унифицированное средство эмуляции, которое «умеет» создавать объектную модель подобную оригиналу и имеет возможность переключать внешний интерфейс.

Архитектура программы приведена на рисунке. Программа должны включать в себя следующие основные элементы:

– генератор объектной модели предназначен для того, чтобы сформировать внутреннее представление множества объектов управления, с которыми осуществляется взаимодействие;

– симулятор потока событий, предназначенный для имитационного моделирования динамики технологического процесса (в данном случае полного соответствия между моделью и оригиналом не требуется);

– модуль трансформации результатов симуляции предназначен для «снятия показаний» с объектной модели и отобрания их на параметры мониторинга, которые доступны при считывании через интерфейс эмулятора;

– модуль преобразования запросов и средство настройки контракта предназначены для адаптации эмулируемого API и протокола интеграции к внутренней инвариантной структуре эмулятора;

– средство настройки алгоритмов и структур данных предназначено для эмуляции вычислений, которые выполняет подсистема управления технологическими процессами при получении данных от объектов управления;

– средство настройки симуляции и трансформации предназначено для настройки параметров поток событий, которые обеспечивают динамику объектной модели, а также для настройки алгоритмов трансформации снимаемых показаний к унифицированному виду.

Поскольку в основу внутреннего представления технологического процесса положена адаптируемая динамическая объектная модель, то описанная архитектура программы-эмулятора подходит для эмуляции подсистем управления технологического процесса может быть использована эмуляции подключения системы к технологическим процессам любого вида. В свою очередь, интегрирующий интерфейс в данной архитектуре может задаваться с помощью контракта (описания API и протокола информационного обмена), что позволяет заменять его без перенастройки объектной модели.

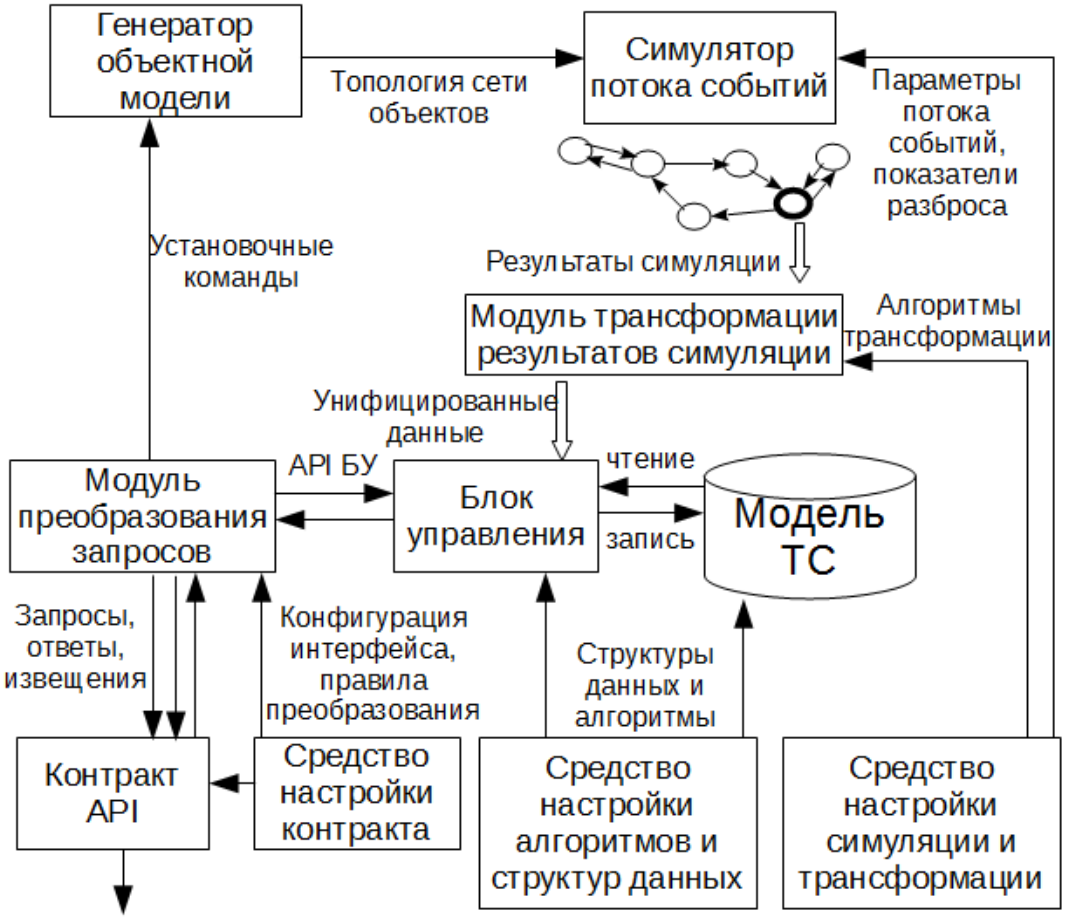


Рисунок. Логическая архитектура программы-симулятора интерфейса интеграции

Список используемых источников

1. Норенков И. П., Кузьмик П. К. Информационная поддержка наукоёмких изделий. CALS-технологии : монография. М. : Изд-во МГТУ им. Н. Э. Баумана, 2002. 319 с.

2. ГОСТ Р 54089-2018. Национальный стандарт Российской Федерации. Интегрированная логистическая поддержка. Электронное дело изделия. Основные положения и общие требования.

3. ГОСТ Р ИСО 10303-1-99. Государственный стандарт Российской Федерации. Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 1. Общие представления и основополагающие принципы.

УДК 004.05
ГРНТИ 50.41.01

СПОСОБ СНИЖЕНИЯ РАЗНООБРАЗИЯ ЯЗЫКОВ ОПИСАНИЯ ФУНКЦИОНАЛЬНОСТИ

А. А. Олимпиев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описан подход к управлению жизненным циклом программного изделия, в котором в качестве основного объекта управления выбран язык описания функциональности информационных систем. Определены основные этапы жизненного цикла языка описания функциональности. Сформулированы актуальные проблемы, которые встают перед разработчиком программного обеспечения при выборе данного пути развития программного обеспечения. Обозначена проблема разнообразия языков, которая наблюдается в многих современных системах и достаточно серьезным препятствием в развитии описанного подхода. Предложен способ решения данной проблемы.

жизненный цикл программного обеспечения, метауправление функциональности, теория трансляции и компиляции, языки описания функциональности информационных систем.

Базовым принципом управления качеством изделия, который применяется во многих наиболее развитых современных предприятиях, является принцип жизненного цикла. Данный принцип позволяет выделить в процессе управления качеством изделия ряд этапов, на которых происходит существенное изменение состояния изделия, начиная от замысла и материализации прототипа до утилизации конечного продукта [1]. С научной точки зрения управление жизненным циклом можно определить как подход к управлению качеством, направленный на систематизацию процессов, которые переводят объект управления из одного состояния в другое. Данный подход позволяет разрабатывать различные модели управления, отличающиеся структурой этапов жизненного цикла, объектами управления, на которых сфокусировано внимание субъекта управления, и, следовательно, набором критериев управления.

Так, например, для управления жизненным циклом телекоммуникаций в качестве приоритетного объекта управления могут быть выбраны услуги

связи, либо телекоммуникационные ресурсы. Для системы образования объектом управления может быть отдельная дисциплина, либо формируемая компетенция. Аналогичным образом можно говорить и об управлении жизненным циклом программного изделия.

В основу одной из таких моделей [2] положена методология управления функциональностью [3], которая позволяет рассмотреть любое программное изделие как совокупность инвариантной программной части и языка описания функциональности (ЯОФ), предназначенного для адаптации программного изделия к изменениям условий функционирования. В качестве приоритетного объекта управления в этой модели должен быть выбран язык описания функциональности, который будет качественно изменяться во времени.

Жизненный цикл программного изделия в этой модели условно делится на следующие этапы:

– этап «Начальная разработка адаптивного программного обеспечения (АПО)» [4], заключающийся в выборе комплекта базовых ЯОФ (БЯОФ) и создании первой версии информационной системы с метауправлением (ИС с МУ);

– этап «Расширение функциональности АПО», в котором происходит формирование библиотеки ресурсов на БЯОФ, содержащих типовые структуры данных и алгоритмы, применяемые в различных условиях использования АПО;

– этап «Оптимизация», который заключается, во-первых, в выделении из всей совокупности библиотек на БЯОФ прикладных ресурсов (структур данных и алгоритмов) и ресурсов общего назначения, во-вторых, в переносе ресурсов общего назначения на уровень интерпретатора — в контекст интерпретации БЯОФ;

– этап «Обобщение», заключается в представлении прикладных ресурсов на декларативном проблемно-ориентированном ЯОФ сверхвысокого уровня (ДПО ЯОФ), полностью заменяющем базовый ИЯОН;

– этап «Визуализация» на котором ДПО ЯОФ заменяется на комбинацию языка диаграмм и диалоговых форм с небольшими алгоритмическими вставками, предназначенными для уточнения отдельных прикладных расчетов.

Предполагается, что данная модель управления обеспечит создание эффективного человеко-ориентированного АПО. Основной целью управления программным изделием в данном случае является снижение стоимости его эксплуатации за счет существенного снижения частоты привлечения разработчиков – то есть пользователь может адаптировать программное изделие под свои нужны в большинстве случаев самостоятельно. Достоинством этой модели является возможность вернуться к этапу «Оптимизация» или «Обобщение» и, используя имеющийся опыт, осуществить быстрый переход на

альтернативные ДПО ЯОФ и языки диаграмм (эта возможность должна закладываться в конструкции ПО). По этой причине данная модель может считаться достаточно гибкой.

Основными проблемами, которые очевидным образом возникают при применении данной модели управления, являются:

– проблема выбора оптимального комплекта базовых ЯОФ, ДПОЯСУ, результирующей совокупности языков диаграмм и проблема их разнообразия;

– проблема адаптации к эволюции искусственных языков (несмотря на то, данная проблема частично устранена за счет внутренней гибкости самой модели управления, недетерменированность, порой нелогичность и непредсказуемость развития искусственных языков не позволяют ее устранить полностью);

– проблема сопровождения АПО на начальных этапах;

– проблема перехода от одного этапа жизненного цикла программного изделия с метауправлением к другому;

– проблема выбора класса программного изделия, создаваемого по методологии метауправления, а также проблема сложности его создания;

– проблема синхронизации семантики компонентов метаинформации на разных функциональных узлах системы, сконструированной с применением АПО;

– проблема управления компонентами метаинформации.

Известно, что переход на новый подход к управлению занимает достаточно много времени и вызывает достаточно сильное сопротивление как у разработчиков, так и у пользователей, поэтому целесообразно подготавливать решение проблем, которые могут возникнуть, заблаговременно.

Одной из таких проблем, с которыми уже много раз сталкивались и продолжают сталкиваться разработчики – проблема разнообразия языков. Для ИС с МУ это разнообразие ЯОФ, которые в ней применяются.

Как правило, для решения данной проблемы применяется три способа:

– использование специализированного стандартного языка, который лучше других подходит для разрабатываемой системы;

– выбор наиболее популярного универсального языка, с которым знакомы подавляющее большинство разработчиков;

– разработка нового перспективного языка, который отвечает самым современным потребностям и соответствует тенденциям развития искусственных языков в данный момент времени.

Недостатком первого способа является то, что стандартные языки, как правило, существенно отстают по уровню развития от текущего уровня развития информационных технологий, требуют дополнительных вложений в обучение пользователей.

Второй способ приводит к тому, что выбранный язык обладает чрезмерной избыточностью, поддержкой различных стилей программирования и включает альтернативные идиомы (исключительно для повышения привлекательности языка). В результате модули с расширением функциональности содержат множество дублирующих друг друга фрагментов кода, а из-за применения различных стилей программирования и альтернативных идиом, сопровождение такой системы становится излишне трудоемким. Помимо перечисленного следует отметить, что интерпретатор избыточного языка тоже избыточен, медленнее работает по сравнению с другими интерпретаторами и занимает большой объем памяти, что делает его неподходящим для применения во встраиваемых системах и системах реального времени.

Третий способ заключается в том, что изучаются наиболее популярные языки программирования и описания функциональности, тенденции и законы развития языков и создается новый язык, напоминающий один из наиболее популярных, но без избыточности. Этот способ обладает определенными достоинствами перед вторым способом, но имеет один большой недостаток: новый интерпретатор обладает множеством дефектов, которые уже устранены в популярных языках в результате их длительной эксплуатации, а новый язык требует больших усилий и вложений в его продвижение для привлечения опытных разработчиков за разумную цену.

Тем не менее, третий способ выглядит наиболее подходящим для решения поставленной задачи по причине того, что он приводит к созданию самых современных и перспективных информационных систем. Однако, в нем недостатки второго способа все еще не полностью устранены. В первую очередь следует отметить, что большинство современных информационных систем состоит из достаточно большого количества функциональных блоков, между которыми распределена ответственность за выполнение той или иной работы. Управление функциональностью различных функциональных блоков в таких системах происходит неравномерно и не для любого из них требуется использовать самые современные языки, обладающие максимальной выразительностью и мощностью. Для некоторых из таких блоков достаточно иметь очень простой язык, применение которого сократит длительность процесса разработки.

Также следует отметить, что различные функциональные блоки информационной системы, как правило, описываются с помощью специальной терминологии и, следовательно, для описания их функциональности эффективнее использовать специальные языки описания функциональности. Очевидным решением данного противоречия является увеличение разнообразия языков описания функциональности.

Чтобы предотвратить рост разнообразия языков, предлагается применять компромиссное решение, которое заключается в следующем: использовать один универсальный язык, но при компиляции интерпретатора для разных функциональных блоков снижать мощность языка для требуемого размера.

Сокращение (и дальнейшее увеличение) мощности языка будет происходить за счет того, что идиомы, применяемые в современных языках, делятся на три группы: базовые идиомы (объявление переменных, операторы и т. п.), составные идиомы (циклы, ветвления, функции) и сложно-составные (классы, структуры, пространства имен и т. п.). Отключение одних идиом недопустимо, другие являются вспомогательными и могут быть исключены из языка.

Так, например, для управления функциональностью одного блока ИС с МУФ будет доступен синтаксис определения классов, для другого не будет; для одного блока будет доступен синтаксис определения пространства имен или процедур, для другого – нет; и так далее.

Данный способ потенциально должен решить проблему размера интерпретатора ЯОФ, так как при отключении синтаксических конструкций можно будет не включать в интерпретатор и блоки кода, которые используются для их исполнения. Также добавление новых перспективных идиом в язык будет происходить сравнительно легче из-за четкой иерархии и модульности структуры транслятора и интерпретатора.

Также имеет смысл применять предлагаемый способ совместно с технологией преобразования ЯОФ в промежуточный код виртуальной машины. Это позволит в дальнейшем облегчить переход на использование нового языка описания функциональности, который неминуемо произойдет рано или поздно.

Список используемых источников

1. Косяков А., Свит У. и др. Системная инженерия. Принципы и практика / пер. с англ. под ред. В. К. Батоврина. М.: ДМК Пресс, 2017. 624 с.

2. Олимпиев А. А. Способ управления жизненным циклом программного изделия. Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27–29 октября 2021 г.: Материалы конференции / СПОИСУ. СПб., 2021. С. 94–95.

3. Шерстюк Ю. М. Основы метауправления функциональностью в информационных системах. СПб.: СПИИРАН, 2000. 155 с.

4. Олимпиев А. А. Методика синтеза системы оперативно-технического мониторинга с метауправлением функциональностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 2. С. 505–510.

УДК 004.423.2
ГРНТИ 50.05.09

ЯЗЫК ПРОГРАММИРОВАНИЯ PYTHON. ОСНОВНЫЕ ОПЕРАЦИИ

И. И. Павлов

Сибирский государственный университет телекоммуникации и информатики

В статье рассматривается история возникновения программирования на языке Python, основные отличительные особенности языка Python. Также рассмотрены основные операторы арифметических действий, присвоения значений и сравнения величин. Для общего понимания приведены примеры при работе на языке программирования Python с результатом выполнения.

Python, программирование, операторы, арифметические действия, присваивание значений, сравнение величин.

В настоящее время в мире существует очень много различных языков программирования. Каждый язык программирования имеет свою популярность, некоторые языки очень популярны, другие не очень. Популярность языка обычно определяется тем количеством программистов, которые его используют при работе. Многие годы популярными языками программирования считаются *Java*, *C++*, *C#*, *JavaScript* и *PHP*. К популярным языкам программирования теперь добавляется язык программирования *Python*.

Python является высокоуровневым языком программирования, *python* – язык интерпретируемый, то есть для вывода результатов используется интерпретатор.

При первом запуске программы на выполнение для нее создается промежуточный код. Именно промежуточный код используется при выполнении программы. Если впоследствии в программу вносятся изменения, то при очередном запуске программы создается новый промежуточный код [1].

В конце восьмидесятых – начале девяностых годов в национальном научно-исследовательском институте математики и компьютерных наук в Нидерландах язык *Python* разработал Гвидо ван Россумом (*Guido van Rossum*). *Python* является составным языком от многих других языков программирования, например, *C, C++* и командной оболочки *Unix*.

Основными отличительными особенностями языка *Python*, которые привлекают начинающих программистов, является:

- ***Python бесплатен*** – это свободно распространяемое программное обеспечение с открытым исходным кодом.
- ***Python легок в изучении*** – он имеет простой синтаксис.

•***Python позволяет создавать легко читаемый код*** – он не перегружен знаками препинания.

•***Python легок в обслуживании*** – имеет модульную структуру.

•***Python располагает богатым «арсеналом»*** – он предполагает большую стандартную библиотеку, которая легко интегрируется в программы.

•***Python портируемый*** – его можно запустить на обширном множестве различных платформ, и везде он будет иметь один и тот же интерфейс.

•***Python расширяемый*** – позволяет добавлять низкоуровневые модули.

•***Python универсален*** – поддерживает как процедурный, так и объектно ориентированный методы программирования.

•***Python гибок в использовании*** – с его помощью можно создавать консольные программы, приложения графического интерфейса, а также сценарии для взаимодействия внешних программ с веб-серверами.

Арифметические действия

Основными операторами арифметических действий, которые используются при программировании на языке *Python* являются:

Сложение	**+**
Вычитание	**–**
Умножение	*****
Деление	**/**
Деление по модулю	**%**
Целочисленное деление	**//**
Возведение в степень	******

Рассмотрим на примере, на входе программы введем:

```
a = 9
b = 2
Addition = a + b
Subtraction = a - b
Multiplication = a * b
Division = a / b
Integer_division = a // b
Remains = a % b
Exponentiation = a ** b
print ('Сложение =', Addition)
print ('Вычитание =', Subtraction)
print ('Умножение =', Multiplication)
print ('Деление =', Division)
print ('Целочисленное деление =', Integer_division)
```

```
print ('Деление по модулю =', Remains)
print (Возведение в степень =', Exponentiation)
```

На выходе программы мы получим:

```
Сложение = 11
Вычитание = 7
Умножение = 18
Деление = 4.5
Целочисленное деление = 4
Деление по модулю = 1
Возведение в степень = 81
```

Оператор % (деление по модулю) делит одно число на другое и выводит остаток от деления. Данный оператор позволяет определить четность или нечетность числа.

Оператор // (целочисленное деление) выводит только целое число, он отбрасывает результат после запятой.

Оператор ** (возведение в степень) возводит первое число в степень второго числа.

Присваивание значений

Основными операторами присваивания значений, являются сокращенными формами от более длинных выражений, которые представлены в таблице ниже.

=	a = b	a = b
+=	a += b	a =(a + b)
–=	a -= b	a =(a - b)
***=**	a *= b	a =(a * b)
/=	a /= b	a =(a / b)
%=	a %= b	a =(a % b)
//=	a //= b	a =(a // b)
****=**	a **= b	a =(a ** b)

Рассмотрим на примере, на входе программы введем:

```
a = 9
b = 2
a += b
print ('Addition & assign:', a)
```

На выходе программы мы получим:

```
Addition & assign: 11
```

Аналогично для остальных операндов:

```
a -= b
print ('Subtraction & assign:', a)
```

```
Subtraction & assign: 7

a *= b
print ('Multiplication & assign:', a)
Multiplication & assign: 18

a /= b
print ('Division & assign', a)
Division & assign 4.5

a //= b
print ('Integer_division & assign', a)
Integer_division & assign 4

a %= b
print ('Remains_assign & assign', a)
Remains_assign & assign 1

a **= b
print (' Exponentiation_assign & assign', a)
Exponentiation_assign & assign 1
```

Сравнение величин

Основными операторами сравнение величин представлены в таблице ниже.

Равенство	==
Неравенство	!=
Больше	>
Меньше	<
Больше либо равно	>=
Меньше либо равно	<=

Оператор равенства == позволяет программисту сравнить две величины и если они равны, то он возвращает *True* (Истина), а если значения величин не равны, то оператор возвращает *False* (Ложь). При этом если значения являются символами, то сравниваются *ASCII*-коды этих символов. Оператор неравенства !=, наоборот, если величины не равны, то он возвращает *True* (Истина), и если величины равны, то возвращает *False* (Ложь).

Оператор «больше» >, сравнивает две величины и если первое значение больше второго, то оператор вернет *True* (Истина), и если первое значение меньше второго, то вернет *False* (Ложь). Оператор «меньше» <, сравнивает

две величины и если первое значение меньше второго, то оператор вернет *True* (Истина), и если первое значение больше второго, то вернет *False* (Ложь).

Оператор «больше либо равно» >=, сравнивает две величины и если первое значение больше или равно второго, то оператор вернет *True* (Истина), и если первое значение меньше второго, то вернет *False* (Ложь). Оператор «меньше либо равно» <=, сравнивает две величины и если первое значение меньше или равно второго, то оператор вернет *True* (Истина), и если первое значение больше второго, то вернет *False* (Ложь).

Рассмотрим на примере, на входе программы введем:

```
a = 1
b = 1
print(a == b)
```

На выходе программы мы получим:

```
True
```

Аналогично для остальных операндов:

```
a = 1
b = 1
print (a != b)
False

a = 1
b = 2
print(a > b)
False

a = 1
b = 2
print(a < b)
True
```

Рассмотрим равенство на примере символов:

```
a = 'a'
b = 'a'
print(a == b)
True

a = 'a'
b = 'b'
print(a == b)
False
```

Приоритет операторов определяет порядок, которому интерпретатор *Python* следует при оценке выражений. Например, в выражении 4+8*2 порядок действий по умолчанию определяет, что умножение будет выполнятся первым, а сложение вторым, таким образом результат будет равен 20.

Список используемых источников

1. Васильев А. Н. Программирование на Python в примерах и задачах. Москва : Эксмо, 2021. 616 с.

2. Майк МакГрат Программирование на Python для начинающих / пер. с англ. М. А. Райтмана. Москва : Эксмо, 2021. 192 с.

УДК 004.633
ГРНТИ 20.17.17

ОБЗОР РЕШЕНИЙ СПЕЦИАЛИЗИРОВАННЫХ СИСТЕМ АВТОМАТИЗИРОВАННОГО СОЗДАНИЯ ДОКУМЕНТАЦИИ

Д. А. Пелих, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире автоматизация технологических процессов, логистики и прочего является актуальнейшей задачей множества специалистов. Не меньше автоматизация затронула и информационную сферу. Фреймворки, имеющие множество готовых решений, no-code платформы сильно упрощают разработку информационных ресурсов. Создание документов также может проходить в автоматическом режиме, сложности возникают только когда необходим интеллектуальный труд человека. О том, как их обойти и пойдёт речь в данной статье.

автоматизация документооборота, информационная система, управление базами данных, нейронные сети.

Разные компании нуждаются в автоматизации документооборота, рассмотрим возможности системы, необходимые для решения данной задачи. Такая система должна брать исходные данные, анализировать их, давать возможность интерактивной настройки необходимых пунктов документации, а также предупреждать об ошибках и несоответствиях в них, и в итоге выдавать готовый документ.

Первое с чем приходится столкнуться при разработке документации – чтение исходных требований, это может быть техническое задание или что-

то ещё. Преимуществом системы автоматизированного создания документации будет работа с файлами, имеющими разное расширение. Помимо текстовых файлов, система должна обрабатывать графические изображения, что можно решить при помощи нейросетевых методов распознавания текста. На рынке программного обеспечения есть готовые решения данной задачи, например, ABBYY FineReader – программа для сканирования документов и распознавания текста, позволяющая также работать с готовым документом, однако её невозможно интегрировать в другую систему. Это приведёт к необходимости выгрузки из программы текстовой информации в подходящем формате и дальнейшей загрузки в систему, что противоречит целям автоматизации.

Также важна кросплатформенность системы. Пользователю нужно иметь доступ к системе не только с десктопного устройства, но и с мобильного, тогда разработка документации становится быстрой и удобной даже в нештатных ситуациях, когда у специалиста нет под рукой ноутбука или рабочего компьютера, что часто бывает при работе с заказчиком в другом часовом поясе. На фоне постоянно увеличивающегося мобильного трафика, возможность работы вне стационарного компьютера особенно актуальна. Так же условие кросплатформенности можно выполнить с помощью ресурса, доступного в сети интернет, адаптированного под все устройства, тогда пользоваться системой будет возможно онлайн с любого браузера. Сейчас многие успешные сервисы работают в облачном формате, среди них конструкторы веб-ресурсов Tilda и Webflow, а также графический редактор Figma.

Для предоставления пользователю возможности корректной настройки необходимых пунктов документации системе необходимо проводить анализ на наличие ошибок и противоречий. В любом технологическом процессе важную роль играет человеческий фактор, который система автоматизации должна сводить к минимуму [2]. При разработке сложной документации система должна через пользовательский интерфейс выдавать пояснения к конкретным характеристикам. А также, если указанный параметр, например, выходит за границу диапазона возможных значений или противоречит другим параметрам, предупредить об этом пользователя.

Также важным преимуществом системы автоматизации документооборота будет возможность работы из пользовательского интерфейса с базой данных, хранящей в себе текстовое и графическое описание отдельных компонентов документации. Это позволит при внесении изменений в одном пункте, автоматически редактировать все места, содержащие такую же информацию.

Обеспечить информационную безопасность позволит разграничение прав доступа пользователей к системе. Каждый сотрудник получает возможность работать только с теми ресурсами, которые ему необходимы, при

этом все документы защищены от случайного, намеренного просмотра или изменения. Пользователь, имеющий ключ доступа, должен иметь возможность внесения необходимых дополнений или изменений в базу данных системы из пользовательского интерфейса программы. Это актуально, так как информация меняется достаточно часто, а редактирование базы данных внешними методами занимает большое количество времени. При вводе данных, должна существовать возможность идентификации пользовательских действий. Например, если каждый пользователь при внесении данных, будет оставлять информацию, ссылающуюся на него, можно узнать пользователя, который ввел эти данные [3].

Готовых реализаций систем создания документации существует достаточно, рассмотрим некоторые из них: Microsoft SharePoint, представляет собой ECM-систему с возможностями управления документооборотом, корпоративным контентом, имеющую возможность интегрирования с MS Office. Данная программа хорошо подходит для организации внутреннего документооборота в компании, но не удовлетворяет требованиям к адаптивности интерфейса и редактированию базы данных [1].

Ещё один интересный пример – DocVision, полнофункциональная BPM/ECM-платформа для автоматизации бизнес-процессов, задач по обработке и хранению документов. Программа предоставляет возможность создания централизованной системы электронного архива, настройки автоматического пополнения, интеграции с учётными системами и операторами электронного документооборота. Также DocVision обеспечивает информационную безопасность и доступ с мобильных устройств. Приложение кросплатформенно, позволяет работать с базой данных, но не удовлетворяет требованиям к адаптивности интерфейса и анализу входных параметров.

Следующей программой будет Alfresco – веб-ориентированная Open Source система для совместной работы в интранете, управления контентом и управления бизнес процессами. Содержит персональные стартовые страницы, библиотеку документов, поисковик, виртуальные рабочие пространства, микроблоги, wiki, блоги, форумы, календари, Данное решение также хорошо подходит для управления бизнес-процессами внутри компании, однако не удовлетворяет требованием к кроссплатформенности и анализу входных данных.

Далее будет рассмотрен онлайн-ресурс FreshDoc, позволяющий создавать любой вид договора при помощи готовых шаблонов. В документе подсвечены места, которые необходимо заполнить – наименования сторон, суммы сделок и др. С помощью уточняющих вопросов пользователю сервис генерирует условия договора под конкретную ситуацию. Всего в базе собрано свыше тысячи документов. FreshDoc доступен с любых устройств, позволяет редактировать документ из графического интерфейса, однако он

заточен под юридические задачи, а также отсутствует возможность редактирования и составления базы данных.

Описанные выше сервисы не позволяют решить всех задач, стоящих перед автоматизированной системой документооборота, поэтому разработка такой программы является актуальной.

Список используемых источников:

1. Сравнительный анализ программных систем делопроизводства и документооборота для автоматизации российских органов государственной власти, предприятий и учреждений. 23.11.2021. URL: https://cs-consult.ru/news-articles/stati-i-materialy/smotret-vse?id=188-sravnitelnyi-analis/ (дата обращения: 23.11.2021).

2. Старостин А. А., Лаптева А. В., Технические средства автоматизации и управления : учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2015. 168 с.

3. Федорова Г. Н. Информационные системы: учебник для студ. Учреждений сред. проф. Образования. 3-е изд., Издательский центр «Академия», 2013. 208 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛИРОВАНИЕ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ С МЯГКОЙ АРХИТЕКТУРОЙ

В. Е. Петрова, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализировано развитие сервис-ориентированных систем с мягкой архитектурой. Рассмотрены вариации в организации интеллектуальных сервис-ориентированных систем. Описаны условия приоритетности применения мажоритарной логики при организации сервис-ориентированных систем с мягкой архитектурой. Выделены альтернативы в моделировании сервис-ориентированных систем. Определен профиль качества сервис-ориентированной системы. Предложена методика построения расширенной объектно-ориентированной модели сервис-ориентированных систем с мажоритарной логикой. Приведены результаты моделирования сервис-ориентированных систем с мягкой архитектурой в случае использования мажоритарной логики.

сервис-ориентированная система, архитектура, приоритетность, мажоритарная логика, качество, моделирование, аналитика.

Современные условия профессиональной деятельности и требования к результатам её выполнения характеризуются высокой интенсивностью изменений, зависящей от особенностей взаимодействия партнеров по деятель-

ности, рынка труда, производимой продукции и оказываемых услуг. Технологические профили информационных инфраструктур, в среде которых осуществляется профессиональная деятельность, находятся в непрерывном развитии. В подобных условиях актуализируется развитие сервис-ориентированных систем с мягкой архитектурой, в которых интеграция объединяемых сервисов выполняется средствами или системами искусственного интеллекта на основании отслеживания изменений в окружающей среде [1–3].

В сервис-ориентированных системах с мягкой архитектурой вариации в объединениях сервисов могут формироваться на базе различных приёмов интеграции агентных, нейросетевых и когнитивных технологий [1]. Описание механизмов интеграции сервисов проводится с применением различных алгебр логики.

При использовании сервис-ориентированных систем с мягкой архитектурой в качестве автоматических систем принятия решений широко применяется мажоритарная логика, позволяющая обеспечить оперативность и идентифицируемость происходящих изменений в объектах, процессах и окружающей среде.

При включении когнитивных технологий в арсенал архитектуры сервис-ориентированных систем предусматривается их моделирование в контексте определения, оценивания и мониторинга качества их функционирования [4–7], приводящее к генерации их модельно-аналитического интеллекта. Качество функционирования сервис-ориентированных систем характеризуется их динамическими характеристиками.

Альтернативы в расширенном объектно-ориентированном моделировании сервис-ориентированных систем формируются в соответствии с типовыми профилями их мягкой интеграции.

В жизненном цикле автоматических систем принятия решений, построенных на базе сервис-ориентированных систем с мягкой архитектурой, опорный вариант их организации ассоциируется с совместным выполнением J критических сервисов. Применительно к этому варианту организации сервис-ориентированных систем целесообразно воспользоваться методологией генерации модельно-аналитического интеллекта посредством расширенного объектно-ориентированного моделирования, основные аспекты которой представляются в [1–7]. Применительно к мажоритарной логике интеграции сервисов реализуется итеративный вычислительный процесс определения и оценивания динамических характеристик сервис-ориентированных систем. Выполнение итераций сопровождается временными затратами, которые могут быть снижены за счет экспресс анализа динамических характеристик сервис-ориентированных систем.

Для выполнения экспресс анализа динамических характеристик сервис-ориентированных систем с мягкой архитектурой предлагаются раскрываемые далее новые формализации их аналитического моделирования.

Пусть каждый *j*-й критический сервис $j = 1, 2, \ldots, J$ описывается в дискретном пространстве состояний и времени. При подобном описании принимается допущение, что каждое состояние длится определённый интервал времени для каждого сервиса из рассматриваемой группы сервисов. При описании каждого *j*-го критического сервиса $j = 1, 2, \ldots, J$ представляется $\mathbf{P}_j$ стохастическая матрица.

В соответствии с описанием *j*-го критического сервиса плотность распределения вероятностей дискретного времени его выполнения определяется согласно выражению

$$f_j(k_j = l) = P^{(l)}_{j,1,N_j+1} - P^{(l-1)}_{j,1,N_j+1},\ k_j = \overline{1, K_j},$$

$$1 - \sum_{k_j=1}^{K_j} (P^{(l)}_{j,1,N_j+1} - P^{(l-1)}_{j,1,N_j+1}) \le \delta_j,$$

где $P^{(l)}_{j,1,N_j+1}$ – $(1, N_j+1)$-й элемент матрицы $\mathbf{P}_j$ после возведения её в степень l;

$P^{(l-1)}_{j,1,N_j+1}$ – $(1, N_j+1)$-й элемент матрицы $\mathbf{P}_j$ после возведения её в степень $(l-1)$;

K_j – верхняя граница дискретного времени выполнения *j*-го критического сервиса;

δ_j – задаваемая и регулируемая величина погрешности представления плотности распределения вероятностей дискретного времени *j*-го критического сервиса.

Для каждого автономно выполняемого *j*-го критического сервиса $R_j(H)$ риск несоблюдения временного регламента выражается соотношением

$$R_j(H) = \sum_{k_j=l>H} (P^{(l)}_{j,1,N_j+1} - P^{(l-1)}_{j,1,N_j+1}),$$

где H – допустимая длительность выполнения *j*-го критического сервиса.

После нахождения плотностей распределений вероятностей дискретного времени их выполнения осуществляется переход к определению интервальных оценок риска несоблюдения временного регламента их совместного завершения.

В процессе исследований динамических характеристик параллельных процессов, синхронизируемых согласно мажоритарной логике, выявляется, что нижняя граница их совместного завершения соответствует случаю при-

менения синхронизации по булевой функции «$\vee$» [5]. При этом верхняя граница их совместного завершения аналогична случаю использования синхронизации по булевой функции «$\wedge$».

Согласно выявленным закономерностям нижняя и верхняя границы риска несоблюдения временного регламента на дискретное время совместного завершения J критических сервисов может определяться по модифицированному методу свертки.

В описанном случае плотность распределения вероятностей $k_{b,1,2,\ldots,j,\ldots,J}$ нижней границы дискретного времени совместного выполнения J критических сервисов вычисляется по следующей формуле

$$f_{b,1,2,\ldots,j,\ldots,J}(k_{b,1,2,\ldots,j,\ldots,J}=l)=(1-P_{1,1,N_1+1}^{(l-1)})\times(1-P_{2,1,N_2+1}^{(l-1)})\times\ldots\times(1-P_{j,1,N_j+1}^{(l-1)})\times\ldots$$
$$\times(1-P_{J,1,N_J+1}^{(l-1)})-(1-P_{1,1,N_1+1}^{(l)})\times(1-P_{2,1,N_2+1}^{(l)})\times\ldots\times(1-P_{j,1,N_j+1}^{(l)})\times\ldots\times(1-P_{J,1,N_J+1}^{(l)}),$$

$$k_{b,1,2,\ldots,j,\ldots,J}=\overline{1,K_{b,1,2,\ldots,j,\ldots,J}},$$

Нижняя граница риска несоблюдения временного регламента совместного выполнения J критических сервисов находится по формуле

$$R_b(H)=\sum_{k_{b,1,2,\ldots,j,\ldots,J}=l>H} f_{b,1,2,\ldots,j,\ldots,J}(k_{b,1,2,\ldots,j,\ldots,J}=l).$$

Плотность распределения вероятностей $k_{t,1,2,\ldots,j,\ldots,J}$ верхней границы дискретного времени совместного выполнения J критических сервисов представляется преобразованием

$$f_{t,1,2,\ldots,j,\ldots,J}(k_{t,1,2,\ldots,j,\ldots,J}=l)=P_{1,1,N_1+1}^{(l)}\times P_{2,1,N_2+1}^{(l)}\times\ldots\times P_{j,1,N_j+1}^{(l)}\times\ldots\times P_{J,1,N_J+1}^{(l)}-$$
$$-P_{1,1,N_1+1}^{(l-1)}\times P_{2,1,N_2+1}^{(l-1)}\times\ldots\times P_{j,1,N_j+1}^{(l-1)}\times\ldots\times P_{J,1,N_J+1}^{(l-1)},\quad k_{t,1,2,\ldots,j,\ldots,J}=\overline{1,K_{t,1,2,\ldots,j,\ldots,J}},$$

Верхняя граница риска несоблюдения временного регламента совместного выполнения J критических сервисов вычисляется согласно соотношению

$$R_t(H)=\sum_{k_{t,1,2,\ldots,j,\ldots,J}=l>H} f_{t,1,2,\ldots,j,\ldots,J}(k_{t,1,2,\ldots,j,\ldots,J}=l).$$

Таким образом, интервальная оценка $R(H)$ риска несоблюдения временного регламента совместного выполнения J критических сервисов выражается следующими неравенствами

$$R_b(H) < R(H) < R_t(H).$$

Выведенные аналитические соотношения для интервальной оценки риска несоблюдения временного регламента совместного выполнения критических сервисов образуют математическое обеспечение опорного варианта сервиса экспресс мониторинга и управления качеством критической сервис-ориентированной системы.

Экспресс мониторинг может опережать реализацию профилирования критической сервис-ориентированной системы с целью выбора таких характеристик её архитектуры, который соответствует требуемому временному регламенту.

Для детализации знаний о качестве критической сервис-ориентированной системы осуществляется переход к вычислению фактического значения риска несоблюдения временного регламента совместного выполнения критических сервисов на основе рекуррентных процедур, раскрытых в [4, 5].

При управлении качеством критической сервис-ориентированной системы предоставляется возможность маневрирования характером и длительностью возможных состояний, а также их числом при параллельной реализации функциональности.

Предложенные формализации расширяют возможности оперативного реагирования критических сервис-ориентированных систем на проявления внештатных ситуаций в функционировании объектов, комплексов, систем и сетей и недопустимые изменения в окружающей среде.

Список используемых источников

1. Птицына Л. К., Птицын А. В. Интеллектуальное конфигурирование сервис-ориентированных систем // Информационные системы и технологии в моделировании и управлении : сборник материалов IV Всероссийской научно-практической конференции с международным участием (21-23 мая 2019 г.) / отв. редактор К.А. Маковейчук. Симферополь : ИТ «АРИАЛ», 2019. С. 48-51.

2. Ptitsyna L. K., Shevchenko N. E. S., Belov M. P., Ptitsyn A. V. Planning Architecture of Service-oriented Systems under Uncertainty // Proceedings of 2020 23rd International Conference on Soft Computing and Measurements. SCM 2020, 2020. pp. 101–104.

3. Птицына Л. К., Эль Сабаяр Шевченко Н., Белов М. П., Птицын А. В. Математическое обеспечение мягких архитектур сервис-ориентированных систем в условиях неопределённости // XXIV Международная конференция по мягким вычислениям и измерениям (SCM-2021). Сборник докладов. Санкт-Петербург. 26–28 мая 2021 г. СПб.: СПбГЭТУ «ЛЭТИ». С. 121–124.

4. Птицына Л. К., Смирнов Н. Г. Разработка и анализ моделей интеграции сервис-ориентированных средств в гетерогенных сетях // Научно-технические ведомости СПбГПУ. 2011. № 6.1 (138). С. 71–81.

5. Птицына Л. К., Соколова Н. В. Параллельные вычислительные процессы в системах мониторинга и управления : учебное пособие / рец.: В. С. Заборовский, Тим-

ченко В. В. ; Федеральное агентство по образованию, Санкт-Петербургский государственный политехнический университет, Приоритетный национальный проект «Образование», Инновационная образовательная программа Санкт-Петербургского государственного политехнического университета. СПб. : Издательство Политехнического университета, 2008. 133 с.

6. Птицына Л. К., Савлиш А. В., Смирнова П. В. Аналитическое моделирование сервис-ориентированной системы с типовой конфигурацией средств // Труды учебных заведений связи. 2016. Т. 2, № 3. С. 55–59.

7. Птицына Л. К. Методология генерации модельно-аналитического интеллекта сервис-ориентированных систем с гарантиями качества // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2017. Т. 3. С. 351–354.

УДК 004.428
ГРНТИ 50.43

АНАЛИЗ И КОНЦЕПЦИЯ РАСШИРЕНИЯ БРАУЗЕРА, ОСУЩЕСТВЛЯЮЩЕГО РОДИТЕЛЬСКИЙ КОНТРОЛЬ

М. Д. Поведайко, З. В. Чубарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается алгоритм работы функции расширения, осуществляющего родительский контроль, который поможет улучшить его работу. В основе данной функции лежит в отличие от других программ данного типа не запрет, а образовательный процесс. Изучена актуальная статистика использования интернета детьми, которая показала важность разрабатываемого алгоритма.

алгоритм, дети, родительский контроль, расширение.

Современным детям и подросткам сложно представить свою жизнь без интернета, для них это не только источник развлечений, но и информационно-образовательная среда. По данным Института статистических исследований и экономики знаний НИУ ВШЭ от 13 января 2022 года, интернетом пользуются 68,3 % российских детей в возрасте от 3 до 6 лет. Хотя еще в 2011 году этот показатель составлял всего 22,6 %. Таким образом, это значение выросло втрое за последние десять лет. Также, из сведений Росстата, в сеть хотя бы раз в сутки выходят более 80 % детей в возрасте от 3 до 14 лет, а для подростков от 12–14 лет данный показатель составляет 95 % [1].

Но, несмотря на всю несомненную пользу интернета, проявляющуюся в виде улучшения мыслительных функций, хорошо развитой слуховой и

зрительной памяти у детей, он может также представлять угрозу их физическому или психическому здоровью, так как большая часть информации не предназначена для детей по определенным моральным или этическим нормам.

На Международной конференции по информационной безопасности детей в современной медиасфере Михаил Астахов – уполномоченный при президенте Российской Федерации по правам ребёнка, заявил следующее: «Больше половины пользователей сети в возрасте до 14 лет осматривают сайты с нежелательным содержанием. Посещают сайты, распространяющие порнографию, 39 % детей, наблюдают сцены насилия 19 %, увлекаются азартными играми 16 % детей». Согласно его данным, 14 % несовершеннолетних пользователей ищут информацию, связанную с алкоголем и наркотическими веществами, 11 % с экстремизмом и национализмом [2].

Ответственность за ограждение ребенка от нежелательного контента в интернете лежит в первую очередь на родителях. Они должны уделять особое внимание тому, чем интересуется ребенок, находясь в сети. Помочь в этом может программное обеспечение с функцией родительского контроля, которое является одним из самых эффективных технических средств обеспечения безопасности.

Такое ПО осуществляет следующие функции:

1. Установка запрета на посещение веб-сайтов. Они определяются разработчиками или родителями с помощью списков фильтрации, которые могут быть белыми – когда запрет вносится на все ресурсы, кроме разрешенных, или черными – запрет только на определенные сайты или категории сайтов.

2. Мониторинг и блокировка исходящего контента, например, конфиденциальных данных.

3. Ограничение на время нахождения в Сети, поскольку интернет-зависимость также является одной из проблем современного общества. Директор Фонда развития интернета, доктор психологических наук Галина Солдатова и нейропсихолог Центра патологии речи и нейрореабилитации Анастасия Вишнева на международной конференции 2019 года Edcrunch, которая была посвящена цифровым инновациям в образовании, назвали оптимальное время использования интернета детьми. Согласно исследованиям, норма использования интернета для детей в возрасте от 5 до 6 лет – до одного часа в день, для школьников 7–11 лет – от одного до трёх часов в день, для младших подростков (12–13 лет) – от трёх до пяти часов [3]. Отклонение от нормы может привести к ухудшению зрения, снижению продуктивности, нарушениям в работе опорно-двигательного аппарата.

4. Отслеживание посещаемого контента с составлением отчетов.

5. Защита зрения с использованием режима ночного экрана, уменьшающего количество синего света.

Однако такое ПО с функцией родительского контроля может стать опасным, так как большое количество контроля и запрета может сказаться на возможностях общения и уровне развития ребенка, привести к формированию характера с элементами интроверсии, аутистичности, социофобии, некоммуникабельности и т. п.

Таким образом, выходит, что чрезмерно опекающий и контролирующий родитель становится причиной трудностей для воспитываемого.

Отсюда можно сделать вывод о том, что родительский контроль хоть и необходим, поскольку с ростом количества информации растут и реальные угрозы для детей, но он не должен строиться только на запретах. Решением этой проблемы будет добавление в расширение функции переадресации с сайта с нежелательным контентом на страницы с обучающей информацией для ребенка. Это могут быть мультфильмы о вреде наркотиков, алкоголя, статьи, написанные специально для детей об анорексии, последствиях увлечения азартными играми и т. д.

Таким образом, в результате вышесказанного можно заявить, что указанное ПО отсутствует и его необходимо разработать и интегрировать в браузер. Первым этапом разработки является алгоритм.

Алгоритм работы данной функции представлен на рисунке.

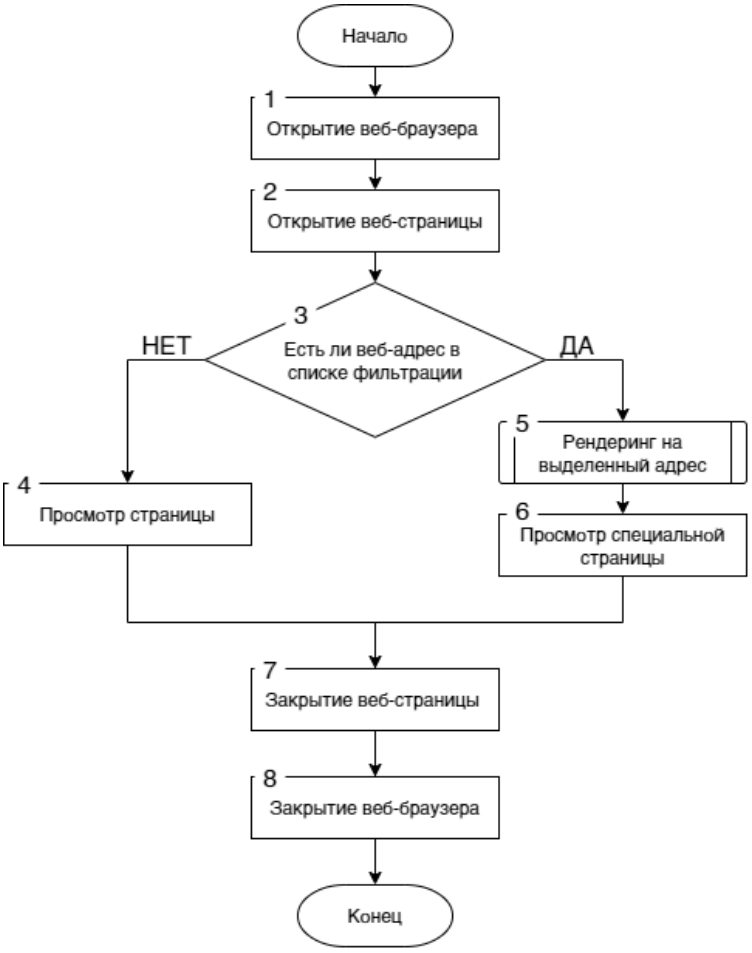


Рисунок. Алгоритм работы функции расширения

Принцип работы функции основан на списках фильтрации, где нежелательным сайтам с запрещенным контентом по какой-то определенной тематике будет соответствовать страница, на которую будет осуществлена переадресация.

Таким образом, в рамках исследования был проведен анализ рисков Интернета, нарушающих безопасность ребенка, а также предложен алгоритм работы расширения для браузера родительского контроля, основанный не на запрете, а на образовательном процессе.

Код, написанный на языке JavaScript и реализующий данную функцию, будет представлен в дипломной работе.

Список, используемых источников

1. Абдрахманова Г. И., Васильковский С. А., Вишневский К. О. и др. Цифровая экономика: 2022: краткий статистический сборник // Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2022. 124 с.

2. Больше половины детей в РФ посещают сайты с нежелательным содержанием // РИА НОВОСТИ. URL: https://ria.ru/20130227/924834355.html (дата обращения: 15.12.2021).

3. Российские ученые определили оптимальное время, которое дети могут проводить онлайн // Коммерсантъ. URL: https://www.kommersant.ru/doc/4117340 (дата обращения: 15.12.2021).

УДК 654.739
ГРНТИ 49.33.29

СТРАТЕГИЯ ПОЗИЦИОНИРОВАНИЯ IT ПРОДУКТА НА ПРИМЕРЕ ПРИЛОЖЕНИЯ DEVICE INSTRUCTION AR

О. П. Погадаева, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель исследования – определить особенности разработки стратегии позиционирования IT-продукта. В статье акцентируется внимание на том, что продуктовая и маркетинговая части должны действовать сообща, т.к. стратегия бренда имеет прямое влияние на дизайн, пользовательский опыт и успех продукта. Позиционирование – это разработка предложения и образа бренда, которые направленны на формирование или закрепление конкурентной позиции бренда на определенном рынке. Позиционировать бренд невозможно для всех, потому что это размывает образ бренда. Позиция бренда должна быть четко сформулированной и непоколебимой. Главная цель позиционирования – дифференцироваться на фоне конкурентов, и укрепить собственные позиции. В результате исследования представлен оптимальный алгоритм позиционирования.

позиционирование, IT-продукт, ASO, приложение, брендинг, пользователь, конкурент, смартфон, продвижение.

Методы позиционирования бренда непрерывно меняются по мере развития цифрового сообщества. С более чем 3,8 миллиардами пользователей

смартфонов по всему миру неудивительно, что индустрия мобильных приложений переживает бум. Использование приложений и доминирование смартфонов по-прежнему растут без каких-либо признаков замедления в обозримом будущем [1].

Разработчики приложений прогнозируют, что к 2023 году рентабельность инвестиций в приложения для смартфонов превысит 935 миллиардов долларов, поскольку в настоящее время в магазине GooglePlay насчитывается более 2,87 миллиона приложений. С другой стороны, в App Store доступно для загрузки 1,96 миллиона приложений [2].

Разработка или улучшение мобильного приложения продвигает бизнес. Для тех, кто только что перенес свой бизнес в Интернет, лучше всего инвестировать в приложение своего бренда уже сейчас, чтобы создать хороший трафик, который в дальнейшем конвертируется.

Необходимо, чтобы пользователи загружали приложение и использовали его одновременно с посещением веб-сайта. Это одна из стратегий цифрового маркетинга, которая обязательно приведет к конверсии.

Таким образом, чтобы приложение было успешным, должны совпасть два фактора:

1) Пользователи должны загрузить приложение;

2) Они должны его использовать.

В переполненном пространстве с миллионами пользователей получить загрузку уже достаточно сложно, вот почему брендинг так важен. Брендинг включает в себя: позиционирование бренда, фирменный стиль и имидж бренда.

Позиционирование бренда приложения (первая часть процесса брендинга) должно произойти в первую очередь. Правильное позиционирование означает, что приложение выделяется среди целевой аудитории и отличается от конкурентов. Исследование рынка включает в себя изучение конкурентов, определение целевой аудитории и определение ключевых слов, соответствующих приложению [3].

Карта позиционирования, основанная на исследованиях, является отличным визуальным инструментом, который поможет определить нишевые категории в конкурентной среде. На примере приложения Device Instruction AR была составлена карта позиционирования (рис. 1).

Согласно полученной карте позиционирования, приложение Device Instruction AR выгодно отличается от конкурентов, обладая высоким usability и высоким качеством сканирования объектов.

Фирменный стиль приложения – это восприятие, которое владелец приложения хочет создать в сознании пользователя. Все принадлежащие элементы – визуальные эффекты, контент, социальные сети, веб-сайт, коммуникации с пользователями – создают фирменный стиль бренда [4].

Рис. 1. Карта позиционирования

Фирменный стиль приложения составляют:

1) Название приложения – обязательно простое и запоминающееся. Использование ключевых слов в названии помогает в поиске. Пример: Device Instruction AR;

Рис. 2. Логотип приложения Device Instruction AR

2) Логотип приложения – графическое представление фирменного стиля (рис. 2). Он должен отражать, о чем приложение и для кого оно предназначено;

3) Значок приложения – дизайн значка приложения должен отражать индивидуальность и стиль бренда. Поскольку иконки предназначены для отображения на экранах смартфонов, они должны быть четкими и простыми, чтобы выделяться, несмотря на их небольшой размер. Часто значок является эмблемой логотипа бренда;

4) Скриншоты приложения – оптимизированные скриншоты играют важную роль в ASO (рис. 3). Они также позволяют показать пользователям, на какой опыт они могут рассчитывать, если решат загрузить приложение;

Рис. 3. Скриншоты приложения Device Instruction AR

5) Видео для предварительного просмотра приложения - отражает то, что символизирует бренд;

6) Фирменные шрифты/цвета – жирный шрифт и яркие цвета подчеркивают индивидуальность, в отличие от округлых, тонких шрифтов и пастельных тонов;

7) Фирменный голос – использование неформальных, разговорных, остроумных формулировок в сообщениях передает тип индивидуальности бренда;

8) Постоянство бренда – все эти элементы должны быть согласованы по всем направлениям.

Уникальность и то, что символизирует бренд, – это то, что помогает брендам выделяться среди конкурентов, привлекает целевую аудиторию и улучшает пользовательский опыт.

На первый взгляд фирменный стиль и имидж бренда могут показаться одним и тем же. Но есть одно фундаментальное отличие: контроль лежит не на бренде (как в случае с фирменным стилем), а на пользователе. Имидж бренда – это о том, как потребитель воспринимает бренд в реальности.

Аспект брендинга направлен на построение отношений бренд-потребитель. Необходимо обращать внимание на рейтинги AppStore: если пользователь недоволен какой-либо функцией, он сообщает об этом. Ответы на отзывы имеют большое значение. Что касается и положительных отзывов, то выражение признательности за отзыв создает связь с лояльными пользователями.

Необходимо стимулировать лояльных пользователей: стимулирование рефералов или предоставление скидок за постоянное использование приложений (например, значки, награды за покупки в приложении и т. д.) поможет укрепить позиции среди пользователей. Поклонники приложения будут делиться с другими или продолжать использовать продукт только в том случае, если у них будет положительное мнение о нем.

Таким образом, радикальное несоответствие между фирменным стилем и имиджем бренда, которое не исправлено, плохо скажется на будущем приложения.

Оптимизация магазина приложений – это бесконечный процесс, поэтому необходимо пробовать что-то новое и оптимизировать свое приложение, чтобы сохранить его рейтинг.

Необходима оптимизация маркетинговых стратегий, таких как создание видеороликов, контента в блогах или использование маркетинга влияния для продвижения бренда и приложения. Нужно тестировать новые способы в стратегиях позиционирования бренда, чтобы оставаться на вершине поисковых рейтингов.

Список используемых источников

1. Морозова Е. А. Сегментирование и позиционирование как ключевые элементы эффективной деятельности ИТ-организации // Научные труды Вольного экономического общества России. 2020. № 3. С. 503–508.

2. Пискунова Н. Л. Особенности интернет-маркетинга в IT-сфере // Интернет-маркетинг. 2019. № 2. С.144–155.

3. Dickson P., Ginter J. Market Segmentation, Product Differentiation, and Marketing Strategy // Journal of Marketing. 1987. Vol. 51. № 2. pp. 1–10.

4. Wedel M. Kamakura W. Market Segmentation: Conceptual and Methodological Foundations. Springer Publishing, 2000. 408 p.

УДК 004; 311.2; 654.1
ГРНТИ 49.01; 50.45

КОМИНИРОВАННЫЙ МОНИТОРИНГ ТЕХНОЛОГИЧЕСКИХ ПАРАМЕТРОВ МАГИСТРАЛЬНЫХ НЕФТЕПРОВОДОВ

О. А. Поляков, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интеллектуализация средств контроля систем автоматизации и управления технологическими процессами в нефтегазовой отрасли в условиях цифровой экономики актуальна в научном смысле и востребована на практике. Представлены результаты исследования вариантов реализации подсистемы сбора технологических параметров магистрального нефтепровода на основе комбинированного беспроводного доступа традиционных датчиков и средств интеллектуальной предобработки видеоданных. Предложены системотехнические решения по построению интеллектуальной точки доступа магистрального объекта мониторинга нефтепроводов.

датчик, интеллектуальная предобработка данных, беспроводный доступ.

Особенности географического положения в нашей стране источников сырьевых ресурсов для экономики, сложные климатические условия эксплуатации инфраструктуры добывающих отраслей, например, магистрального трубопроводного транспорта нефти и нефтепродуктов, обусловливают актуальность исследования направлений развития систем мониторинга объектов инфраструктуры и системотехнических решений по их построению [1]. Протяженность магистрального нефтепровода в России составляет около 50 тыс. км, нефтепродуктопровода – 20 тыс. км, при этом доля нефти в общем объеме грузооборота составляет более 40 %, а нефтепродуктов – меньше, чем на порядок процентов. Количество перекачивающих станций приближается к отметке 500 единиц.

Для трубопроводного транспорта нефти и нефтепродуктов характерны следующие проблемы, как противоречия, которые не могут в явном виде быть разрешены существующими способами, например, между:

– необходимостью повышения доходности нефтепровода и ужесточением затратных требований к экологической и эксплуатационной безопасности линейных и площадных объектов нефтепроводов [2];

– востребованностью в комплексном техническом перевооружении подсистем мониторинга технологических процессов, объектовой и информационной безопасности объектов нефтепроводов и традиционным раздельным развитием подсистем мониторинга [3, 4];

– необходимостью оптимизации численности персонала служб эксплуатации магистральных нефтепроводов и усложнением внедряемых на линейных и площадных объектах нефтепроводов системотехнических решений, информационных и телекоммуникационных технологий [5–8].

Объектом исследования являются (рис. 1) линейная часть (магистральный трубопровод, сооружения связи) и площадной объект (здания, сооружения и технические устройства для обеспечения объектов требованиям безопасности) в понятиях, регламентированных нормативными документами (например, ГОСТ Р 57512-2017).

Рис. 1. Объект исследования систем мониторинга нефтепроводов

Предметом исследования является организация мониторинга параметров магистрального нефтепровода и системотехнические решения в части подсистем сбора технологических и иных параметров.

Существующая организация системы сбора технологических параметров магистрального нефтепровода описана в ряде корпоративных документов (например, в ОТТ-17.020.00-КТН-0286-21 ПАО «Транснефть»), охватывает системы нижнего уровня АСУ ТП (приборы контроля и регулирования, средства обнаружения пожара, средства оповещения и управления, щиты приборные и манометрические сборки), характеризуется реализацией автоматизированного управления рассредоточенными объектами с раздельной или комплексной архитектурой средств и интерфейсом последовательного радиального типа.

Анализ уровня технической реализации подсистемы сбора показывает, что технологические параметры магистрального нефтепровода определяют по участкам (рис. 2) в специально оборудованных контролируемых точках (рис. 3), расстояние между которыми составляет до 50 км, данные от которых агрегируют в контроллерах и передают по выделенным линиям связи на корпоративный специализированный сервер АСУ ТП.

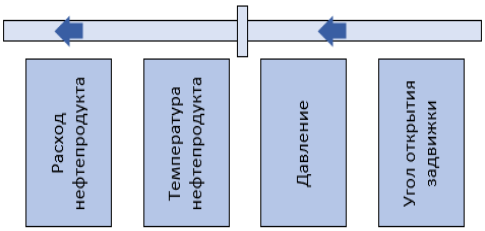


Рис. 2. Данные мониторинга участка

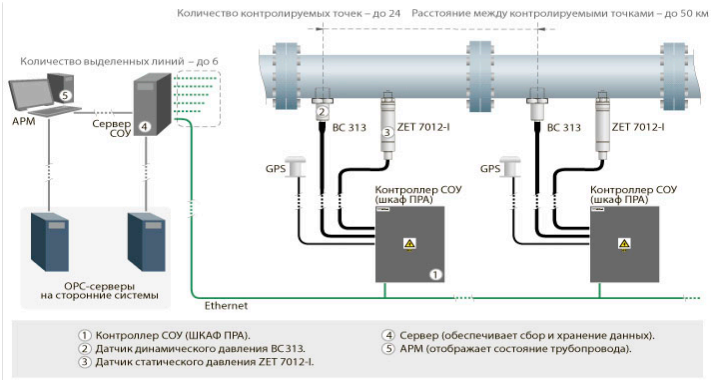


Рис. 3. Оборудование участка мониторинга (*источник: https://tdgears.ru/device/id39996.htm*)

Данные от средств видеонаблюдения используются либо при мониторинге объектовой безопасности (рис. 4), либо в реализациях извещателей пожарных (оптических) при мониторинге пожарной безопасности (по ГОСТ 53325-2015), то есть в различных подсистемах сбора данных магистрального нефтепровода.

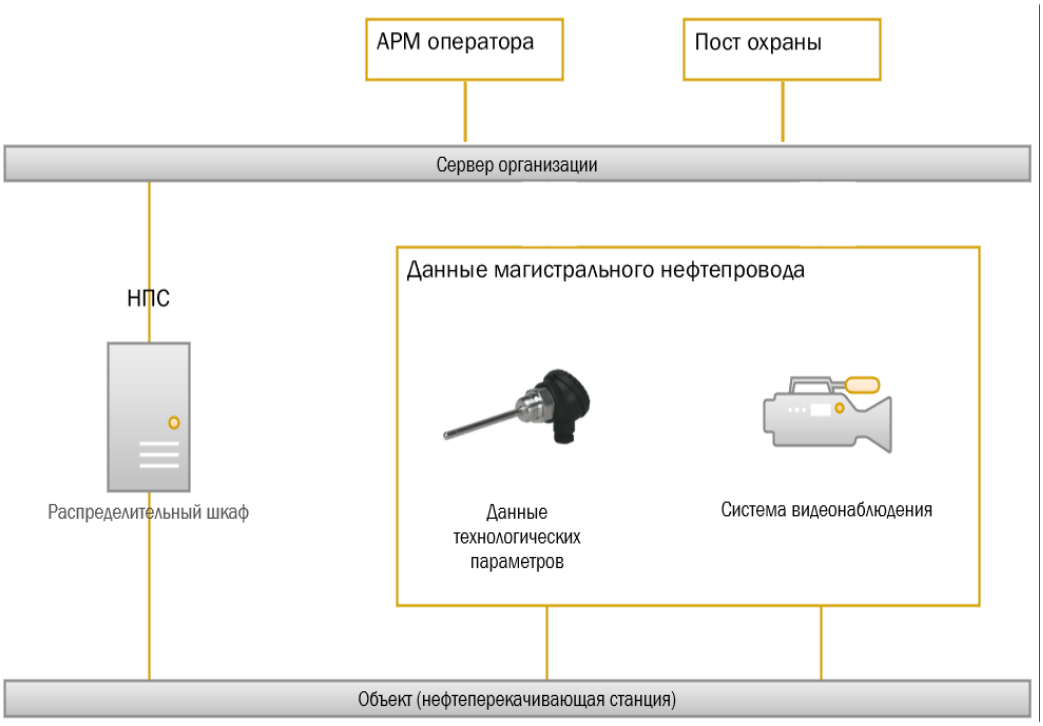


Рис. 4. Организация подсистем сбора данных различных подсистем АСУ ТП

Одним из рациональных подходов разрешения существующих проблем трубопроводного транспорта нефти является реализация технического решения по построению подсистемы сбора данных на основе комплексного применения датчиков технологических параметров, средств видеонаблюдения с интеллектуальной предобработкой видеопотока данных, сетевой технологии с низким энергопотреблением (LoRa, Long Range) и сервисов «облачного хранилища данных» (рис. 5).

Современные интеллектуальные видеокамеры (например, BEWARD SV3210DBS, Dahua DH-IPC-HDBW5442EP-ZE, Acumen AiP-B24N-05Y2B) реализуют несколько режимов детекции, такие как вход/выход объекта, движение и пересечение линий, дым и другие, что позволит перейти от непрерывной передачи видеотрафика к передаче событийных данных.

Переход от кабельных или оптоволоконных линий связи, как линейных объектов магистрального нефтепровода, к беспроводным сервисам, например, сетевой технологии LoRaWAN имеет существенные преимущества (рис. 6) и позволит снизить капитальные и операционные затраты на реализацию подсистемы сбора данных технологических параметров.

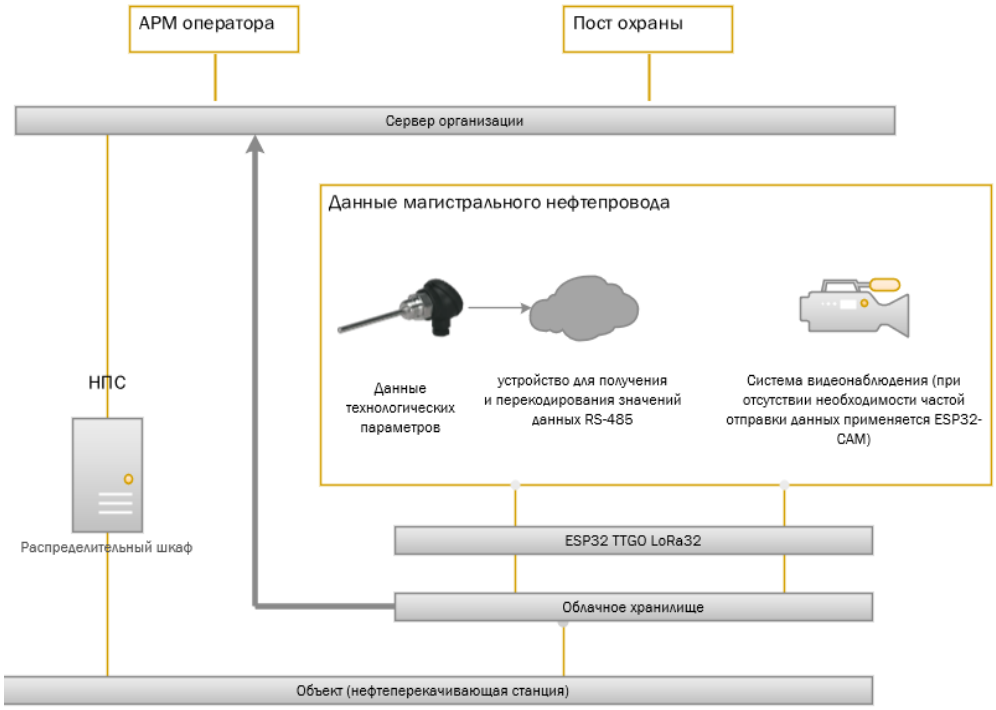


Рис. 5. Организация комбинированного мониторинга технологических параметров магистральных трубопроводов

Применение в подсистеме сбора данных сервисов «облачных хранилищ данных» обусловлено стремительным развитием архитектуры информационного взаимодействия «Интернет Вещей» посредством внедрения новых технологий «облачных» или «туманных вычислений».

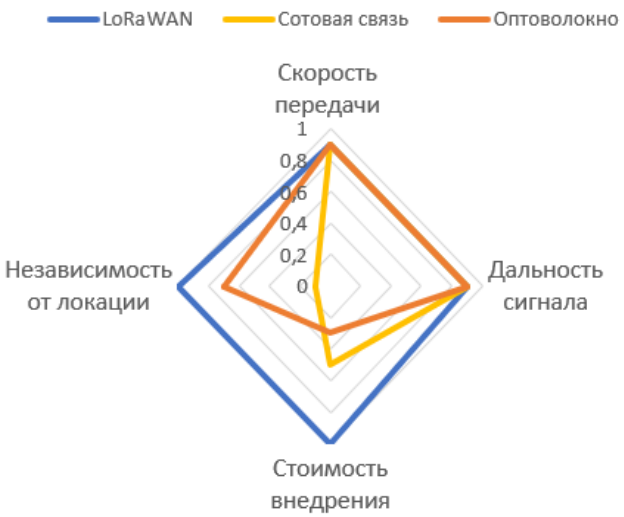


Рис. 6. Результаты оценки применимости технологий в подсистеме сбора данных

Таким образом, предлагаемые системотехнические решения комбинированного мониторинга технологических параметров магистральных нефтепроводов обеспечат:

– разрешение противоречий между доходностью нефтепровода и обеспечением экологической и эксплуатационной безопасности за счет внедрения типовых энергосберегающих устройств многоцелевого применения;

– частичное снижение противоречия между комплексным техническим перевооружением подсистем мониторинга и раздельным их развитием

за счет внедрения многофункциональных средств встроенной видеоаналитики;

– частичное снижение противоречия между сокращения служб эксплуатации нефтепроводов и усложнением технических средств посредством внедрения многоуровневой автоматизированной системы интеллектуальной обработки данных мониторинга.

Материалы подготовлены в рамках прикладных научных исследований СПбГУТ за счет средств федерального бюджета.

Список используемых источников

1. Шестаков А. В., Фролова К. А., Плетнев Я. А. Геоинформационные системы в управлении и мониторинге техногенных объектов. Схемы и QR-ссылки: учебное пособие. СПб: Любавич, 2021. 100 с. ISBN 978-5-907440-62-3.

2. Лисин Ю. В., Александров А. А. Мониторинг магистральных нефтепроводов в сложных геологических условиях // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. 2013. № 2 (10). С. 22–27.

3. Худяков С. А., Таламанов В. Н., Козенков В. А., Козенкова Г. Л. Система мониторинга магистральных нефтепроводов // Эксплуатация морского транспорта. 2020. № 2 (95). С. 119–121.

4. Поляков О.А. Анализ технического уровня интеллектуализации систем мониторинга магистральных нефтепроводов // Студенческие научные исследования: сб. ст. IX Международной научно-практической конференции. В 2 ч. Ч. 1. Пенза: МЦНС «Наука и Просвещение», 2021. С. 69–72.

5. Кочеткова Л. И. Анализ основных методов мониторинга магистральных нефтепроводов в режиме реального времени // Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство. Сб. науч. стат. по итогам VIII международ. научн. конф. 2019. С. 134–137.

6. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

7. Pham V., Kisel V., Kirichek R., Koucheryavy A., Shestakov A. Evaluation of A Mesh Network based on LoRa Technology // 2021 23rd International Conference on Advanced Communication Technology (ICACT). pp. 1280–1285. DOI: 10.23919/ICACT51234.2021.9370792.

8. Kukunin D., Berezkin A., Zadorozhnyaya A., Karelin E., Shestakov A. Model of Adaptive Data Transmission System // 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). DOI: 10.1109/ICUMT 54235.2021.9631637.

УДК 004.932.2
ГРНТИ 28.23.15

СЕГМЕНТАЦИЯ ЦВЕТНОГО ИЗОБРАЖЕНИЯ НА ОСНОВЕ РАЗЛИЧНЫХ МОДЕЛЕЙ ЦВЕТОВОГО ПРОСТРАНСТВА ПРИ ПОМОЩИ АВТОМАТИЧЕСКОЙ ТЕХНИКИ GRABCUT

М. И. Рысюков

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В данной статье представлено сравнительное исследование с использованием различных цветовых пространств для оценки эффективности сегментации цветного изображения с использованием автоматической техники GrabCut.

цветовые пространства, сегментация, техника GrabCut.

Введение

GrabCut считается одним из полуавтоматических методов сегментации изображений, поскольку он требует взаимодействия с пользователем для инициализации процесса сегментации. Автоматизация методики GrabCut предлагается как модификация исходной полуавтоматической, чтобы исключить взаимодействие с пользователем. Автоматический GrabCut использует неконтролируемую методику кластеризации Orchard и Bouman для фазы инициализации. Сравнение с оригинальным GrabCut показывает эффективность предложенного автоматического метода с точки зрения сегментации, качества и точности. Поскольку для каждой задачи сегментации не рекомендуется использовать явное цветовое пространство, автоматический GrabCut применяется с цветовыми пространствами RGB, HSV, CMY, XYZ и YUV.

Модели цветовых пространств

Наиболее широко используемым цветовым пространством является цветовое пространство RGB, где цветовая точка в пространстве характеризуется тремя цветовыми компонентами соответствующего пикселя: красным (R), зеленым (G) и синим (B). Однако, поскольку существует много цветовых пространств, полезно классифицировать их по меньшему количеству категорий относительно их определений и свойств. Ванденбрук[1] предложил классификацию цветовых пространств на следующие категории.

Основные пространства, основанные на теории, предполагающей, что можно сопоставить любой цвет, смешав соответствующее количество трех основных цветов - это реальный RGB, субтрактивный CMY и воображаемые основные пространства XYZ. Преобразование из RGB в CMY и из RGB в XYZ производится согласно формулам (1) и (2):

$$\begin{gathered} \mathrm{C}' = 1 - R \quad C = \min(1, \max(0, \mathrm{C}' - K')) \\ M' = 1 - G \quad M = \min(1, \max(0, M' - K')) \\ Y' = 1 - B \quad Y = \min(1, \max(0, Y' - K')) \\ K' = \min(\mathrm{C}', M', Y') \end{gathered} \tag{1}$$

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.412453 & 0.357580 & 0.180423 \\ 0.212671 & 0.715160 & 0.072169 \\ 0.019334 & 0.119193 & 0.950227 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2}$$

Рассматривая пространства яркости-цветности, которые вычисляются из одного цветового компонента, который представляет яркость, и двух цветовых компонентов, которые представляют цветность можно выделить цветовое пространство YUV. Преобразование из RGB в YUV осуществляется по формуле (3):

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.2989 & 0.5866 & 0.1145 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{3}$$

Так же существуют пространства восприятия, которые пытаются количественно оценить субъективное восприятие цвета человеком с помощью трех мер: интенсивности, оттенка и насыщенности: HSV является примером перцептивного цветового пространства. Преобразование из RGB в HSV осуществляется согласно формулам (4), (5), (6):

$$H = \begin{cases} 0, & \text{if Max} = \text{Min} \\ \left(60^{\circ} \times \dfrac{\mathrm{G} - \mathrm{B}}{\text{Max} - \text{Min}} + 360^{\circ}\right) \\ \quad \times \bmod 360^{\circ}, & \text{if Max} = \mathrm{R} \\ 60^{\circ} \times \dfrac{\mathrm{B} - \mathrm{R}}{\text{Max} - \text{Min}} + 120^{\circ}, & \text{if Max} = \mathrm{G} \\ 60^{\circ} \times \dfrac{\mathrm{R} - \mathrm{G}}{\text{Max} - \text{Min}} + 240^{\circ}, & \text{if Max} = \mathrm{B} \end{cases} \tag{4}$$

$$S = \begin{cases} 0, & \text{if max} = 0 \\ \dfrac{\text{Max} - \text{Min}}{\text{Max}} & \text{otherwise} \end{cases} \tag{5}$$

$$V = \text{Max} \tag{6}$$

Сегментация изображений с использованием GrabCut

Сегментация изображений – это простой процесс разделения изображения на переднюю и заднюю части. Метод Graph Cut [2] рассматривался как эффективный способ сегментации монохромных изображений, который основан на алгоритме Min-Cut / Max-Flow [3]. GrabCut [4] – мощное расширение алгоритма Graph Cut для итеративной сегментации цветных изображений и упрощения взаимодействия с пользователем, необходимого для заданного качества результатов сегментации. В следующем разделе объясняется исходный полуавтоматический алгоритм GrabCut, разработанный Rother et al. в [4].

Оригинальный полуавтоматический GrabCut

Алгоритм GrabCut изучает цветовые распределения переднего плана и фона, давая каждому пикселю вероятность принадлежности к кластеру других пикселей. Это можно объяснить следующим образом: для цветного изображения I рассмотрим $z = (z_1, \dots, z_n, \dots, z_N)$ количество N пикселей, где $z_i = (C_{1i}, C_{2i}, C_{3i}), i \in [1, \dots, N]$, и C_j - это j-ый компонент цвета в используемом цветовом пространстве. Сегментация определяется как массив $\alpha = (\alpha_1, \dots, \alpha_N), \alpha_i \in \{0,1\}$, присваивающий каждому пикселю изображения метку, указывающую, принадлежит ли он фону или переднему плану. Алгоритм GrabCut состоит в основном из двух основных шагов: инициализации и итеративной минимизации.

Инициализация при помощи GrabCut.

Новизна метода GrabCut заключается в «неполной маркировке», которая позволяет снизить степень взаимодействия с пользователем. Взаимодействие с пользователем заключается в простом указании только пикселей фона путем перетаскивания прямоугольника вокруг желаемого объекта переднего плана (рис.).

(а) (б)

Рисунок. Пример сегментации GrabCut. (а) GrabCut позволяет пользователю перетаскивать прямоугольник вокруг интересующего объекта, который нужно сегментировать. (б) Сегментированный объект

Заключение.

В этой статье была рассмотрена модификация GrabCut, которая устраняет необходимость первоначального взаимодействия с пользователем для управления сегментацией и, следовательно, преобразования GrabCut в метод автоматической сегментации. Модификация включает использование методов неконтролируемой кластеризации для инициализации процесса сегментации GrabCut. Эксперименты показали, что автоматический GrabCut с использованием кластеризации превосходит исходный GrabCut. Это снижает необходимость вмешательства пользователя при сегментации и добавляет дополнительные преимущества GrabCut за счет автоматизации. Кроме того, он обеспечивает надежную и точную сегментацию со средней частотой ошибок 3,64% по сравнению со средней частотой ошибок 4,28%, достигнутой оригинальным GrabCut. Кроме того, производительность автоматического GrabCut оценивается с использованием пяти различных цветовых пространств: RGB, YUV, HSV, XYZ и CMY. Результаты экспериментов показывают, что результаты сегментации в зависимости от цветового пространства RGB обеспечили лучшие результаты сегментации по сравнению с другими цветовыми пространствами.

Список используемых источников

1. Vandenbroucke N., Macaire L., and Postaire J.-G., “Color image segmentation by pixel classification in an adapted hybrid color space. Application to soccer image analysis // ” *Computer Vision and Image Understanding*, vol. 90, no. 2, pp. 190–216, 2003.

2. Boykov Y. Y. and Jolly M.-P., “Interactive graph cuts for optimal boundary & region segmentation of objects in N-D images,” in *Proceedings of the 8th International Conference on Computer Vision (ICCV '01)*, vol. 1, pp. 105–112, IEEE, Vancouver, Canada, July 2001.

3. Boykov Y. and Kolmogorov V., “An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 26, no. 9, pp. 1124–1137, 2004.

4. Rother C., Kolmogorov V., and Blake A., “GrabCut”: interactive foreground extraction using iterated graph cuts,” *ACM Transactions on Graphics*, vol. 23, no. 3, pp. 309–314, 2004.

Статья представлена старшим научным сотрудником НИО-3 НИЦ ВАС, кандидатом технических наук, доцентом В. А. Мешалкиным.

УДК 519.711.2
ГРНТИ 28.23.29

ОПЫТ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОЙ ЛАБОРАТОРИИ ДЛЯ ОНТОЛОГИЧЕСКОГО АНАЛИЗА ДАННЫХ

В. А. Семенова

Самарский государственный технический университет
Самарский ФИЦ РАН, Институт проблем управления сложными системами РАН

Онтологии являются одной из ведущих парадигм структурирования информационного контента. Преимуществом их использования в качестве средства познания является системный подход к изучению предметной области. Поэтому актуальна разработка методов и средств конструирования онтологий, в частности, автоматический вывод онтологий из данных.

объектно-признаковые данные, онтологический анализ, программное приложение.

В ИПУСС РАН разрабатывается программная лаборатория OntoWorker, которая реализует расширенную методологию вывода формальных понятий и строит формальные онтологии предметных областей (ПрО), представленных объектно-признаковыми данными [1]. Конкурентоспособность OntoWorker среди имеющихся средств бикластеризации объектно-признаковых данных [2, 3] обеспечивается:

- Обобщенным представлением исходных данных, отражающим реалии накопления эмпирической информации (наличие в общем случае нескольких серий измерений свойств для каждого попавшего в обучающую выборку объекта ПрО, наличие конкурирующих процедур измерения одного и того же свойства, учет достоверности серий измерений и степеней доверия к процедурам измерения и др.);
- Эффективным механизмом обработки данных о произвольных неоднородных отношениях между объектами исследуемой ПрО [4];
- Использованием при обработке данных многозначной векторной логики [5], позволяющей иметь адекватную оценку истинности базовых семантических суждений (БСС) о ПрО вида «объекту g присуще свойство m»;
- Учетом при анализе данных априорных ограничений существования свойств (ОСС) [6];
- Построением онтологии с редукцией множества понятий до конструктивно определяемых классов объектов ПрО с целью реализации объектно-ориентированного подхода при создании компьютерных ресурсов.

Представим возможности OntoWorker на примере анализа данных о сортах мягкой яровой пшеницы [7, 8].

Для иллюстрации этих возможностей модифицируем и расширим демонстрационный пример из [7] следующим образом:

- вместо измеряемого свойства «в госреестре» будем рассматривать «госреестр» как объект исследуемой ПрО. Множество измеряемых свойств пополним сопряженной парой свойств-валентностей [4] «включает»-«включен» для отражения включения ряда сортов пшеницы в госреестр;
- отражая соответствие рассматриваемых сортов пшеницы в части содержания белка классам мягкой пшеницы по ГОСТ [9], реконструируем распределение сортов пшеницы по классам. В примере это приведет, во-первых, к расширению состава соответствующих свойств (для представления всех классов пшеницы по ГОСТ), а, во-вторых, к неопределенности отнесения рассматриваемых сортов пшеницы к гостовским классам. При этом будем придерживаться той точки зрения, что в действительности сорт пшеницы должен быть отнесен к одному и только одному классу. Т. е. свойства, описывающие характеризующий класс, считаем несовместимыми, представляя гостовскую номинальную шкалу для измерения содержания в зерне белка. Информацию о принадлежности сортов пшеницы из [9] детализируем в форме различных степеней принадлежности сортов пшеницы к классам ГОСТ. Поскольку в [9] приведен лишь диапазон величины содержания белка в зерне, то разумно рассчитать искомую степень принадлежности при условии равномерного распределения зерновой массы по указанным диапазонам.

Эмпирические данные о рассматриваемых сортах пшеницы представляются в виде обобщенной таблицы «объекты-свойства» (ОТОС), скриншот которой дан на рис. 1 (None соответствует ложному БСС). При этом сведения о системе измеряемых свойств (СИС) – множестве измеряемых свойств с заданным на нем ограничениями существования – вводятся в форме таблицы соответствия «пара сопряженных свойств – члены пары».

OntoWorker преобразует ОТОС в исходный формальный контекст (ИФК), где измерения заменяются совокупностью оценок истинности БСС, а СИС представляется в виде совокупности пересекающихся субструктур – групп свойств, однородных по характеру экзистенционального сопряжения свойств-членов:

- в ВЗО-группе все свойства взаимообусловлены;
- в О-группе одна ВЗО-группа свойств обусловливает другую ВЗО-группу свойств;
- в Н-группе все составляющие ее ВЗО-группы попарно несовместимы.

На основе ИФК OntoWorker формирует рабочий формальный контекст (РФК), исключая заведомо ложные БСС, а все оставшиеся признавая истинными.

Заданная обобщенная таблица "объекты-свойства" - ОТОС:														
			p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_10	p_11	p_12	p	p_13
			100	100	100	100	100	100	100	100	100	100	100	100	100
			з/устойчив	высоко з/устойчив	экстремально з/устойчив	достаточно устойчив к БР	устойчив к БР	иммунитет к БР	5-й класс (белок < 10)	4-й класс (10 <= белок < 12)	3-й класс (12 <= белок < 13,5)	2-й класс (13,5 <= белок < 14,5)	1-й класс (белок >= 14,5)	включен	включает
s	100	Жигулевская	X	X	None	X	None	None	None	None	None	<20; 0>	<80; 0>	X	None
s_2	100	Самсар	X	None	None	X	None	None	None	None	None	<49; 0>	<51; 0>	X	None
s_3	100	Тулайковская 5	X	None	None	X	X	X	None	None	None	None	<100; 0>	X	None
s_4	100	Тулайковская 10	X	X	None	X	X	X	None	None	None	None	<100; 0>	X	None
s_5	100	Тулайковская 100	X	X	None	X	X	X	None	None	None	<20; 0>	<80; 0>	X	None
s_6	100	Тулайковская золотистая	X	X	X	X	X	X	None	None	None	None	<100; 0>	X	None
s_7	100	Экада 70	X	None	None	X	None	None	None	None	None	None	<100; 0>	X	None
s_8	100	Экада 66	X	None	None	X	None	None	None	None	None	None	<100; 0>	X	None
s_9	100	Тулайковская 110	X	X	None	X	X	None	None	None	None	None	<100; 0>	X	None
s_10	100	Тулайковская надежда	X	X	None	X	X	None	None	None	<75; 0>	<25; 0>	None	X	None
s_11	100	Тулайковская победа	X	X	None	X	X	None	None	None	None	<25; 0>	<75; 0>	None	None
s_12	100	Тулайковская 116	X	X	X	X	X	None	None	None	None	<17; 0>	<83; 0>	None	None
s_13	100	Экада 214	X	None	None	X	X	None	None	None	<55; 0>	<45; 0>	None	None	None
s_14	100	Зауральская волна	X	None	None	X	None	None	None	None	None	None	<100; 0>	None	None
s_15	100	госреестр	None	None	None	None	None	None	None	None	None	None	None	None	X

Рис. 1. Обобщённая таблица «объекты-свойства»,
представляющая известные данные о сортах мягкой яровой пшеницы

В РФК рассматриваемого примера ОСС нарушены, т. к. некоторые сорта пшеницы оказываются отнесенными одновременно к двум классам мягкой пшеницы по ГОСТу. Для каждого исследуемого сорта пшеницы OntoWorker идентифицирует так называемые «проблемные» группы сопряженных свойств – группы, состав которых у рассматриваемого сорта свидетельствует о нарушении ОСС. Для изменения этой ситуации в OntoWorker предусмотрена возможность нормализации РФК, когда удовлетворение ОСС достигается надлежащим исключением из РФК наименее достоверной эмпирической информации [10].

Из РФК выводятся формальные понятия (можно получит индексы их поддержки и устойчивости), строится решетка формальных понятий, а также её транзитивная редукция.

В OntoWorker реализован новый метод редуцирования множества формальных понятий и заданного на нем отношения обобщения, ориентированный на эффективную компьютерную реализацию концептуального описания ПрО в рамках объектно-ориентированного подхода. Учитывается, что описание классов, сопоставляемых формальным понятиям с пустым оригинальным объемом и пустым отличительным содержанием, оказывается сугубо формальным и может быть исключено путем надлежащей перестройки межклассовых связей, реализующих отношение обобщения на множестве формальных понятий. Это позволяет перейти к относительно компактной множественной иерархии (таксономии) абстрактных и *data*-классов, и именно она квалифицируется в OntoWorker как онтология ПрО.

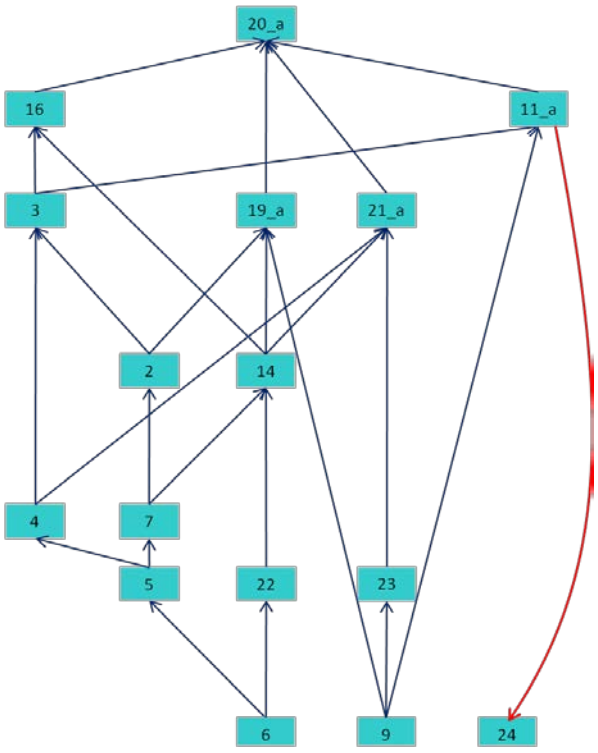


Рис. 2. Транзитивная редукция таксономии классов исследуемой предметной области (постфикс «а» цифрового имени дан у абстрактных классов)

Скриншот на рис. 2 показывает графическое изображение получаемой в рассматриваемом примере транзитивной редукции построенной таксономии классов, где изогнутая дуга описывает отношение включения сортов пшеницы в государственный реестр.

Разумеется, результаты, полученные с помощью любых инструментальных средств онтологического моделирования, в полной мере могут интерпретировать, оценить и использовать только эксперты исследуемой

предметной области, поэтому онтологический анализ данных следует проводить в сотрудничестве таких экспертов и специалистов по технологиям обработки информации. Разрабатываемая программная лаборатория предоставляет для этого богатые функциональные возможности и эргономичный пользовательский интерфейс. Программной платформой для OntoWorker служит хорошо известное и широко используемое приложение Excel [11].

Список используемых источников

1. Semenova V. A., Smirnov S. V. Extended methodology for deriving formal concepts // Journal of Physics: Conference Series 2099 (2021) 012026. pp. 1–9.

2. Ignatov D. I. Introduction to Formal Concept Analysis and Its Applications Information Retrieval and Related Fields // In: P. Braslavski, N. Karpov, M. Worring, Y. Volkovich, D. I. Ignatov (Eds.): Information Retrieval. Revised Selected Papers 8th Russian Summer School, 2014 (Nizhniy Novgorod, Russia, August 18-22, 2014). Springer Int. Publ., 2015. pp. 42–141.

3. Ferré S., Huchard M., Kaytoue M., Kuznetsov S. O., Napoli A. Formal Concept Analysis: From Knowledge Discovery to Knowledge Processing // In: P Marquis, O Papini, H Prade (eds.): A Guided Tour of Artificial Intelligence Research. Vol. II: AI Algorithms. Springer International Publishing, 2020. pp. 411–445.

4. Смирнов С. В. Построение онтологий предметных областей со структурными отношениями на основе анализа формальных понятий // Знания – Онтологии – Теории: Материалы Всерос. конф. с международным участием (3–5 октября 2011 г., Новосибирск, Россия). Т. 2. Новосибирск: Институт математики СО РАН, 2011. С. 103–112.

5. Аршинский Л. В. Векторные логики: основания, концепции, модели. Иркутск: Иркутский гос. ун-т, 2007. 228 с.

6. Lammari N., Metais E. Building and maintaining ontologies: a set of algorithms // Data & Knowledge Engineering. 2004. Vol. 48 (2). pp. 155–176.

7. Семенова В. А. Опыт бикластеризации данных о сортах сельскохозяйственных культур // Известия Самарского научного центра РАН. 2020. Т. 22, № 1. С. 86–92.

8. Каталог инновационных разработок Самарского НИИ сельского хозяйства имени Н. М. Тулайкова на 2018 год / под ред. С. Н. Шевченко. Самара: Изд-во СамНЦ РАН, 2018. 92 с.

9. ГОСТ 9353-2016 Пшеница. Технические условия. URL: https://pdf.standartgost.ru/catalog/Data2/1/4293751/4293751950.pdf (дата обращения: 27.12.2021).

10. Семенова В. А. Эвристика и численный метод нормализации эмпирического V^{TF}-контекста в задаче онтологического анализа данных // Информационные и математические технологии в науке и управлении. 2021. № 2 (22). С. 61–69.

11. Уокенбах Дж. Excel 2010: профессиональное программирование на VBA. М.: ООО «Вильямс», 2011. 944 с.

Статья представлена научным руководителем,
доктором технических наук, профессором С. В. Смирновым.

УДК 004.021
ГРНТИ 82.33.13

АКТУАЛЬНОСТЬ ФОРМАЛИЗАЦИИ И РАЗРАБОТКИ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ПОДДЕРЖКИ ТВОРЧЕСКИХ ПРОЦЕССОВ

Ю. А. Торшенко, В. П. Юрманова

Санкт-Петербургский университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием цифровой среды автоматизация процессов приобретает всю большую актуальность, появляется спрос на средства поддержания профессиональной деятельности творческих работников. Для создания подобных продуктов необходимо формализовать все этапы жизненного цикла произведения.

формализация, автоматизация, творческие компетенции.

За последние десятилетия формализация и автоматизация процессов стали неотъемлемой частью целого ряда технологий, изначально не связанных с информатикой. Это является следствием не только стремления к сокращению затрат как материальных, так и, главным образом, трудовых и временных, а также возрастающей потребности в снижении количества ошибок так называемого «человеческого фактора».

Современные реалии постепенного перехода к шестому технологическому этапу дали толчок к цифровизации практически всех сфер деятельности [1]. Однако общественность до сих пор склонна считать, что существуют области, не поддающиеся логико-математическому описанию, прежде всего это различные творческие активности: написание художественных текстов, стихов, создание произведений скульптурного и изобразительного искусства, музыки и т. п. В то время как непосредственный рабочий процесс художника или писателя можно без особых затруднений представить в виде типовых алгоритмов, сам толчок, побудивший его к созданию произведения, часто является понятием, плохо поддающимся объяснению даже силами самого творца.

Рассмотрим эту проблему подробнее – какими путями возникает замысел нового произведения? Для более чёткого определения границ исследуемого объекта остановимся на художественной литературе. Случаи, когда автор пишет текст на заказ или развивает некую актуальную тему, принимать во внимание не будем, их, конечно же, не стоит исключать из общей модели, но для исследования более остро стоит вопрос спонтанного вдохновения [2]. Обращаясь к самим писателям, можно установить, что сиюминутные идеи

для сюжетов чаще всего имеют вполне объяснимое происхождение: они навеяны какими-либо воспоминаниями, впечатлениями или аналогиями, проведенными автором между несколькими событиями-триггерами (рис. 1).

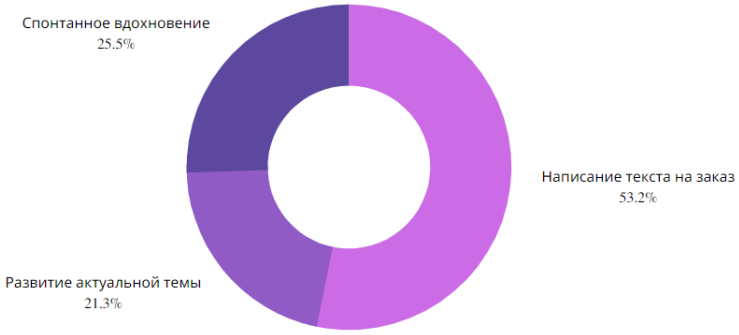


Рис. 1. Опрос – что подало идею

Несмотря на случайность фактора возникновения, формат события-триггера остается неизменным: это может быть некая ситуация, образ, эмоция или их комбинация [3, 4]. Таким образом, можно предположить, что выборка из достаточно широкой, но всё же конечной базы подобных событий при определенных настройках может прогнозируемо спровоцировать у автора стартовую идею для сюжета произведения или его части. Эту гипотезу подтверждает тот факт, что с развитием информационной среды, появляется всё больше информационных инструментов, помогающих писателю не только распланировать свой рабочий процесс, но и спровоцировать состояние вдохновлённости.

Для определения наиболее популярных сервисов, способствующих повышению творческих компетенций, среди сетевых писателей (217 человек) был проведён опрос. Его результаты представлены на рис. 2.

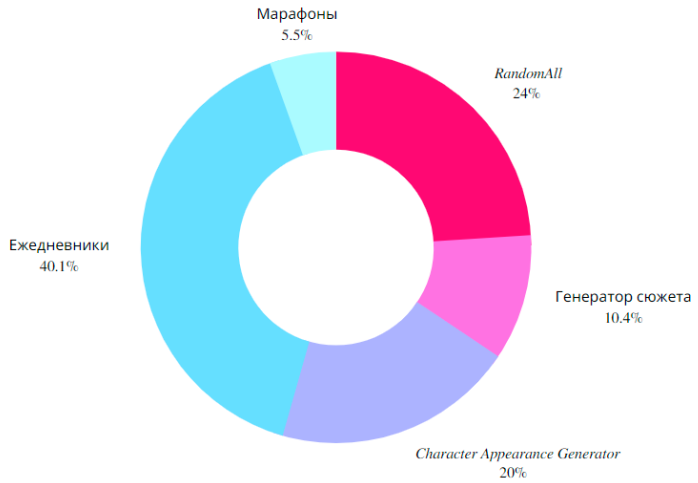


Рис. 2. Опрос – способы повышения творческих компетенций

Самым популярным способом поддержки писательского навыка пока остаётся ежедневник, который можно вести как в традиционном формате, так и в электронном. В ежедневниках визуализируется прогресс. Данные отметки добавляют мотивации работать больше. Но многие пользователи периодически забывают отмечать прогресс, поэтому зачастую ежедневники быстро становятся ненужными, что приводит к резкой потере мотивации.

Вторым по популярности оказался сервис *RandomAll* (*https://randomall.ru*), на котором можно сгенерировать всё, что необходимо для написания сюжета истории или создания персонажа для своей собственной вселенной. Принцип работы данного генератора – пользователи или сам создатель сайта придумывают идеи, а генератор случайным образом выбирает одну из идей и предлагает её тому, кто воспользовался тем или иным генератором.

Третьим по популярности является генератор *Character Appearance Generator*, который случайным образом генерирует внешность и физическое описание персонажа.

Следующий по популярности – генератор сюжета (*https://litgenerator.ru/*). Данный генератор не прописывает идею полностью, только подталкивает к придумыванию своей собственной истории.

Еще одним способом является марафон. Марафоны обычно проводятся в течение месяца. Для определённого промежутка задаётся определённая тематика. В этот период необходимо поделиться своей работой в социальных сетях, так как соревновательный момент повышает мотивацию участников работать дальше.

Если писательский ежедневник – довольно традиционный инструмент, имевший широкое распространение еще в середине двадцатого века, то марафоны совместного творчества начали активно развиваться после 1999 года, а различного рода генераторы стали доступны начиная с 2015-2017 годов. Таким образом, за последние пять лет наблюдается довольно резкий подъем популярности, до 54 %, принципиально нового типа средств поддержки творческого процесса, что позволяет говорить о востребованности именно инструментов генерации идей.

Возросший спрос на подобные средства обусловлен не только интересом к новым технологиям, но и действительными потребностями авторов. В нестабильное кризисное время эмоциональный фон людей творческих страдает особенно ощутимо, что сказывается на их продуктивности, и если на технологических этапах творчества это можно почти беззатратно нивелировать более строгим подходом к составлению расписаний и распределению рабочего времени, то на старте создания произведения этот вопрос стоит наиболее остро. Следовательно, актуальность разработки автоматизированных средств поддержки рабочего процесса и повышения творческих компетенций в прогнозируемом будущем будет повышаться.

Список используемых источников

1. Птицына Л. К., Птицын А. В., Птицын Н. А., Индивидуализация и персонализация процессов формирования компетенций при подготовке кадров для сферы ИТ-технологий // Современное образование: содержание, технологии, качество. 2020. Т. 1. С. 466–468.
2. The MasterClass Staff. How to Boost Creativity and Improve Your Creative Writing. URL: https://www.masterclass.com/articles/how-to-boost-creativity-and-improve-your-creative-writing#5-tips-for-writing-more-creatively
3. Ожегов С. И. Толковый словарь русского языка: около 100 000 слов, терминов и фразеологических выражений / под общ. ред. Скворцов Л. И. 28-е изд., перераб. Москва: Мир и Образование: ОНИКС, 2012. 1375 с. ISBN 978-5-94666-657-2
4. Свидерская И. Где черпать идеи для творчества? URL: https://www.mann-ivanov-ferber.ru/sovet/gde-cherpat-idei-dlya-tvorchestva/

УДК 004.942
ГРНТИ 28.17.19

ИНФОРМАЦИОННОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЛИЦЕНЗИРОВАНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Д. В. Чуприн

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю Российской Федерации

На основе статической и технологической информационных моделей деятельности лицензирующего органа на основных этапах процесса функционирования системы лицензирования по технической защите конфиденциальной информации разработана динамическая информационная модель, определившая возможность разработки автоматизированных компонентов подсистемы принятия решений о готовности лицензирования организаций-заявителей.

лицензирование, техническая защита конфиденциальной информации, информационная модель, динамическая модель, граф, стохастическая сетевая модель.

В настоящее время деятельность системы лицензирования ФСТЭК России в области защиты информации обусловлена расширением перечня и содержания лицензируемых видов деятельности [1-8]. Увеличи-

лось количество запросов организаций-заявителей на предоставление, продление, переоформление лицензий и проведение специальных экспертиз. Значительно обновилась законодательная и нормативная методическая база, регламентирующая организацию и порядок осуществления лицензионной деятельности по технической защите конфиденциальной информации (ТЗКИ).

Таким образом, возникла необходимость создания ИС лицензирования ФСТЭК России, обеспечивающей внедрение информационных технологий на всех этапах деятельности лицензирующего органа. В рамках решения задачи по созданию и развитию указанной ИС было проведено информационное моделирование процессов функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей.

Разработанная модель процесса функционирования системы лицензирования представляет собой совокупность моделей деятельности лицензирующего органа и обеспечивает оценку эффективности лицензирования с учетом основных видов показателей, определенных Методикой проведения мониторинга эффективности лицензирования [9].

С использованием модели процесса функционирования системы лицензирования становится возможным:

– определить показатели оценки альтернативных вариантов создания и развития ИС лицензирования в части разработки подсистемы принятия решения о готовности лицензирования организаций-заявителей;

– сформировать альтернативные варианты направлений создания и развития ИС лицензирования в части разработки подсистемы принятия решения о готовности лицензирования организаций-заявителей;

– выбрать из сформированных альтернативных вариантов наиболее приоритетные.

Разработаны модели деятельности лицензирующего органа на основных этапах процесса функционирования системы лицензирования, содержащие статическую, технологическую и динамическую информационные модели.

Статическая (описательная) информационная модель подсистемы принятия решения о готовности лицензирования организаций-заявителей отражает ее роль и место в системе лицензирования ФСТЭК России, возложенные на нее задачи и функции, состав используемых средств автоматизации и связи, а также внутренние и внешние потоки информации.

Технологическая (алгоритмическая) информационная модель подсистемы принятия решения о готовности лицензирования организаций-заявителей отражает порядок (последовательность) выполнения возложенных на нее функций и задач, порядок формирования одних элементов форм представления данных из других, методы (правила) автоматизированного выполнения (решения) функций и задач.

Динамическая (аналитическая) информационная модель подсистемы принятия решения о готовности лицензирования организаций-заявителей – это стохастическая сетевая модель ее функционирования [10]. Она построена при помощи системы моделирования, описанной в [11], и позволяет моделировать динамику изменения состояний процессов обработки, преобразования, хранения и передачи информации путем подачи на ее вход значений характеристик информационного состава и структуры подсистемы принятия решения о готовности лицензирования организаций-заявителей и на этой основе определять вероятностно-временные характеристики процессов выполнения возложенных на нее функций и задач, а также значения информационной нагрузки средств автоматизации и связи.

Основные условия моделирования характеризуются следующим.

Время моделирования задается равным 2 000 часам рабочего времени в году.

Разработаны ориентированные взвешенные графы, отражающие логические схемы выполнения элементами подсистемы принятия решения о готовности лицензирования организаций-заявителей действий (работ) по обработке, преобразованию, хранению и передаче информации в рамках основных процессов функционирования системы, первый из которых представлен на рисунке.

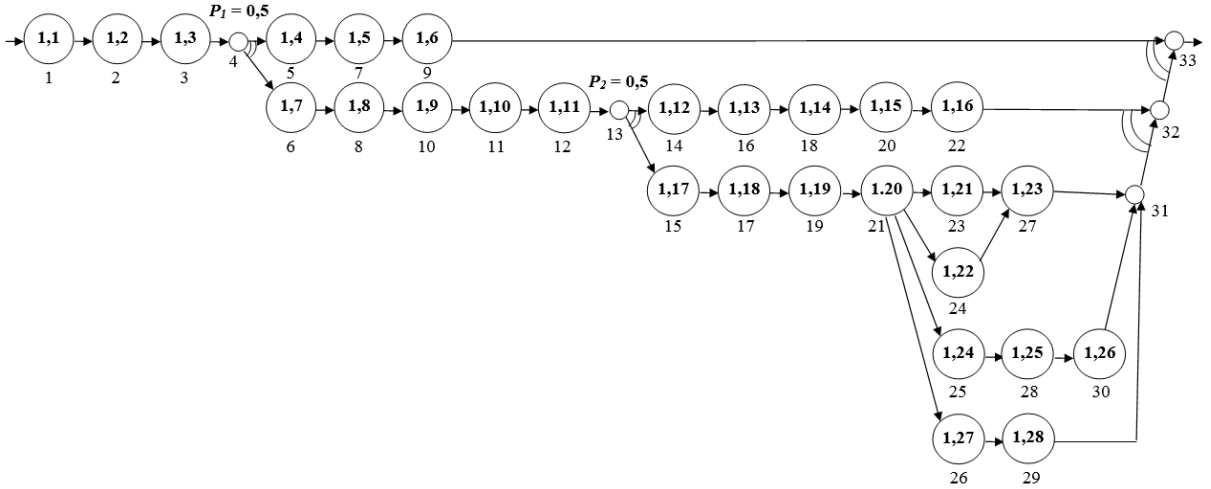


Рисунок. Граф, отражающий предоставление или продление лицензии, либо отказ в предоставлении или продлении лицензии по ТЗКИ

Вершинам графов соответствуют действия (работы) по обработке, преобразованию, хранению и передаче информации, а дугам – отношения последовательности выполнения этих действий (работ).

Вершины графа на рисунке взвешены двумя весами, первый из которых определяет условный номер действия (работы), а второй – элемент подсистемы принятия решения о готовности лицензирования организаций-заявителей (должностные лица, ПЭВМ, автоматизированные рабочие места,

средства связи и обмена данными и т. п.), ответственный за выполнение этого действия (работы) по обработке, преобразованию, хранению и передаче информации.

Каждому графу, описывающему конкретный *k*-й процесс функционирования системы, поставлены в соответствие периодичность выполнения процесса N_k и требуемое время выполнения процесса $T_k^{треб}$.

Здесь индексы *k* соответствуют условным номерам процессов функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей:

k = 1 – предоставление (продление) лицензии или отказ в предоставлении (продлении) лицензии по ТЗКИ;

k = 2 – переоформление лицензии или отказ в переоформлении лицензии по ТЗКИ;

k = 3 – предоставление дубликата (копии) лицензии по ТЗКИ;

k = 4 – приостановление лицензии по ТЗКИ;

k = 5 – возобновление действия лицензии по ТЗКИ;

k = 6 – аннулирование лицензии по ТЗКИ;

k = 7 – прекращение действия лицензии;

k = 8 – выдача сведений по конкретной лицензии (предоставление информации из реестра лицензий) по ТЗКИ;

k = 9 – информирование о порядке исполнения государственных услуг по лицензированию деятельности по ТЗКИ;

k = 10 – консультирование о порядке исполнения государственных услуг по лицензированию деятельности по ТЗКИ;

k = 11 – контроль соблюдения лицензионных требований и условий по ТЗКИ.

Периодичности выполнения процессов N_k задавались регулярными законами распределения с соответствующими параметрами n_k, принимающими следующие значения: n_1 = 60 час.; n_2 = 20 час.; n_3 = 250 час.; n_4 = 650 час.; n_5 = 700 час.; n_6 = 900 час.; n_7 = 200 час.; n_8 = 10 час.; n_9 = 15 час.; n_{10} = 40 час.; n_{11} = 1 час. Указанные значения n_k выбраны такими для того, чтобы в течение моделируемого времени, с одной стороны, все моделируемые процессы функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей были выполнены, по крайней мере, один раз, а с другой стороны, в максимальной степени соответствовали реальной средней интенсивности возникновения потребности в их выполнении.

Требуемое время выполнения процессов определялось следующими значениями: $T_1^{треб}$ = 170 час.; $T_2^{треб}$ = 140 час.; $T_3^{треб}$ = 104 час.; $T_4^{треб}$ = 64 час.; $T_5^{треб}$ = 64 час.; $T_6^{треб}$ = 64 час.; $T_7^{треб}$ = 64 час.; $T_8^{треб}$ = 64 час.; $T_9^{треб}$ = 160 час.; $T_{10}^{треб}$ = 320 час.; $T_{11}^{треб}$ = 200 час.

Моделирование осуществлялось без «отказов» [11] элементов подсистемы принятия решения о готовности лицензирования организаций-заявителей.

Анализ и обобщение результатов проведенных имитационных экспериментов позволили заключить следующее.

1. При принятых условиях моделирования автоматизация основных процессов функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей сокращала время их выполнения в 1,5–6 раз. При этом вероятность выполнения за требуемое время практически всех процессов составляла 0,8–1.

2. Длительности 1–3 процессов, являющихся критическими («узким местом») для функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей, в различной степени зависят от длительностей выполнения функций (задач) по поиску информации, принятию решений и обмену данными. Сокращение времени выполнения функций (задач) по поиску информации и принятию решений в большей степени влияет на длительности выполнения этих процессов, чем сокращение времени выполнения функций (задач) по обмену данными. При этом существенное сокращение длительности выполнения процессов функционирования подсистемы принятия решения о готовности лицензирования организаций-заявителей наблюдается при уменьшении времени выполнения функций (задач) по обмену данными, начиная со значения, равного 20 минутам.

Список используемых источников

1. Постановление Правительства Российской Федерации от 3 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации» : офиц. текст предоставлен КонсультантПлюс. 8 с.

2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» : офиц. текст предоставлен КонсультантПлюс. 10 с.

3. Положение о государственном лицензировании деятельности в области защиты информации, утвержденное совместным решением Гостехкомиссии России от 24.04.1994 № 10 и ФАПСИ России от 24.06.1997 № 60.

4. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» : офиц. текст предоставлен КонсультантПлюс. 20 с.

5. Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» : офиц. текст предоставлен КонсультантПлюс. 48 с.

6. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государствен-

ную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» : офиц. текст предоставлен КонсультантПлюс. 9 с.

7. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» : офиц. текст предоставлен КонсультантПлюс. 12 с.

8. Приказ Федеральной службы по техническому и экспортному контролю от 17 июля 2017 г. № 134 «Об утверждении административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» : офиц. текст предоставлен КонсультантПлюс. 54 с.

9. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 467 «О подготовке и представлении докладов о лицензировании отдельных видов деятельности, показателях мониторинга эффективности лицензирования и методике его проведения» : офиц. текст предоставлен КонсультантПлюс. 9 с.

10. Емельянов А. А. Стохастические сетевые модели массового обслуживания // Прикладная информатика. 2009. № 5 (23). С. 103–111.

11. Бакумов В. В., Гречишников В. И. Имитационная модель функционирования системы управления предприятием // Телекоммуникации. 2001. № 11. С. 19–24.

Статья представлена научным руководителем,
доктором технических наук, с. н. с. А. В. Анищенко.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ И СИСТЕМ СВЯЗИ

УДК 533.9.072
ГРНТИ 29.27.43

ВЧ-ГЕНЕРАТОР ВОДОРОДНОЙ ПЛАЗМЫ ДЛЯ ВЫСОКОВАКУУМНЫХ УСТАНОВОК

В. Н. Алимов, А. О. Буснюк, С. Р. Кузенов, А. И. Лившиц, Е. Ю. Передистов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлен портативный генератор низкотемпературной водородной плазмы для установки «СУПМЕМ-1» по исследованию сверхпроницаемости по водороду металлических мембран. Ионизация молекулярного водорода происходит с помощью ВЧ-индукционного разряда низкого давления. Ожидается, что представленная модель генератора позволит получить портативный источник водородной плазмы для высоковакуумного оборудования.

ВЧ газовый разряд низкого давления, высоковакуумное оборудование.

Сверхпроницаемые металлические мембраны по водороду способны решить проблему прямого внутреннего рециклинга D/T топлива в современных установках управляемого термоядерного синтеза типа Токамак.

Металлические мембраны макроскопической толщиной 100–200 мкм могут быть сверхпроницаемы для водородных частиц (атомов, ионов), если их энергия (кинетическая, химическая или внутренняя) превышает ~ 1 eV. Это означает, что практически весь падающий поток надтепловых водородных частиц проходит сквозь мембрану независимо от её толщины и температуры. Металлические мембраны практически непроницаемы для любых других газов, включая He, а также для обычных тепловых молекул водорода (H2, D2, T2) и способны автоматически сжимать проникающий водород на порядки величины.

Для достижения вероятности проникновения атомарного водорода через металлическую мембрану близкой к 1, на входной стороне металлической мембраны должно иметься монослойное покрытие из неметалла с высоким энергетическим барьером [1–4]. Экспериментально было обнаружено, что самый высокий энергетический барьер имеет монослойное покрытие из серы на атомарно-чистой поверхности металлов [5, 6].

Один из способов получения адсорбционных слоев из серы – пиролиз сероводорода на предварительно очищенной поверхности. Контроль осаждения неметаллических примесей на очищенную поверхность металла можно найти в работах [6, 7].

Целью данной работы было создание портативного устройства, способного путем ионизации молекулярного водорода синтезировать сероводород из кристаллической серы для исследования явления сверхпроницаемости металлических мембран по водороду.

ВЧ генератор низкотемпературной водородной плазмы для синтеза сероводорода

Сероводород планируется получать с помощью ВЧ индукционного разряда низкого давления, в котором разрядным газом является молекулярный водород, а реагентом кристаллическая сера. Мы выбрали данный способ синтеза сероводорода по нескольким причинам.

Во-первых, для эксперимента по осаждению серы требуется H2S в количестве не более 10 см^3 при нормальных условиях. Использование баллонов со сжатым сероводородом представляется нецелесообразным для проведения эксперимента по осаждению серы в лаборатории ВУЗа из-за опасности утечки газа и его крайне токсичным эффектом (ГОСТ 22387.2-2014) Во-вторых, индукционный ВЧ-разряд низкого давления обладает рядом достоинств: возможность получения высокой концентрации электронов при относительно невысоком уровне подводимой ВЧ-мощности, отсутствие контакта плазмы с металлическим электродами, низкий потенциал плазмы относительно стенок, ограничивающих разряд из-за относительно небольшой температуры электронов [8] и высокая реакционная способность паров серы вступать во взаимодействие с ионизированными газами.

В-третьих, индукционный ВЧ-разряд низкого давления с успехом используется более полувека в наукоемких технологиях микроэлектроники [9] и в космической промышленности [10] и этот факт говорит о высокой надежности и эффективности данного способа получения низкотемпературной плазмы.

В условиях работы металлических мембраны при сверхвысоком вакууме недопустимым является наличие течей в тракте напуска H2/H2S, поэтому мы не рассматривали химический способ получения сероводорода путем взаимодействия сульфида железа с сильными кислотами, поскольку

планируется синтезировать H2S при отсутствии посторонних газов, в т.ч. поступающих из атмосферного воздуха. Также мы не рассматривали термический способ получения H2S из-за крайне малого выхода сероводорода указанным способом при большом расходе H2, что также является недопустимым с точки зрения безопасности проведения эксперимента в лаборатории вуза [11].

Описание ВЧ-генератора низкотемпературной водородной плазмы

Генератор плазмы состоит из разрядной части, в которую входят разрядная камера и ВЧ индуктор (ВЧИ) и ВЧ тракта генерации, включающего генератор ВЧ сигналов, усилитель сигналов и линии передачи и согласования ВЧ сигнала с ВЧИ. Схема тракта генерации и передачи ВЧ сигнала представлена на рис. 1.

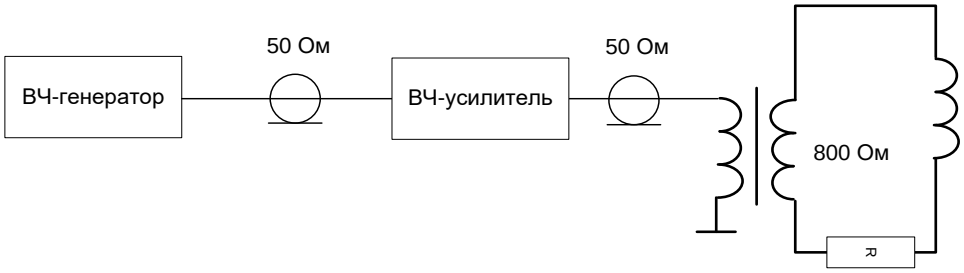


Рис. 1. Радиотехническая схема ВЧ генератора плазмы

В качестве задающего генератора был использован коммерчески доступный лабораторный генератор MHS-5200A, способный синтезировать сигналы синусоидальной формы частотой до 25 МГц и значениями тока и напряжения 50 мА и 20 В на выходе. ВЧ сигнал от генератора поступает на транзисторный усилитель по коаксиальному кабелю, усиленный до 10–15 А сигнал на выходе усилителя поступает на симметрирующий трансформатор с ферриторым сердечником, согласовывающий характеристические сопротивления ВЧ индуктора и коаксиальной линии на частоте 13.56 МГц.

Разрядная камера выполнена из молибденового стекла, являющегося диэлектриком и данный материал прозрачен для ВЧ-сигналов. Молибденовое стекло герметично соединяется с молибденовой частью камеры, которая в свою очередь с помощью сварки соединяется с конструкционной частью, выполненной из стали марки 12Х18Н10Т. Также из стали марки 12Х18Н10Т выполнены коммуникации напуска H2 и удаления H2S из разрядной камеры, выбор материала обусловлен низкой коррозионной активность по отношению к сернистым газам (ГОСТ Р 53678-2009). Камера с трубопроводными коммуникациями соединяется с помощью фланца Conflat. На рис. 2 представлен чертеж камеры, на рис. 3 схема тракта газонапуска: напуск H2 –

синтез H2S – откачка смеси H2/H2S в высоковакуумную камеру. Таким образом, камера герметично соединяется с трактом напуска H2 и с высоковакуумной камерой.

Напуск H2 в камеру осуществляется регулятором-расходомером газов производства Alicat Scientific с электронным управлением. Выпуск смеси газов из разрядной камеры происходит с помощью натекателя СНА-1. На выходе СНА-1 давление должно быть ниже и соответствовать высокому вакууму, который обеспечивается ТМН и форвакуумным насосами. Регулируя поток с помощью регулятора Alicat и натекателя СНА-1, мы можем регулировать давление в разрядной камере.

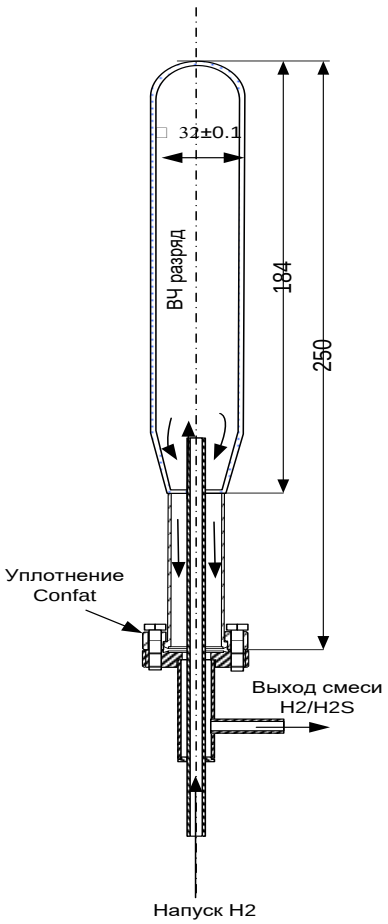


Рис. 2. Разрядная камера

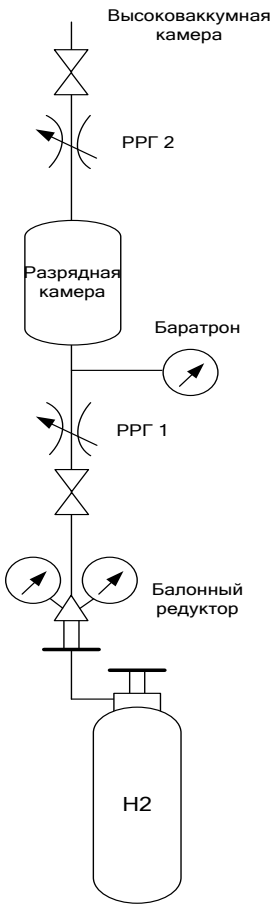


Рис. 3. Тракт напуска газов: РРГ-1 регулятор расхода газов Alicat, РРГ2-регулятор расхода газов СНА-1

Камера располагается в объеме ВЧИ, ось разрядной камеры должна совпадать с осью ВЧИ. Переменный ток, протекающий по индуктору, порождает переменное магнитное поле B, значение которого зависит от амплитуды силы тока I_0 протекающего по индуктору и его циклической частоты ω, а также от геометрии индуктора.

Переменное магнитное поле, согласно 1-му уравнению Максвелла и закону Фарадея индуцирует вихревое радиальное электрическое поле E, напряженность которого является функцией $E = f(B, r)$, где B –индукция переменного магнитного поля, r – расстояние от оси разрядной камеры (ВЧИ), причем величина поля растет пропорционально r.

Поскольку мы рассматриваем случай ВЧ разряда низкого давления, то основную роль здесь играет объёмная ионизация газа, происходящая за счёт ускорения электронов в электромагнитном поле индуктора. Ёмкостную составляющую разряда, существующую за счёт наличия паразитной

ёмкости между витками индуктор в процессе стационарной работы мы не рассматривали, поскольку расчет поля проводился при стационарном режиме работы индуктора [12].

Мы рассматриваем описание движения заряженных и нейтральных частиц в рамках статистики Максвелла-Больцмана. Для возникновения ВЧ пробоя молекулярного водорода кинетическая энергия электрона должна превышать энергию ионизации молекулы водорода. Если электрон теряет энергию после соударения, но не рекомбинирует с ионом плазмы, энергия, вкладываемая в разряд, расходуется на повторное ускорение электрона. Таким образом, в РК создается и поддерживается квазинейтральное плазменное образование.

Движение электрона в однородном переменном электрическом поле в отсутствии столкновений описывается уравнением

$$m_e \frac{d^2x}{dt^2} = -e \cdot E_0 \cdot sin\omega t, \quad (1)$$

где E_0 – амплитуда электрического поля, m_e – масса электрона, ω – циклическая частота переменного поля. В наших расчетах в качестве ω использовалась циклическая частота задающего генератора, работающего на частотах f от 1 до 25 МГц. Из уравнения (1) можно найти скорость и кинетическую энергию электрона W_e, движущегося под воздействием поля E.

При описании ударной ионизации атомов и молекул, немаловажную роль играет использование понятия сечений ионизации соответствующих атомов и молекул.

Для расчёта сечения ионизации молекулы H2 мы использовали формулу Томсона, используемую для классической теории [13]

$$\sigma_{ион} = \frac{\pi}{W_{ион}} \cdot f\left(\frac{W_e}{W_{ион}}\right), \quad (2)$$

где $W_{ион}$ – энергия ионизации молекулы водорода (15.44 эВ), W_e – кинетическая энергия налетающего электрона, f – функция ионизации. Максимум функции $\sigma_{ион}(E)$ наблюдается при значении E ≈ $3E_{ион}$, т. е. при кинетической энергии электрона равной ≈ 50 эВ. В нашем случае, с учетом размеров разрядной камеры и геометрии индуктора с заданным значением $I(f)$, с наибольшей вероятностью разряд будет гореть в пристеночной области камеры.

Другим условием достижения ВЧ разряда низкого давления является неравенство

$$\lambda_{H2} \leq r, \quad (3)$$

где λ_{H2} – длина свободного пробега молекул *H2*, r – радиус разрядной камеры. Для достижения неравенства (3) давление H2 в разрядной камере должно составлять около ≈ 10 Па при указанных выше силе тока и частоте сигнала.

Основным реагентом, участвующим в синтезе H2S, является кристаллическая сера классификации ОСЧ-15-3, которая до проведения ВЧ разряда помещается в виде порошка в разрядную камеру (ось камеры располагается горизонтально при проведении эксперимента). Давление насыщенных паров кристаллический серы составляет ≈1–10 Па при комнатной температуре и почти совпадает с давлением напускаемого в камеру H2. Давление в камере регулируется мембранно-емкостным датчиком (баратрон) фирмы Inficon, нечувствительным к сорту газов, а также устойчивым к коррозионным газам. Поскольку сера является химически активным веществом, предполагается, что вероятность синтеза H2S с ионизированным водородом будет высока, а поскольку процесс образования H2S является эндотермическим, ожидается что реакция образования H2S не будет сопровождаться заметным тепловыделением.

Список используемых источников

1. Livshits A. I. Superpermeability of Solid Membranes and Gas Evacuation // Part_I. Theory, Vacuum 29 (1979) 103.

2. Livshits A. I., Notkin M. E. and Samartsev A. A., Physico-chemical origin of superpermeability – large-scale effects of surface chemistry on “hot” hydrogen permeation and absorption in metals // J. Nucl. Mater. 170 (1990) 74.

3. Livshits A., Sube F., Notkin M., Soloviev M. and Bacal M., Plasma Driven Suprerpermeation of Hydrogen through Group Va Metals // J. Appl. Phys., 84 (1998) 2558–2564.

4. Livshits A. I., Alimov V. N., Notkin M. E. and Bacal M., Hydrogen superpermeation resistant to sputtering // Appl. Phys. Let, v. 81, #14, pp. 2656-2658, 2002

5. Hatano Y., Watanabe K., Livshits A., Busnyuk A., Alimov V., Effects of bulk impurity concentration on the reactivity of metal surface: Sticking of hydrogen molecules and atoms to polycrystalline Nb containing oxygen // Journal of Chem. Phys., 127 No. 20 (2007) 204707 1-13.

6. Дорошин А. Ю., Лившиц А. И., Самарцев А. А. Специфика взаимодействия атомов водорода с поверхностью палладия при ее пассивации адсорбционными слоями серы, Поверхность // Физика, химия, механика. 1985. № 3. С. 31–35.

7. Дорошин А. Ю. Роль поверхности в поглощении и пропускании водорода палладием: дис. ... канд. физ.-мат. наук: 01.04.07 // Ленинград, 1988. с. 100–135.

8. Кралькина Е. А. Индукционный высокочастотный разряд давления и возможности оптимизации источников плазмы на его основе // Успехи физических наук. 2008. Т. 178, № 5.

9. Hopwood J. Plasma Sources // Sci. Technol. 1.1992. 109.

10. Godyak V. A. Alexandrovich B.M., Piejak R. B., US Patent 5, 834,905 (November 19, 1998).

11. Кнунянц И. Л. и др. Химическая энциклопедия. М.: Советская энциклопедия, 1995. Т. 4. 639 с.

12.Кожевников В. В. Исследование локальных параметров плазмы в разрядной камере высокочастотного ионного двигателя малой мощности: дис. … канд. техн. наук: 05.07.05 / Кожевников Владимир Владимирович. М., 2017. 139 с.

13. Семиохин И. А. Элементарные процессы в низкотемпературной плазме. М.: Изд-во Моск. ун-та, 1988. 142 с.

УДК 621.396.67.091.1
ГРНТИ 47.45.29

ИССЛЕДОВАНИЕ ЧАСТОТНЫХ СВОЙСТВ СВЕРХШИРОКОПОЛОСНОЙ СОТОВОЙ ФРАКТАЛЬНОЙ АНТЕННОЙ СТРУКТУРЫ

Р. А. Алли, Э. Ю. Седышев, В. А. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Выполнено компьютерное моделирование антенн фрактальных структур. Проведено исследование их частотных свойств и их зависимости от способа ввода питания антенны. Проведена оптимизация согласования фрактальных структур в широкой полосе частот.

микроволновая техника, СВЧ, антенные системы, компьютерное моделирование, фрактальные антенны, сверхширокополосные антенны, широкополосные антенны.

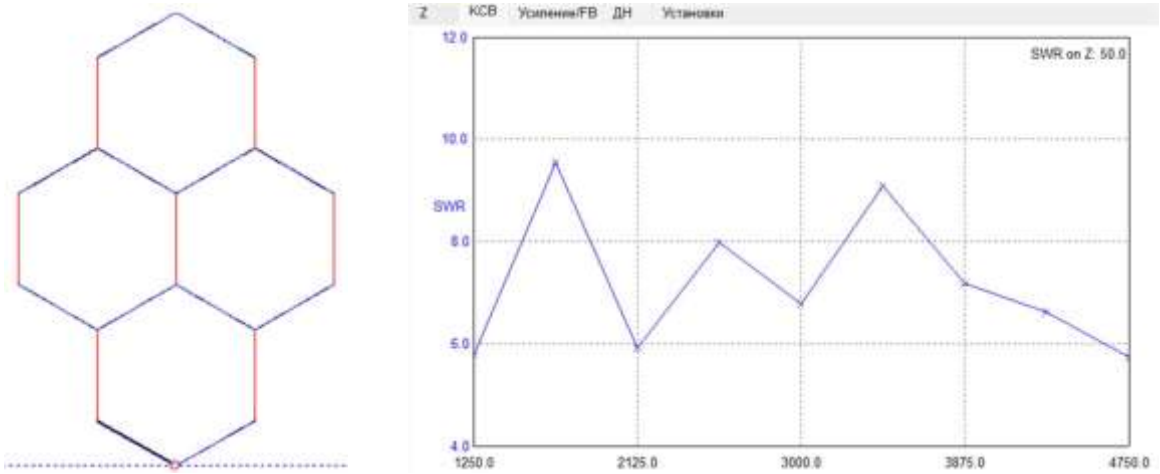
В работе был выполнен анализ сотовой фрактальной структуры.

Данная работа является продолжением исследования фрактальных структур [1, 2], целью которого является получение антенны для сбора энергии в широкой полосе частот.

Целью исследования является улучшение согласования структуры в широкой полосе частот. В ходе исследования частотных свойств антенны было проведено её компьютерное моделирование с помощью системы электромагнитного моделирования NEC. При этом не учитываются потери в материале антенны и отражение электромагнитного излучения от окружающих антенну объектов (считается, что антенна находится в безэховой камере).

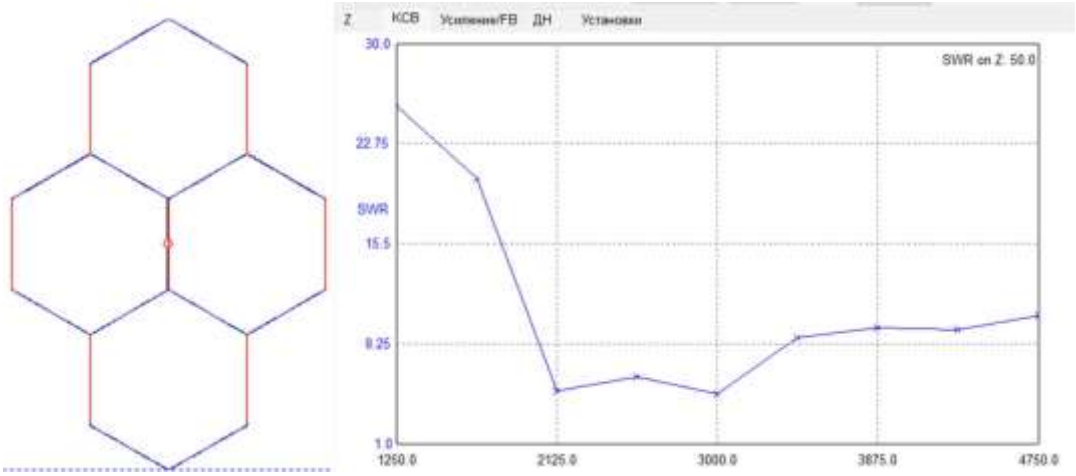
Как можно заметить из результатов анализа, частотные характеристики антенны сильно зависят от места съёма сигнала. Наилучшие результаты были достигнуты в диапазоне 2 125–3 000 МГц.

На графиках ниже (рис. 1–6) по оси x – частота в МГц, по оси y – КСВ. На рис. 1–3 компьютерное моделирование проводится при согласовании антенны на 50 Ом.



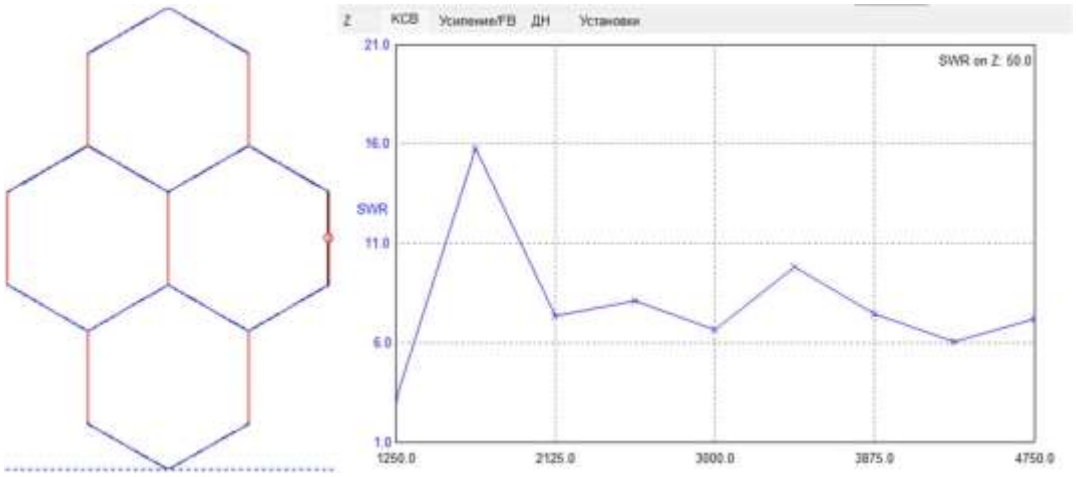
(A) (B)

Рис. 1. Сотовая фрактальная структура с питанием из угла (A)
и её КСВ в диапазоне 1 250–4 750 МГц при согласовании на 50 Ом (B)



(A) (B)

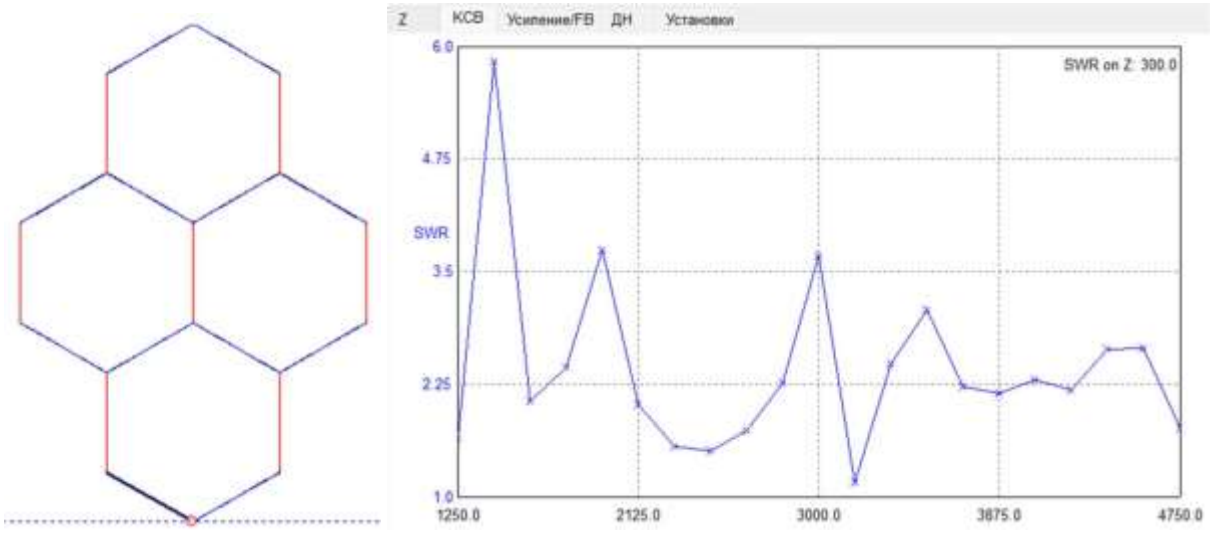
Рис. 2. Сотовая фрактальная структура с питанием из центра центрального сегмента
(A) и её КСВ в диапазоне 1 250–47 50 МГц при согласовании на 50 Ом (B)



(A) (B)

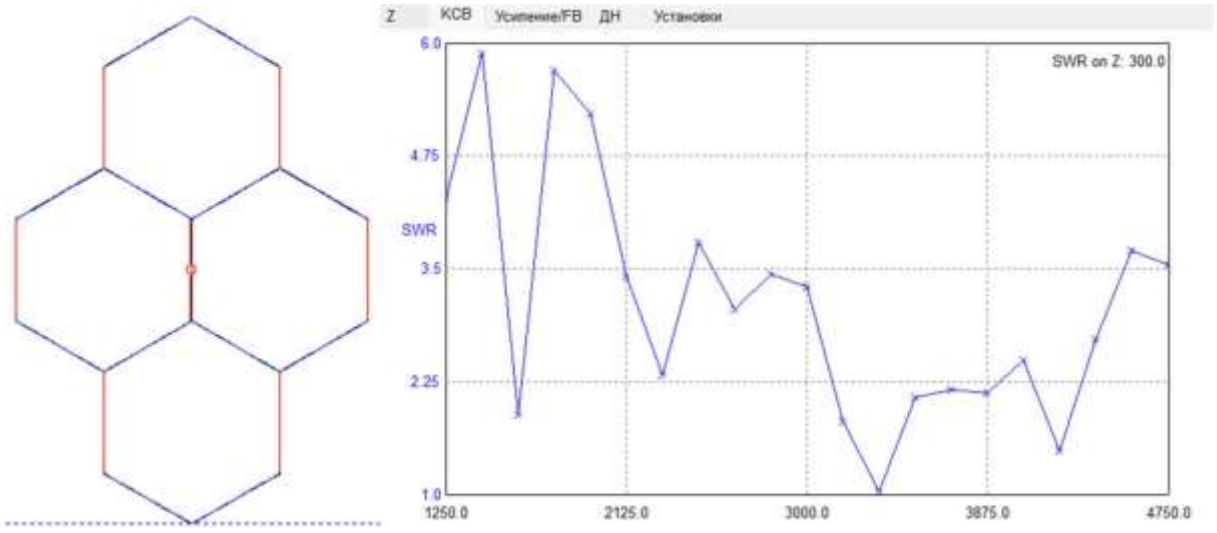
Рис. 3. Сотовая фрактальная структура с питанием из центра крайнего сегмента (A)
и её КСВ в диапазоне 1 250–4 750 МГц при согласовании на 50 Ом (B)

Компьютерное моделирование также было проведено при согласовании антенны на 300 Ом (рис. 4–6). При этом показатели КСВ значительно улучшились.



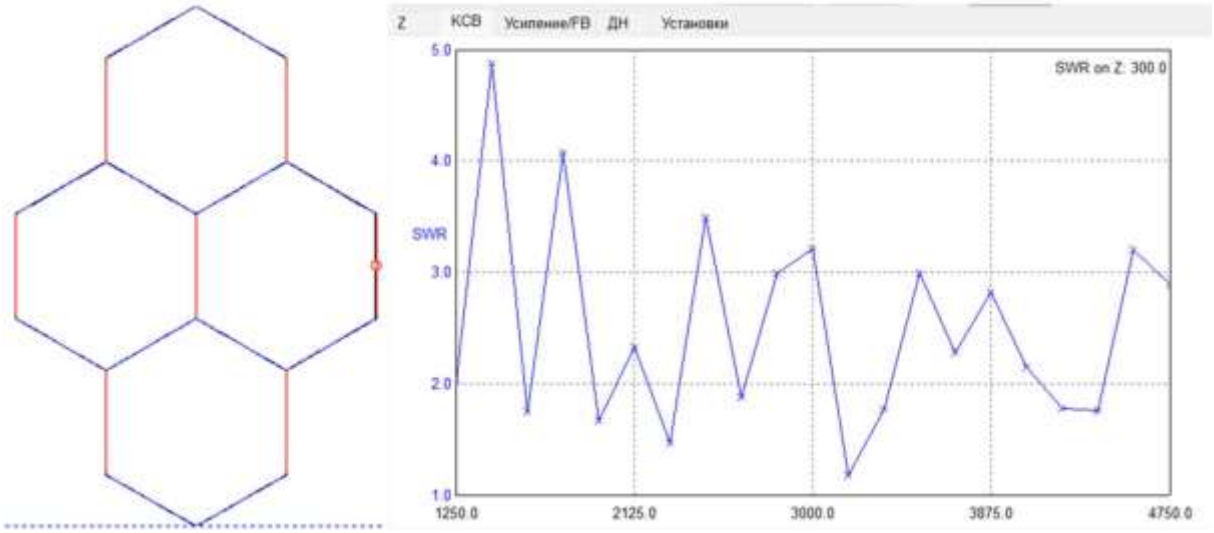
(A) (B)

Рис. 4 Сотовая фрактальная структура с питанием из угла (A)
и её КСВ в диапазоне 1 250–4 750 МГц при согласовании на 300 Ом (B)



(A) (B)

Рис. 5. Сотовая фрактальная структура с питанием из центра центрального сегмента (A)
и её КСВ в диапазоне 1250 – 4750 МГц при согласовании на 300 Ом (B)



(A) (B)

Рис. 6. Сотовая фрактальная структура с питанием из центра крайнего сегмента (А) и её КСВ в диапазоне 1250 – 4750 МГц при согласовании на 300 Ом (В)

Исходя из полученных данных, можно прийти к выводу, что питание с краю и с угла не только проще реализовать технологически, но и целесообразнее с точки зрения минимизации коэффициента стоячей волны.

Питание с угла обеспечивает наилучшее согласование в частотном диапазоне 2 125–2 800 МГц. Питание с краю обеспечивает наиболее равномерную КСВ.

В ходе данной работы было проведено компьютерное моделирование, в результате которого были исследованы частотные свойства сотовой фрактальной структуры и влияние на них способа питания антенны.

Преимуществом рассмотренной антенны является технологичность изготовления, возможность планарного исполнения, множество вариантов питания и широкополосность. Планируется макетирование антенны и исследование её частотных свойств при согласовании с детекторным СВЧ диодом AA-112A-80.

Список используемых источников

1. Алли Р. А., Седышев Э. Ю. Разработка многочастотной древовидной фрактальной антенны для ректенного преобразователя // Студенческая весна - 2021. 75-Я Юбилейная Региональная научно-техническая конференция студентов, аспирантов и молодых ученых: сб. науч. ст. СПб.: СПбГУТ, 2021. С. 65–69.

2. Алли Р. А., Седышев Э. Ю. Частотные свойства древовидных фрактальных антенн // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 444–448.

3. Воскресенский Д. И. Антенны и устройства СВЧ. Москва: Советское радио, 1972. 320 с.

4. Пименов Ю. В. Вольман В. И, Мурамцов А. Д. Техническая электродинамика. Москва: Радио и связь, 2002.

5. Фальковский О. И. Техническая электродинамика: учебник. 2-е изд. СПб.: изд-во «Лань», 2009. 432 с.

УДК 621.3.011.7
ГРНТИ 47.59

ВАРИАНТЫ ИНТЕРПРЕТАЦИИ РАЗДЕЛА «ПЕРЕХОДНЫЕ ПРОЦЕССЫ» В ТЕОРИИ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ

Ю. В. Алышев, Б. И. Николаев

Поволжский государственный университет телекоммуникаций и информатики

Рассматриваются проблемные вопросы методического обоснования переходных процессов в линейных электрических цепях. Предлагается иная интерпретация переходных процессов на основе параметрических цепей, а также внедрение соответствующих экспериментальных схем в лабораторный практикум.

переходные процессы, параметрические цепи.

При анализе переходных процессов в электрических цепях рассматривается скачкообразное изменение единственного параметра – сопротивления или проводимости резистора (ключа, работающего на замыкание или размыкание). При этом первый и второй закон коммутации оговаривают определённые условия, протекающие в реактивных элементах (ток в индуктивном элементе мгновенно измениться не может, невозможен скачок напряжения на ёмкостном элементе), хотя параметрическим элементом является не реактивный элемент (*L* или *C*), а резистор (ключ с $R = \infty/0$ – разомкнут/замкнут).

Для анализа переходных процессов используется либо операторный метод, либо классический, использующий дифференциальные уравнения [1]. Однако в некоторых примерах замыкания и размыкания получаются сложные ситуации, которые приводят к невозможности анализа подобными методами: разрыв цепи, содержащей индуктивный элемент или шунтирование ёмкостного элемента проводником, имеющим нулевое сопротивление.

В лабораторных работах переходный процесс реализуется с помощью скачкообразного входного сигнала. Однако при этом цепь остаётся линейной (не параметрической).

Цель доклада заключается в предложении другого подхода для рассмотрения переходных процессов, а именно рассматривать эти процессы как частный случай общих процессов в параметрических цепях. При этом параметрическими элементами могут выступать как реактивные элементы, так и резисторы, номиналы которых изменяются во времени. При этом скачкообразные изменения будут рассматриваться как вырожденный случай.

Исходя из этой точки зрения авторы намерены модернизировать лабораторные стенды, где можно не только изменять параметры элементов, но контролировать и управлять параметрами этого изменения.

Ниже приводятся частные случаи традиционных пояснений в учебном процессе, а также альтернативные предложения, которые, по мнению авторов, должны быть внедрены в учебный процесс.

Вводятся понятия «переходный процесс» и «установившийся» («стационарный») режим. Потом появляются требования, чтобы новый переходный процесс начинался только после того, как закончится предыдущий и схема перейдёт в установившийся режим. При этом смешиваются разнородные понятия: перепад входного напряжения (рис. 1) – и подача на вход цепи постоянного напряжения через ключ на замыкание (рис. 2).

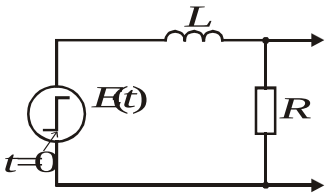


Рис. 1. Скачкообразное изменение входного напряжения во входной цепи

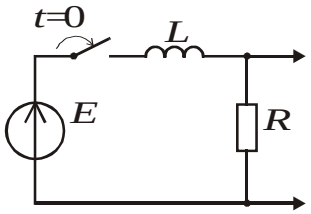


Рис. 2. Подача на вход цепи постоянного напряжения через ключ на замыкание

В первом случае мы имеем обычную линейную цепь под воздействием переменного входного напряжения. Внутреннее сопротивление источника постоянное (на схеме $R_i = 0$), и все параметры цепи постоянные.

Во втором случае мы имеем линейно-параметрическую цепь под воздействием постоянного входного напряжения. Роль параметрического резистора играет ключ.

Допустим, что в схеме рис. 2 закончился переходный процесс и наступил стационарный режим: $i(\infty) = E/R$. На практике считается, что переходный процесс заканчивается в некоторый момент времени $t_2 \neq 0$. Если разомкнуть ключ (в момент t_2), то не получится найти обратный переходный процесс с учётом первого закона коммутации. При этом образуется электрическая дуга, потому что на зажимах катушки возникает бесконечно большое напряжение, пробивающее всё на пути тока. В рамках лабораторных работ такое явление недопустимо.

Теоретически можно предположить, что время перелёта якоря реле от одного контакта к другому равно нулю (рис. 3).

Однако на практике в момент переключения (t_2) всё равно остаётся неопределённость по отношению к пути протекания тока.

Иногда используют более сложные контактные группы (рис. 4): в момент $t_1 = 0$ сначала замыкается K_1, а потом размыкается K_2, а при $t = t_2$ сначала замыкается K_2 – и только потом размыкается K_1. При этом исключается опасность перенапряжения. Однако в момент переключения накоротко замыкается источник E, что недопустимо.

Обе проблемы («перенапряжение» и«переток») преодолеваются известным простым способом – включением диода в поперечную ветвь (рис. 5).

При замыкании ключа диод заперт, и его ветвь разомкнута. При размыкании ключа ток $i(t)$ движется через открытый $p-n$ переход диода, и на его зажимах остаётся небольшое напряжение с обратной полярностью. Таким образом, комбинация ЭДС E, ключа и диода D образуют источник прямоугольного импульса с почти нулевым внутренним сопротивлением, что соответствует эквивалентной схеме, уже не содержащей ни ключа, ни диода (рис. 6).

Анализ схемы рис. 6 при различных (не обязательно скачкообразных) воздействиях гораздо проще, чем рис. 5. Это линейная схема с постоянными параметрами, и для нахождения отклика по заданному воздействию не надо применять операторный метод. Здесь достаточно использовать метод Фурье, а при цифровой реализации – основанный на нём метод z-преобразования или временной метод – интеграл наложения или свёртку (интеграл Дюамеля).

Рассмотрим, как ведёт себя схема, в которой вместо катушки стоит конденсатор. Это тоже накопитель энергии: там $W_L = \dfrac{Li^2}{2}$, а здесь $W_C = \dfrac{Cu^2}{2}$.

Видно, что речь идёт о дуальной схеме (рис. 7).

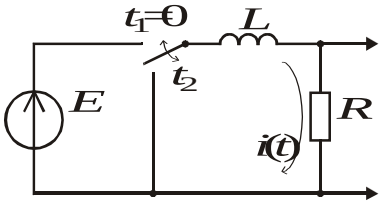


Рис. 3. Абстрактный переключатель для пояснения переходного процесса при размыкании ключа в цепи с последовательным соединением индуктивности и сопротивления

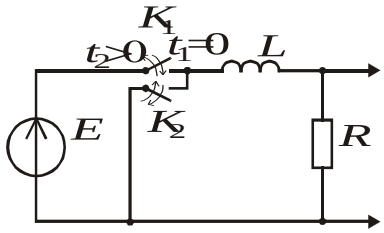


Рис. 4. Контактные группы переключателей для реализации переходного процесса при размыкании ключа в цепи с последовательным соединением резистивного сопротивления и индуктивности

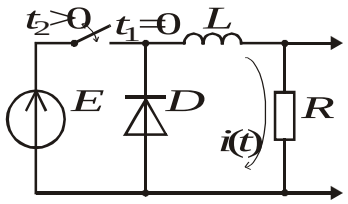


Рис. 5. Линейные (*L* и *R*), нелинейный (*D*) и параметрический (ключ) элементы

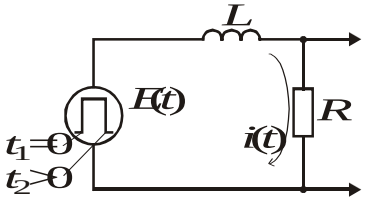


Рис. 6. Схема замещения цепи, приведённой на рис. 5

Начиная с момента времени $t = 0$, конденсатор начинает заряжаться. При $t = \infty$ заряд прекращается. При этом $i_R = J$, значит, $u_C = u_R = J \cdot R$ и $W_C = \frac{C(J \cdot R)^2}{2}$. При надлежащем выборе C, J и R величина накопленной энергии W_C может оказаться как угодно большой. Если по окончании процесса заряда конденсатора (в момент $t_2 \neq 0$) снова замкнуть ключ, чтобы получить обратный переходный процесс (разряда конденсатора), то ток разряда конденсатора будет равен бесконечности, так как по второму закону коммутации после замыкания ключа напряжение должно остаться равным $u_C = J \cdot R$, а оно стало равным нулю. На практике это приводит к расплавлению и слипанию (сварке) контактов ключа, что дуально повторяет процесс образования электрической дуги в схеме с катушкой индуктивности. В то же время оставлять разомкнутым путь тока J нельзя. Здесь также при проведении лабораторных работ такие процессы недопустимы.

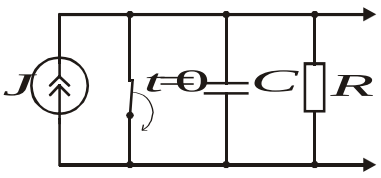


Рис. 7. Схема, дуальная по отношению к рис. 2

Обе проблемы («перенапряжение» и «переток») для дуальной схемы также преодолеваются включением диода (рис. 8).

В момент замыкания ключа ток J перестаёт идти в сторону конденсатора, а тот начинает разряжаться через сопротивление резистора.

Аналогичные рассуждения можно применить и для анализа цепей более высокого порядка.

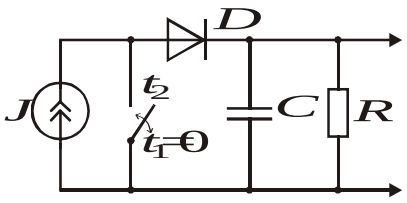


Рис. 8. Линейные (*C* и *R*), нелинейный (*D*) и параметрический (ключ) элементы

Список используемых источников

1. Бакалов В. П., Дмитриков В. Ф., Крук Б. И. Основы теории цепей. М.: Радио и связь, 2000. 592 с.

УДК 62-405
ГРНТИ 47.09.31

ТЕРМОМЕХАНИЧЕСКАЯ УСТОЙЧИВОСТЬ ЦИРКОНИЕВО-ПЕРИКЛАЗОВЫХ ДИЭЛЕКТРИЧЕСКИХ МАТЕРИАЛОВ

А. И. Арсирий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Получение и исследование свойств новых материалов для современной радиоэлектроники - одна из важнейших задач. Керамические диэлектрические материалы на основе диоксида циркония способны длительное время сохранять свои исходные характеристики, в том числе при повышенных температурах.

диэлектрические материалы, циркониевая керамика, термическое старение, свойства.

Безостановочное стремление к миниатюризации микроэлектроники требует поиска новых материалов, способных обеспечить требуемый уровень параметров при меньших толщинах, более плотной компоновке и снижении уровня потребляемой мощности. При уменьшении технологических норм должна быть уменьшена в том числе и толщина диэлектрика в МДП структурах. В настоящее время минимальная толщина подзатворного диэлектрического слоя из диоксида кремния составляет порядка 1,2 нм. Меньшие толщины этих слоев, на данный момент не реализованы, вследствие существенного возрастания туннельных проскоков и появления токов утечки, благодаря которым практически утрачиваются диэлектрические свойства SiO_2.

Решение этой проблемы может быть найдено в разработке материалов, которые в тонких слоях не показывают эффекта тунеллировния и имеют высокую диэлектрическую проницаемость от 20 до 30. В качестве таких диэлектриков в настоящее время рассматриваются: оксид гафния HfO_2 или близкий к нему диоксид циркония ZrO_2 ($\varepsilon \approx 25$) и другие оксиды [1].

Наиболее перспективным можно считать диоксид циркония, который помимо достаточно высокой ε, обладает большой шириной запрещенной зоны (Eg = 5.1 эВ), высокой термической стабильностью до 1000°C. Помимо этого коэффициент теплового расширения циркониевой керамики и металлов близки. Подложки из диоксида циркония обладают высокой трещиностойкостью и ударной вязкостью.

Структура кристаллической решетки ZrO_2 изучена достаточно хорошо. При температурах до 1 000–1 200°*C*, чистый диоксид циркония имеет моноклинную кристаллическую решетку, но эта структура чувствительна к изменению внешней среды (примесям и температуре).

При температурах выше 2 300°*C* диоксид циркония имеет кубическую структуру типа флюорита (CaF_2) (рис.).

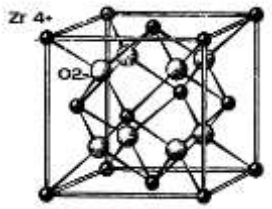


Рисунок. Кристаллическая решетка кубического ZrO_2 (тип флюорита)

Элементарная ячейка кубического диоксида циркония представляет собой куб, в вершинах и в центре граней которого находятся ионы циркония, а ионы кислорода занимают центры всех восьми октантов тетрагональных пустот данной плотноупакованной ячейки.

Как показали исследования наиболее стабильной является именно кубическая кристаллическая решетка диоксида циркония, но получение такой структуры технологически затруднено [2]. С середины прошлого столетия для получения устойчивых как в термическом, так и в химическом отношении циркониевых материалов применяют методику стабилизации тетрагональной кристаллической структуры, путем получения искаженной решетки типа флюорита при температурах существенно меньших температуры фазового перехода.

В подавляющем большинстве стабилизацию проводят путем перевода в псевдокубическую (искаженную тетрагональную) модификацию с кристаллической решеткой типа флюорита (см. рисунок). При этом в кристаллической структуре кристаллов на основе диоксида циркония обнаруживается большое число кислородных вакансий, наличие которых определяет физические свойства этих материалов. Стабилизация тетрагональной модификации диоксида циркония возможна в широком диапазоне температур. Устойчивость кристаллической решетки достигается в результате образования твердых растворов замещения. Как известно, стабильные структуры твердых растворов образуются при различии ионных радиусов элементов, входящих в их состав не превышающем 10–15 % [3]. Для образования устойчивого в широком диапазоне температур и при воздействии различных агрессивных компонентов, таких как расплавы металлов, стекол и полимеров часть ионов Zr^{4+} (r = 0,82 Å), ионный радиус которых, слишком мал для идеальной решетки флюорита, характерной для тетрагонального диоксида циркония, необходимо заместить ионами немного большего размера. Стабилизация проводится внедрением в кристаллическую решетку диоксида циркония оксидов щелочноземельных (*Ca, Mg*) или редкоземельных металлов. Наилучшими показателями с точки зрения устойчивости обладают композиции, полученные на основе оксида иттрия (r = 0,96 Å).

Немаловажным является и устойчивость композиций на основе диоксида циркония, стабилизированного в высокотемпературной форме оксидами металлов к термическому и другим видам старения. Для изучения возможности применения циркониевой керамики в контакте с различными электротехническими материалами, например с защитными неорганическими эмалями, имеющими состав близкий к составу кварцевого стекла, были проведены исследования термического старения циркониевой керамики в контакте с агрессивными средами.

Объектами исследования служили кубические твердые растворы диоксида циркония, стабилизированного оксидами магния и кальция. Состав твердых растворов был представлен композициями 88мол.%ZrO_2 + 12мол.%MgO и 88мол.%ZrO_2 + 12мол.%CaO. Изменения в структуре и фазовом составе образцов отслеживали через каждые 5–10 часов обжига в слабо окислительной среде при температурах до 1 400 °C.

Для составов, содержащих диоксид циркония, стабилизированный 12мол.% CaO, и периклаз в качестве магниевой добавки, даже после 100 часов обжига на рентгенограммах идентифицируются только рефлексы, принадлежащие циркониево-кальциевому кубическому твердому раствору. Таким образом, материал на основе композиций из ZrO_2, стабилизированного оксидом кальция и периклаза, вводимого в количестве от 5 до 50 %, можно рекомендовать для работы в условиях длительного воздействия высоких температур. В случае введения в качестве магниевой добавки MgO марки х. ч., фазовый состав сохраняется неизменным только при 50 % содержании магниевой составляющей. При меньших количествах MgO происходит некоторый распад кубических твердых растворов.

Для образцов из циркониево-магниевых твердых растворов постоянство состава сохраняется и после 100 часов обжига. Для содержания магниевой добавки менее 50 %, а также в случае введения MgO марки х.ч. процесс дестабилизации начинается после 50 часов обжига. Содержание моноклинного ZrO_2 возрастает с увеличением времени обжига. Максимальная степень дестабилизации обнаруживается у образцов состава 80 % цирконием-магниевого твердого раствора и 20 % оксида магния марки х. ч., степень дестабилизации составляет около 40 %.

Определение прочностных, в том числе термомеханических характеристик, так же показало приоритетный выбор цирконием-кальциевых композиций.

Таким образом, материалы на основе диоксида циркония, стабилизированного оксидом кальция в присутствии оксида магния, в количестве не превышающем 50 %, показали высокие параметры механических, термомеханических свойств, а также достаточно хорошую стабильность фазового состава.

Список используемых источников

1. Шевченко А. В., Рубан А. К., Дудник Е. В. Высокотехнологическая керамика на основе диоксида циркония // Огнеупоры и техническая керамика. 2000. № 9. С. 2–8.
2. Арсирий А. И., Страхов В. И., Мигаль В. П. О фазовых соотношениях и свойствах материалов циркониево-периклазовых композиций // Огнеупоры и техническая керамика. 2009. №10. С. 12–14.
3. Юм-Розери В. Введение в физическое металловедение / Пер. с англ. В. М. Глазова и С. Н. Горина. Москва: Металлургия, 2013. 203 с. ISBN 978-5-458-28643-5.

УДК 621.372.413
ГРНТИ 47.45.33

ИССЛЕДОВАНИЕ МИКРОВОЛНОВОГО УСТРОЙСТВА ЧАСТОТНОЙ СЕЛЕКЦИИ НА ЦИЛИНДРИЧЕСКОЙ ПОВЕРХНОСТИ

Е. И. Бочаров, М. А. Васяткин, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается кольцевой резонатор СВЧ в цилиндрическом исполнении с питанием различными линиями: компланарной и микрополосковой. Проведено компьютерное моделирование этих устройств в прикладном пакете RFSimm, представлены два макета и результаты эксперимента структуры на микрополосковой линии.

компланарный волновод, объемный кольцевой резонатор, микрополосковая линия, цилиндрическая поверхность.

В настоящее время существует потребность в СВЧ устройствах различной конфигурации (конформных), в данной работе представлены два микроволновых устройства частотной селекции на цилиндрической поверхности с микрополосковым объемным кольцевым резонатором. Один макет выполнен на микрополосковой линии, другой на компланарном волноводе.

Компланарный волновод (КПВ) представляет собой трехпроводную линию, в которой распространение электромагнитной волны происходит по зазорам между проводящими пластинами, находящимися в одной плоскости [1]. Компланарные волноводы нашли широкое применение в интегральных схемах СВЧ. Конфигурация компланарного волновода и его вариация на цилиндрической поверхности представлены на рис. 1.

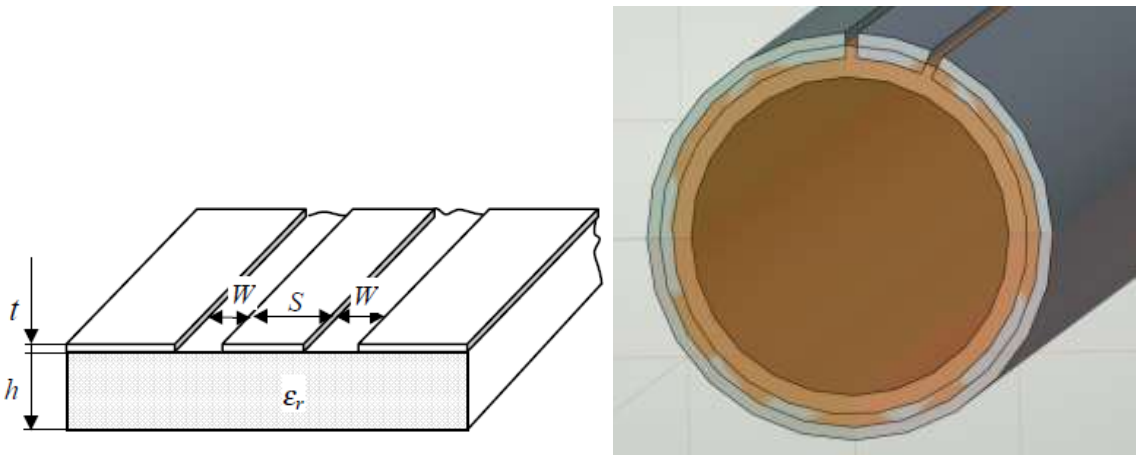


Рис. 1. Классический компланарный волновод (слева) и компланарный волновод на цилиндрической поверхности (справа)

Конфигурация микрополосковой линии (МПЛ) показана на рис. 2. Микрополосковая линия является неоднородной линией передачи, так как не все силовые линии поля между полоском (проводником) и заземленной пластиной проходят через подложку. МПЛ является самой простой и недорогой линией ИС СВЧ.И может легко трансформироваться в другие типы линий, ее целесообразно использовать для макетирования новых устройств.

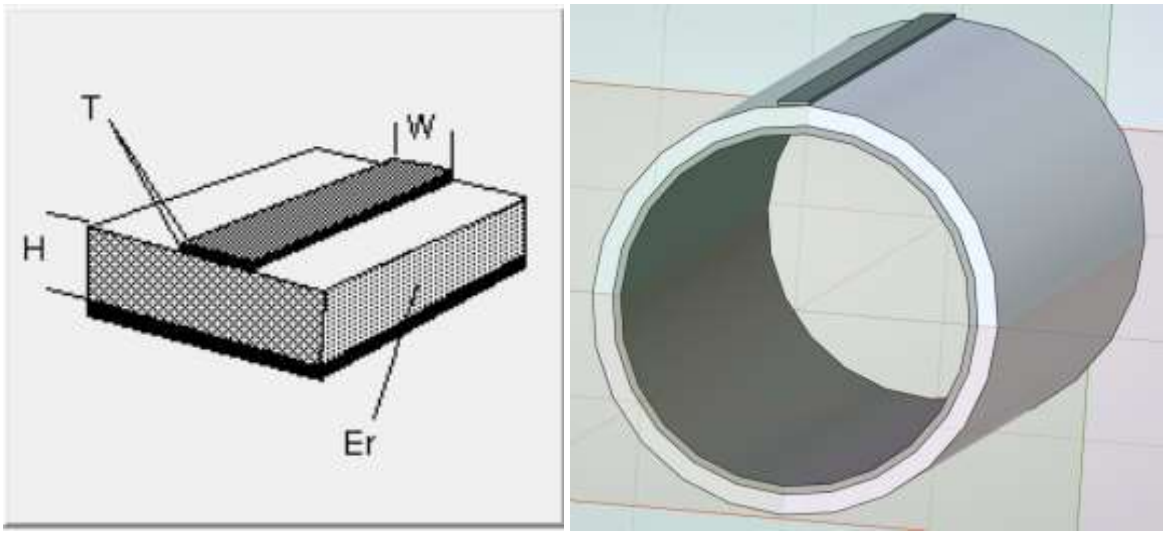
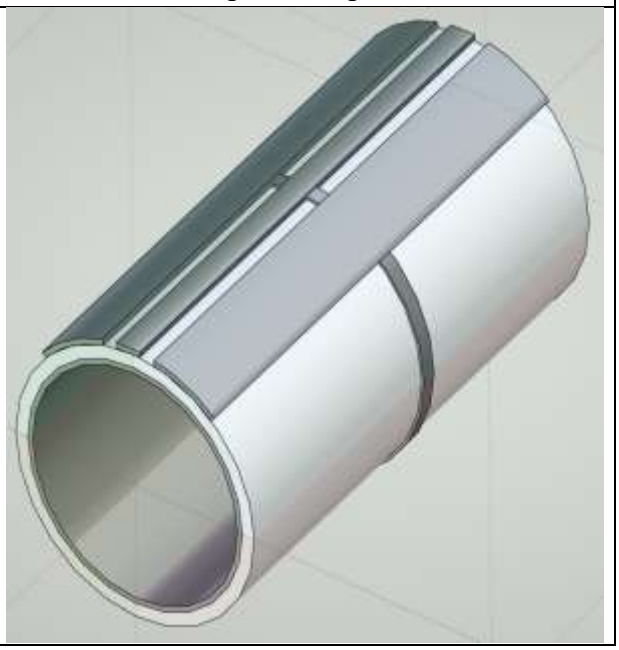


Рис. 2. Классическая МПЛ и МПЛ на цилиндрической поверхности

Модели исследуемых структур представлены в таблице 1.

ТАБЛИЦА 1. Модели исследуемых структур.

Модель резонатора на МПЛ	Модель резонатора на КПВ
	

Исследуемые конфигурации являются резонаторами бегущей волны [3, 4], поэтому длина окружности резонатора будет основным параметром, влияющим на резонансную частоту. Расчет резонансной частоты проведем по формуле:

$$f = \frac{c}{\pi * d * \sqrt{\varepsilon}},$$

где d – диаметр внешнего кольца.

Выберем для нашего макета $d = 49$ мм и $\varepsilon = 2.4$ получаем первую резонансную частоту:

$$f_1 = 1.258 \text{ ГГц}.$$

Принципиальная схема устройства на МПЛ представлена на рис. 3. Результаты эмуляции в прикладном пакете RFSimm99 представлены на рис. 4. Первый резонанс наблюдается на частоте 1.24 ГГц, второй на частоте 2.74 ГГц.

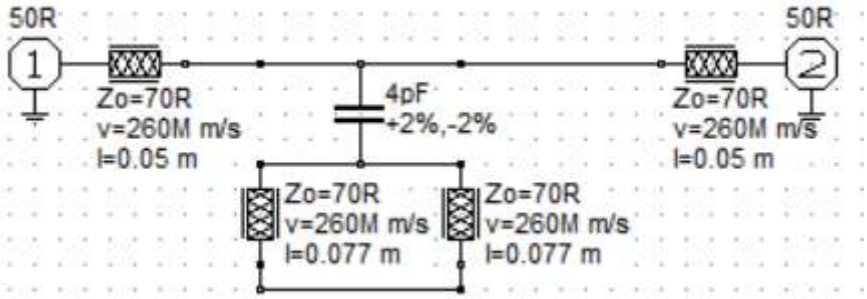


Рис. 3. Принципиальная схема резонатора и питающей линии

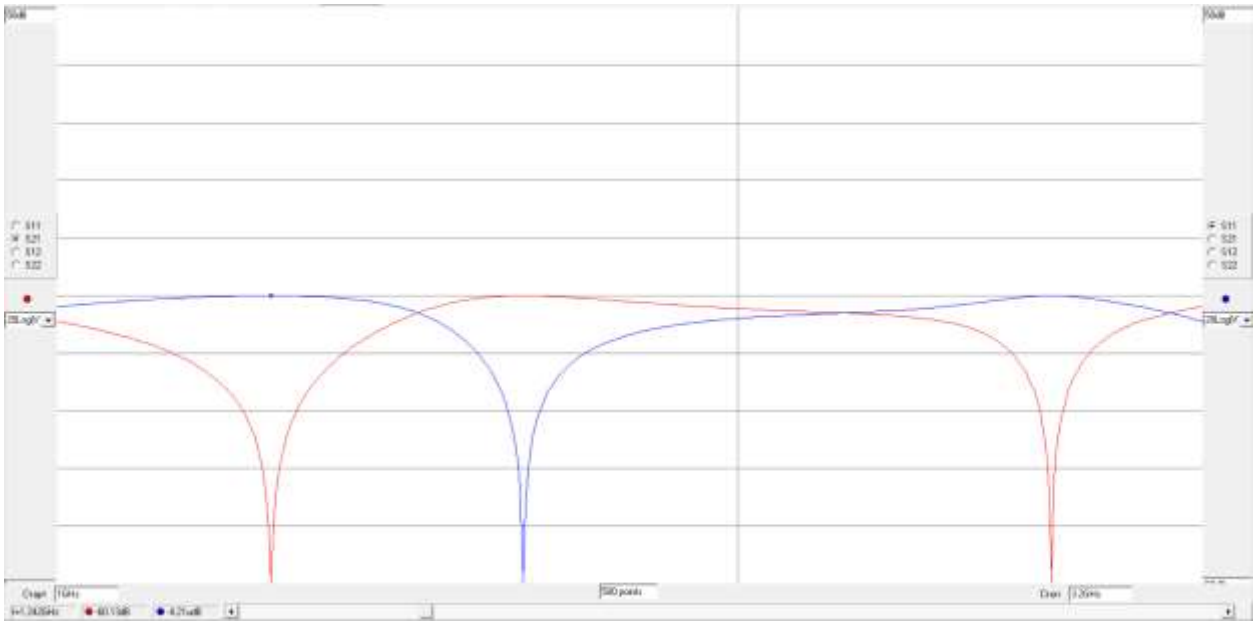


Рис. 4. Частотные характеристики МПЛ с резонатором

Для проведения эксперимента был изготовлен макет устройства на МПЛ, он представлен на рис. 5. Результаты эксперимента представлены на рис. 6. Видно, что ослабление на первой гармонике составляет −37 dB на частоте 1,046 ГГц, второй резонанс наблюдается на частоте 3 ГГц, ослабление порядка −30 dB.

Рис. 5. Макет устройства на МПЛ

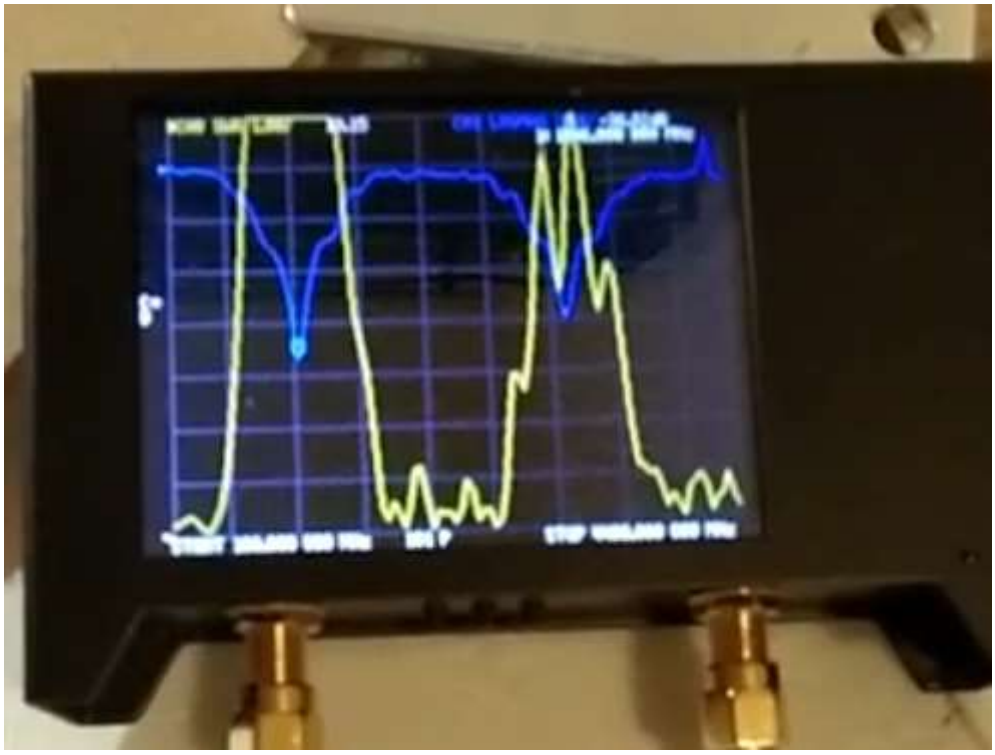


Рис. 6. Результаты эксперимента

Макет устройства на КПВ также был создан, он представлен на рис. 7. К сожалению, резонанс с КПВ получить на данный момент не удалось, требуется доработка узла питания резонатора, что является нетривиальной инженерно-технической задачей.

Рис. 7. Макет устройства на КПВ

Таким образом, можно сделать вывод, что конструктив устройства на МПЛ является полностью рабочим, наблюдаются два ярко выраженных кратных резонанса. На структуре с КПВ резонанс на данный момент не получен, устройство нуждается в доработке. В целом, можно сделать вывод, что изучение устройств подобной конфигурации является весьма перспективным, так как позволяет размещать устройства конформно на круглых волноводах, коаксиальных кабелях и различных цилиндрических поверхностях.

Список используемых источников

1. Бахарев С. И., Вольман В. И., Либ Ю. Н. Справочник по расчету и конструированию СВЧ полосковых устройств. М.: Радио и связь, 1982. 328 с.

2. Проектирование полосковых устройств СВЧ. Учебное пособие. Ульяновск: Ульяновский государственный технический университет, 2001. 123 с.

3. Григорьев А. Д., Янкевич В. Д. Резонаторы и резонаторные замедляющие системы СВЧ. М.: Радио и связь, 1984. 248 с.

4. Бочаров Е. И., Рыбалко И. А., Седышев Э. Ю., Селиверстов Л. А., Сикора Г. Р. Устройства частотной селекции и стабилизации частоты на эллиптических резонаторах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т. СПб.: СПбГУТ, 2017. С. 426–431.

УДК 621.373
ГРНТИ 47.41.31

НАЧАЛЬНАЯ СИНХРОНИЗАЦИЯ ДЕМОДУЛЯТОРА СИГНАЛА С ПРЯМЫМ РАСШИРЕНИЕМ СПЕКТРА С ИСПОЛЬЗОВАНИЕМ БЫСТРОГО ПРЕРБРАЗОВАНИЯ ФУРЬЕ

Е. А. Брусин

АО «РИРВ»

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сигналы с прямым расширением спектра (Direct Spread Spectrum Signals) в настоящее время широко используются в различных системах связи и навигации. Основной особенностью систем связи и навигации, использующих указанные сигналы, является необходимость начальной синхронизации демодуляторов по несущей частоте и задержке. Предлагаемый подход к решению проблемы начальной синхронизации основан на совместном оценивания указанных параметров с использованием быстрого преобразования Фурье. Приведены результаты анализа эффективности предложенного алгоритма начальной синхронизации методами компьютерного моделирования.

прямое расширение спектра, начальная синхронизация, быстрое преобразование Фурье.

Постановка задачи

Под начальной синхронизацией демодуляторов сигналов с прямым расширением спектра фактически понимается процедура определения задержки принимаемого сигнала по отношению к заданной расширяющей последовательности и оценивания несущей частоты принимаемого сигнала. Традиционный подход основан на использовании набора корреляторов [1]. В последние время используются методы начальной синхронизации, основанные на использовании процедур быстрого преобразования Фурье (БПФ) [2…4]. В работе представлен алгоритм начальной синхронизации, основанный на использовании БПФ, и проведён анализ эффективности предлагаемого алгоритма.

Алгоритм начальной синхронизации

Будем рассматривать сигнал двухпозиционной фазовой модуляции (ФМ-2), включающий в себя умножение на сигнатуру (расширяющую спектр последовательность) $s_k(t)$.

Принимаемый сигнал можно представить в виде:

$$\tilde{s}_k(t; b_k) = s_k(t - \tau_k) \cdot B_k(t - \tau_k) \cdot \cos(2\pi(f_0 + f)t + \varphi_k) + n_\tau(t),$$

где τ_k – задержка в канале;

φ_k – фаза несущей частоты;

$B_k(t) = b_{k,i} = \pm 1$ – информационные символы, передаваемые на интервалах $(i-1)T_b < t \leq T_b$, T_b – длительность информационного символ (бита);

f_0 – номинальное значение частоты несущего колебания;

f – смещение частоты несущего колебания относительно заданного номинального значения;

$n_\tau(t)$ – отсчёты шума.

Предлагаемый алгоритм состоит в следующем. Вычислим комплексное преобразование Фурье вида:

$$R_l = \sum_{n=0}^{N-1} \left(s_k(t_n) + j s_k(t_n)\right) \cdot e^{-j\frac{2\pi nl}{N}},$$

где N – длина преобразования Фурье;

$l = 0{,}1 \ldots N-1$;

$s_k(t_n)$ – отсчёты расширяющей последовательности.

Сформируем отсчёты опорного сигнала:

$$\hat{R}_l = R_l^* .$$

Здесь R_l^* – комплексно-сопряженные отсчёты преобразования Фурье R_l, $l = 0{,}1 \ldots N-1$.

Далее вычислим M преобразований Фурье вида:

$$S_{ml} = \sum_{n=0}^{N-1} \tilde{s}_k(t_n; b_k) \cdot e^{-j2\pi(f_0 + m\cdot\Delta f)t_n} \cdot e^{-j\frac{2\pi nl}{N}}$$

Здесь m меняется от $-M/2$ до $M/2$, Δf – шаг сетки частот. Вычислим M обратных преобразований Фурье:

$$s_{ml} = \frac{1}{N} \sum_{n=0}^{N-1} S_{ml} \cdot \hat{R}_n \cdot e^{j\frac{2\pi nl}{N}} \qquad (1)$$

В выражении (1) m определяет частотный канал, l – позицию расширяющей последовательности. Дискретная функция неопределённости (ambiguity function) вычисляется следующим образом:

$$\rho(m,l) = |s_{ml}| \qquad (2)$$

Для нахождения искомого смещения по несущей частоте и искомой позиции по отношению к опорной расширяющей последовательности ищется глобальный максимум (2):

$$\{M_f, L_f\} = arg\left\{\max_{m,l} \rho(m,l)\right\},$$

где $m = -M/2, \ldots -1,0,1, \ldots M/2$;

$l = 0,1 \ldots, N-1$.

В результате получаем искомую позицию по отношению к опорной расширяющей последовательности L_f и оценку смещения несущей частоты принимаемого сигнала относительно заданного номинального значения:

$$\hat{f} = M_f \cdot \Delta f.$$

Для анализа предлагаемого алгоритма было проведено моделирование алгоритма начальной синхронизации при следующих условиях: длительность информационного символа $T_b = 50$ мкс (информационная скорость 20 кбит/с), диапазон поиска по несущей частоте ± 40 кГц, шаг сетки частот – одна четверть от информационной скорости. При формировании расширяющей последовательности использовалась укороченная последовательность Голда длиной 2046.

Соответствующий результат вычисления обратного преобразования Фурье (1) для одного из частотных каналов представлен на рис. 1.

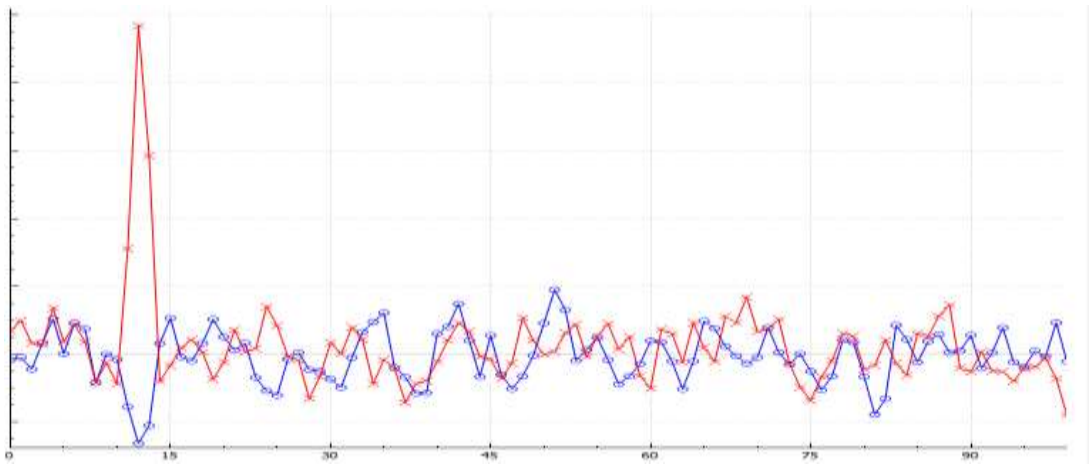


Рис. 1. Компоненты обратного БПФ. $f = 0$ кГц, E_s/N_0 = – 10 дБ

Модуль преобразования (1) представлен на рис. 2. Фактически на рис. 2 представлен корреляционный пик, максимум которого указывает на искомую позицию L_f. Результат вычисления функции неопределённости $\rho(m, l)$ представлен на рис. 3.

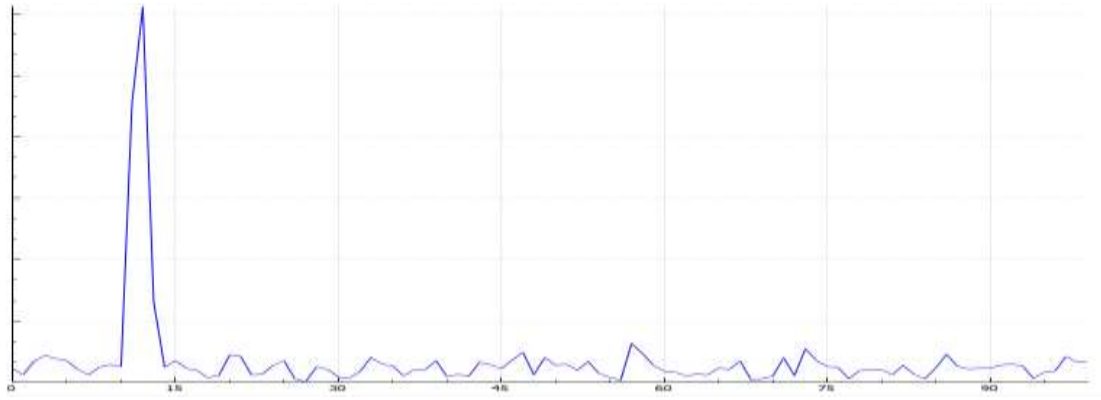


Рис. 2. $|s_{ml}|$. f = 0 кГц. E_s/N_0 = – 10 дБ

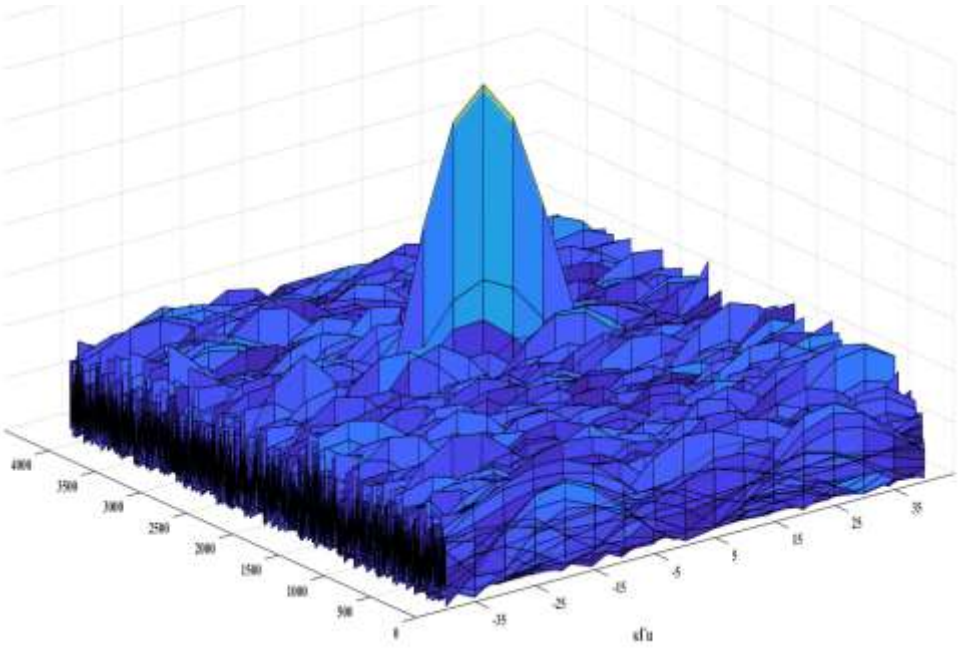


Рис. 3. $\rho(m, l)$. f = 0 кГц, L_f = 2196, E_s/N_0 = – 10

Моделирование процедуры начальной синхронизации проводилось для интервалов наблюдения, составляющих 1, 4 и 8 информационных символов. Анализировалась вероятность обнаружения сигнала и нормированная к информационной скорости дисперсия оценки несущей частоты. Считалось, что обнаружение произошло, если найденная позиция L_f совпадала с переданной. Зависимости вероятности обнаружения от отношения сигнал/шум на чип, полученные по результатам моделирования, представлены на рис. 4.

Полученная в ходе моделирования зависимость нормированной дисперсии оценки несущей частоты представлена на рис. 5.

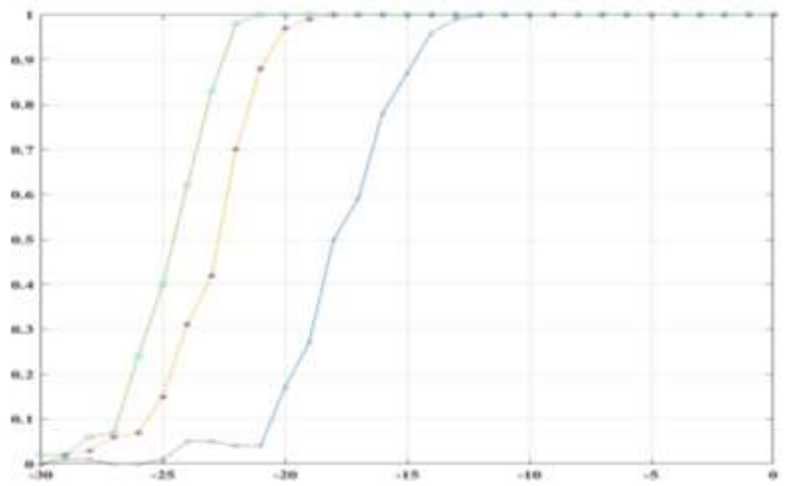


Рис. 4. Вероятность обнаружения. L_f = 12. +– N = 4 096, *– N = 16 384, x– N = 32 768

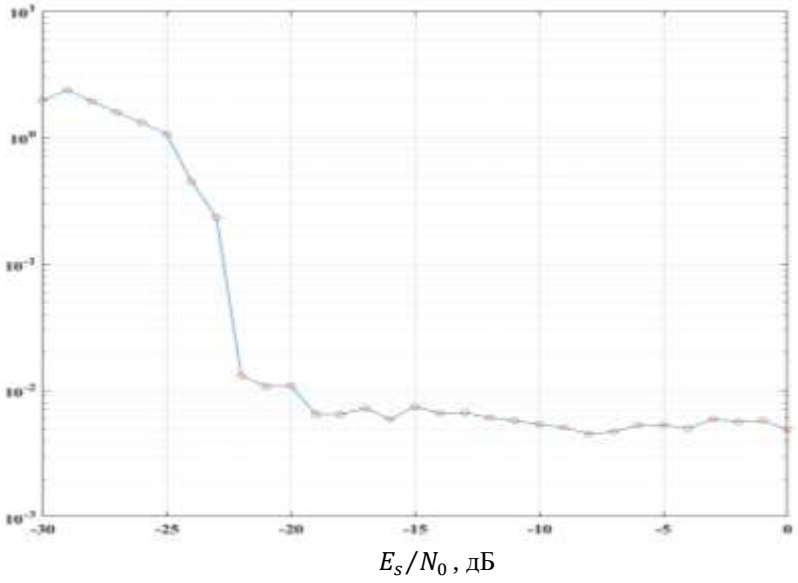


Рис. 5. Нормированная дисперсия оценки несущей частоты. N = 32 768. L_f = 12.

Выводы

Предложен подход к реализации процедуры начальной синхронизации демодулятора сигнала с прямым расширением спектра, основанный на использовании методов преобразования Фурье. Результаты моделирования показывают, что предлагаемый алгоритм начальной синхронизации обеспечивает вероятность обнаружения, близкую к единице, при достаточно низком отношении сигнал/шум на чип. Получаемая дисперсия оценки несущей

частоты существенно «сжимает» начальную частотную неопределённость принимаемого сигнала по частоте несущего колебания.

Список используемых источников

1. Spread Spectrum and CDMA. Principles and Applications Valery P. Ipatov. John Wiley & Sons Ltd 2005.

2. Alexandre P. Almeida, Rui Dinis, Francisco B. Cercas, An FFT-based Acquisition Scheme for DS-CDMA Systems // 2007 International Symposium on Communication and Information Technologies. 17-19 Oct. 2007.

3. XUE J., ZHAO Q. & WU Z.J., Research on PN code fast acquisition algorithm based on FFT. Journal of Telemetry, Tracking and Command, 29(6), pp. 41-46, 2008.

4. Chen S., Guo L. L., Sun Z. G., Wang B. C., X.Y. & Ning, Research on Time-Frequency Domain Acquisition Algorithm of Parallel Combinatory Spread Spectrum System Based on FFT // International Conference on Computer Information Systems and Industrial Applications (CISIA 2015).

УДК 621.372
ГРНТИ 47.45.99

ПРОБЛЕМЫ СИНТЕЗА КОПЛАНАРНОГО ВОЛНОВОДА И МЕТОДЫ ОЦЕНКИ ЕГО РАБОЧИХ ПАРАМЕТРОВ

В. С. Вахрамеева, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

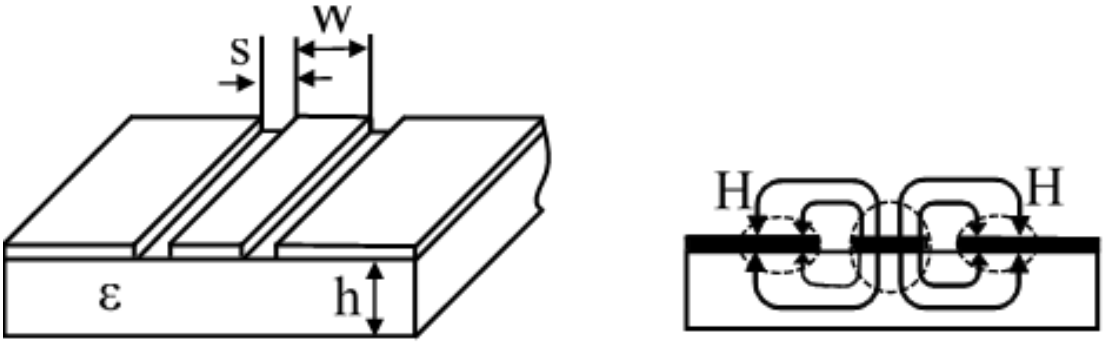
В работе представлены основные проблемы синтеза копланарного волновода. Сравниваются методики расчёта волнового сопротивления передающей линии интегральных схем СВЧ. Методики расчёта представлены из различных источников. Теоретический расчёт проведён с помощью аппроксимирующего выражения.

копланарный волновод, расчёт, волновое сопротивление.

Копланарный волновод широко используется в современных СВЧ устройствах. В отличии от других типов линий, он имеет наименьшую электромагнитную связь с соседними линиями и удобен для монтажа навесных элементов. При этом отсутствует необходимость высверливать и металлизировать отверстия, что позволяет удешевить процесс производства СВЧ устройств. Тем не менее, точный расчёт параметров копланарного волновода является сложной инженерно-технической задачей [1].

На рис. 1 (а) изображён копланарный волновод – трехпроводная полосковая линия передачи, образованная двумя параллельными узкими щелями

в металлическом листе на одной стороне диэлектрической пластины. Структура электрического поля в поперечном сечении волновода представлена на рис. 1 (б). Средний проводник является токонесущим, а два проводника по бокам – «земля». Особенностью такой линии является распространение волны с двух сторон от центрального проводника.



а) б)

Рис. 1. Поперечное сечение копланарного волновода

На рис. 1 W – ширина линии, S – ширина зазора, ε – относительная проницаемость диэлектрика, h – толщина подложки.

При создании копланарного волновода важно точно сопоставить геометрию волновому сопротивление $Z_в$, которое является основным параметром передающей линии. В таблице 1 представлены формулы из различных источников [2–5] для расчёта волнового сопротивления.

ТАБЛИЦА 1. Формулы для расчёта волнового сопротивления

$Z_в = \frac{133.2}{\sqrt{\varepsilon+1}} * \frac{K'(k)}{K(k)}$	$k = \left(1+\frac{2S}{W}\right)^{-1}, k' = \sqrt{1-k^2}$
$Z_в = \frac{60\pi}{\sqrt{(\varepsilon+1)/2}} * \frac{1}{K(k)}$	$k = \left(1+\frac{2S}{W}\right)^{-1}$
$Z_в = \frac{30\pi}{\sqrt{\varepsilon_{эф}}} * \frac{K'(k)}{K(k)}$	$k = \frac{W}{W+2S}, k' = \sqrt{1-k^2}, \varepsilon_{эф} = \frac{1+\varepsilon}{2}$
$Z_в = \frac{30\pi}{\sqrt{(\varepsilon+1)/2)}} * \frac{K'(k)}{K(k)}$	$k = \operatorname{sech}\left(\frac{\pi * W}{2h}\right), k' = \sqrt{1-k^2}$

Используемые в формулах эллиптические интегралы первого рода были рассчитаны с помощью аппроксимирующего выражения (1), которое обеспечивает точность вычислений до шестого знака.

$$\frac{K'(k)}{K(k)} = \begin{cases} \frac{1}{\pi}\ln\left(2\frac{1+\sqrt{k}}{1-\sqrt{k}}\right), & 0.707 \le k \le 1 \\ \left(\frac{1}{\pi}\ln\left(2\frac{1+\sqrt{k\prime}}{1-\sqrt{k\prime}}\right)\right)^{-1}, & 0 \le k \le 0.707 \end{cases} \quad (1)$$

Для оценки точности формул были изготовлены и исследованы пять различных макетов копланарного волновода. В таблице 2 содержатся параметры исследуемых линий, необходимые для расчёта волнового сопротивления.

ТАБЛИЦА 2. Параметры макетов

№ макета	*S*, мм	*W*, мм	ε
1	0,5	1,7	4,2
2	0,5	3,6	
3	0,2	4	
4	0,2	14,2	
5	1	11,8	

В таблице 3 представлены результаты вычислений волнового сопротивления по предложенным формулам, все они дают разные результаты. Отличия варьируются в диапазоне от сотых до десятков Ом. Сложно сказать, какие из предложенных формул более точные, так как нет законченных методик оценки точности параметров линий.

ТАБЛИЦА 3. Результаты вычислений волнового сопротивления

№ макета	R1	R2	R3	R4
1	53,078	65,859	53,113	27,3
2	64,828	59,521	64,871	14,463
3	82,372	50,366	82,426	13,163
4	105,291	40,618	105.36	-
5	73,149	55,038	73,197	-

Проанализируем результаты измерений макетов. На рис. 2 и 3 видно, что на волновое сопротивление копланарного волновода существенно влияет ширина заземлённых линий и равномерность зазоров. Большие потери в 1 макете могут образоваться из-за разной толщины заземлённых линий, а во 2 макете из-за неравномерности зазоров.

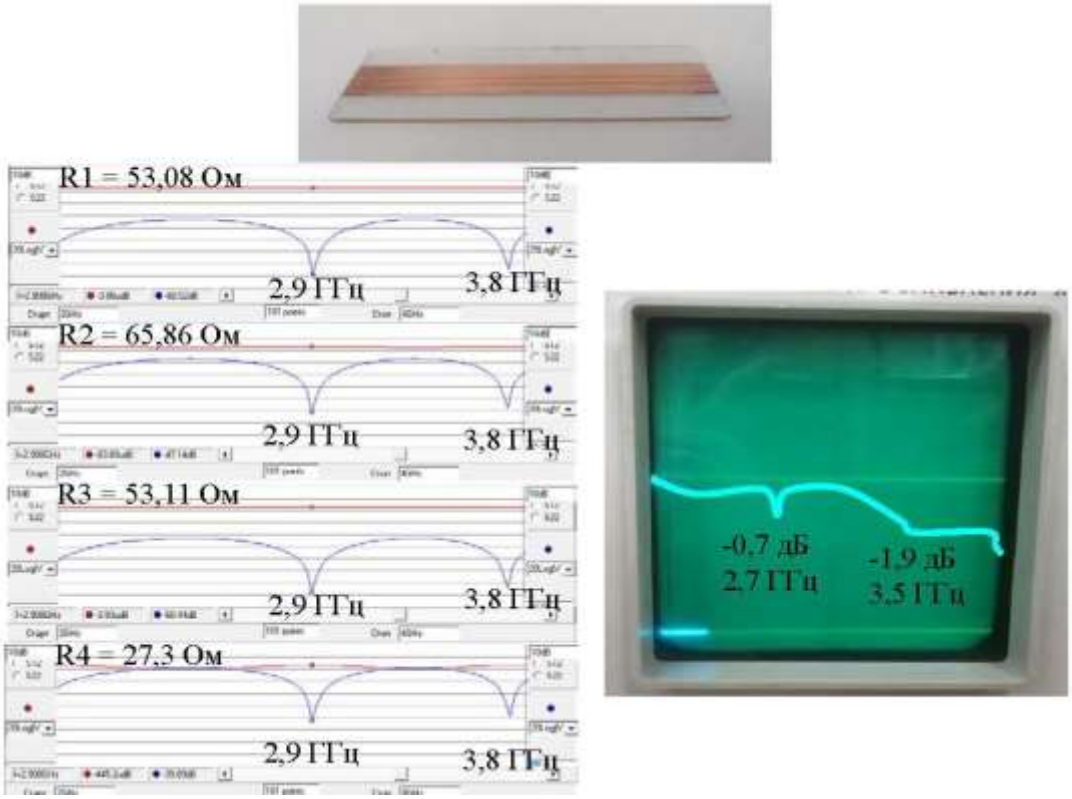


Рис. 2. Макет № 1, характеристики ослабления

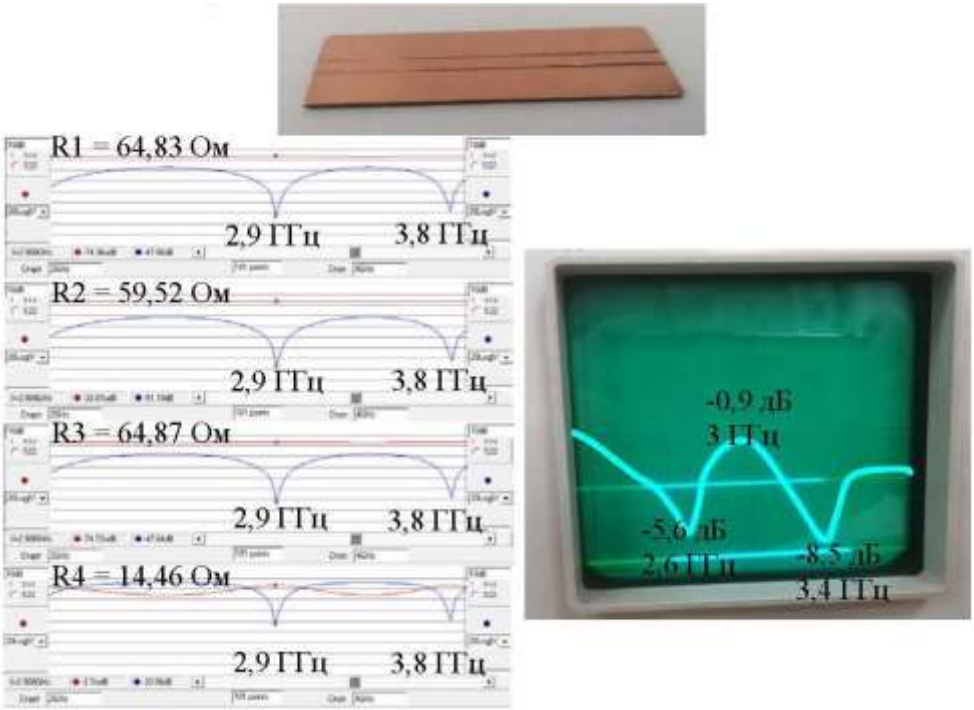


Рис. 3. Макет № 2, характеристики ослабления

На рис. 4 и 5 представлены аналогичные макеты, по характеристикам ослабления которых видно, что на потери влияет ширина токонесущей линии, а также материал, из которого изготовлен копланарный волновод.

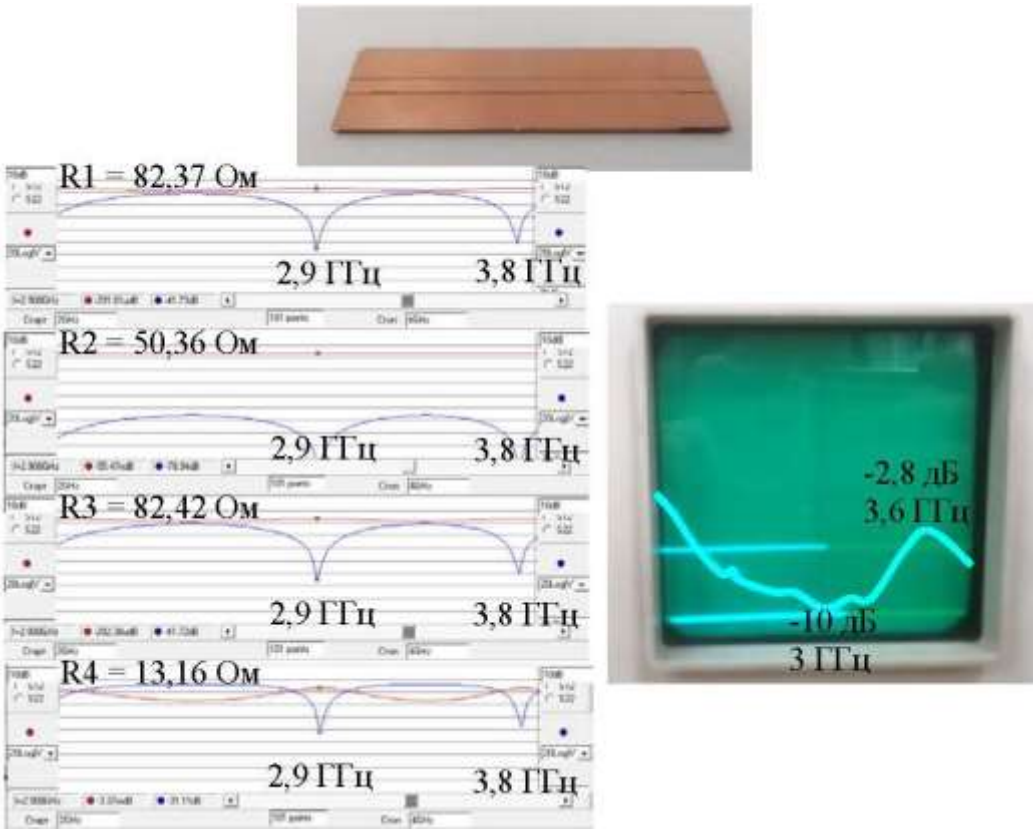


Рис. 4. Макет № 3, характеристики ослабления

Например, 4 макет не пропускает волну на всех частотах, кроме частоты 2,885 ГГц с потерями в 8,2 дБ.

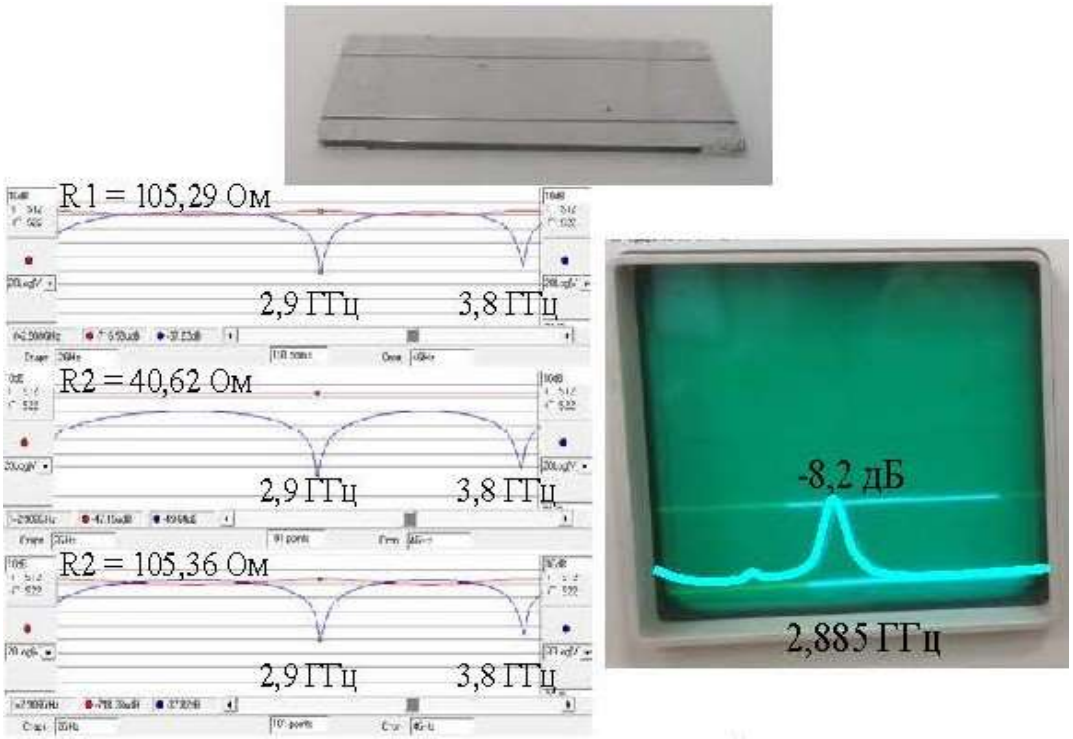


Рис. 5. Макет № 4, характеристики ослабления

Изменяя ширину токонесущей линии и зазоров, можно добиться меньших потерь для частоты, когда копланарный волновод пропускает сигнал. Например, в 5 макете (рис. 6) волна проходит на частоте 2,937 ГГц с потерями 3,4 дБ.

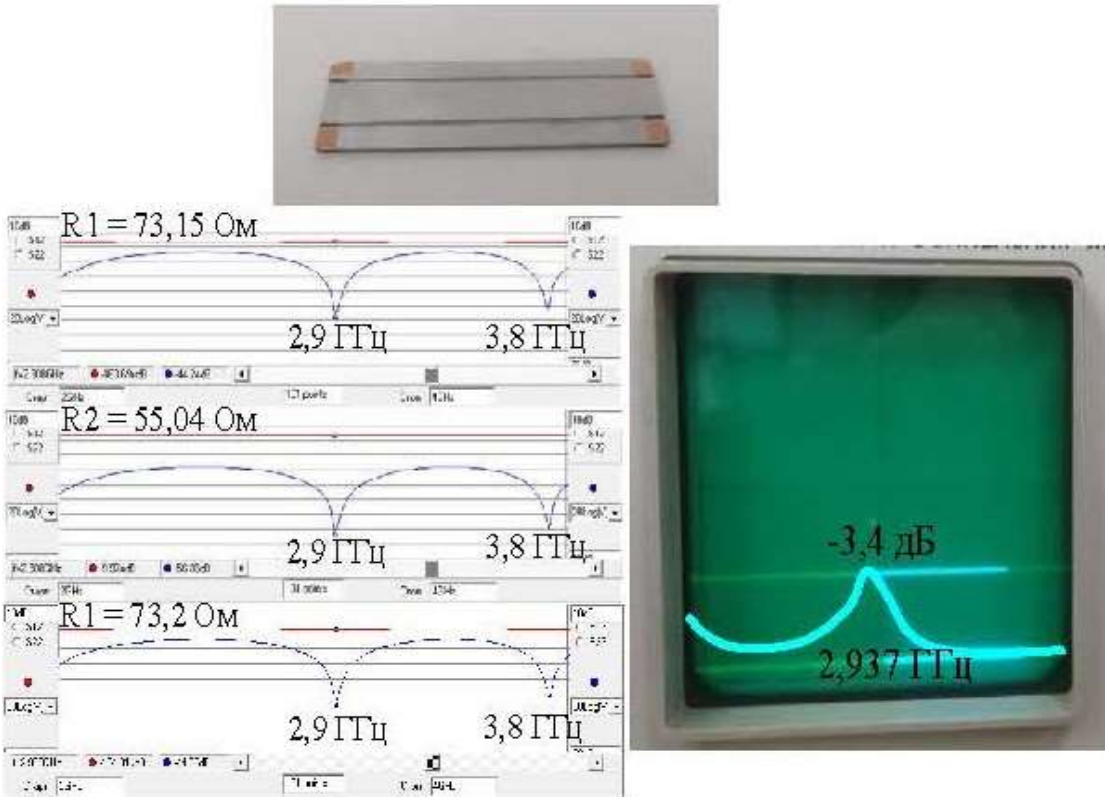


Рис. 6. Макет № 5, характеристики ослабления

На рис. 7 представлен копланарный волновод под микроскопом с увеличением в 100 раз. Можно сделать вывод, что внутреннее устройство линии имеет огромное количество нерегулярностей. Толщина полос линии неравномерна, имеются различные неровности металла. Всегда есть асимметрия зазоров, которая в нашем случае изменяется от 20 до 40 микрон, неравномерность краёв в 10–20 микрон. Всё это существенно влияет на потери и отклонения волнового сопротивления от среднего. Учесть это в расчёте практически невозможно.

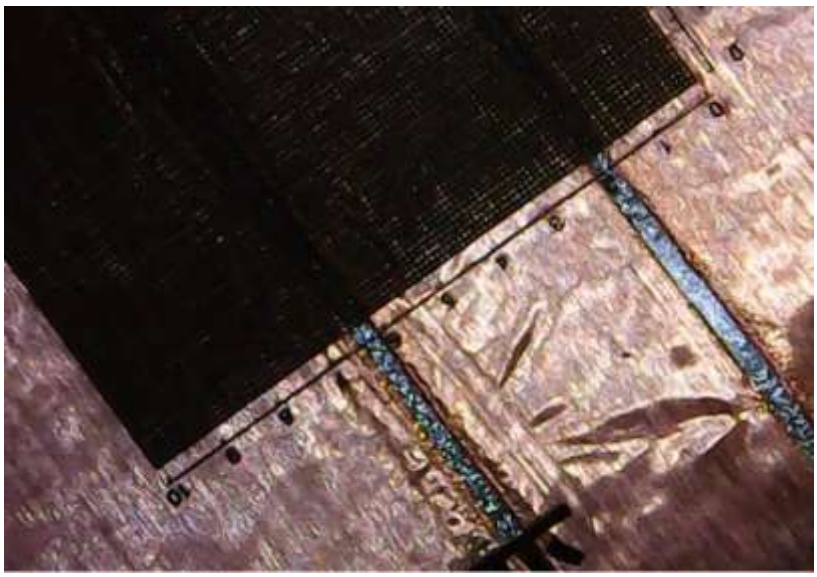


Рис. 7. Копланарный волновод под микроскопом

Основной вывод работы в том, что формулы не гарантируют должную точность, их мало и они дают очень разные результаты. Неравномерности геометрии линий существенно влияют на волновое сопротивление и не учитываются формулами найденных методик. Таким образом, оценка точности расчёта волнового сопротивления копланарного волновода представляет собой нерешённую на данном этапе инженерно-техническую задачу. Проверить точность расчёта на сегодняшний день практически невозможно, так как нет конкретных методик для оценки точности параметров линий в интегральной схемотехнике СВЧ.

Список используемых источников

1. Боброва К. В., Булатова И.А., Иванова Е.А., Седышев Э.Ю. Расчёт модифицированных линий передач для объёмных интегральных схем СВЧ // Электроника и микроэлектроника СВЧ. 2015. Т. 2. С. 161–170.

2. Вольман В. И., Бахарев С. И. и др. Справочник по расчёту и конструированию СВЧ полосковых устройств. Москва: Радио и связь, 1982. 328 с.

3. Фельдштейн А. Л. Справочник по элементам волноводной техники. Москва: издво «Советское радио», 1967. 651 с.

4. Ганстон М. А. Р. Справочник по волновым сопротивлениям фидерных линий СВЧ. Москва : Связь, 1976. 152 с.

5. Лавренко Ю. Е., Грачев С. В. Л13 Устройства СВЧ: конспект лекций. СПб.: Издво СПбГЭТУ «ЛЭТИ», 2014. 92 с.

УДК 004, 51.3, 51-7, 537, 614.2
ГРНТИ 59.14, 47.14, 20.53.23, 28.15.15, 76.13.99

СХЕМНЫЕ РЕШЕНИЯ ПО ПРОЕКТИРОВАНИЮ СИСТЕМЫ УПРАВЛЕНИЯ АНТРОПОМОРФНОЙ РОБОТИЗИРОВАННОЙ РУКИ

Г. С. Великоборец, В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Антропоморфные конечности спроектированы и построены так, чтобы имитировать человеческую форму и движения. В конечном счете, они должны напоминать размер и физические способности человеческих конечностей, чтобы функционировать в среде, ориентированной на человека. Это крайне важно при протезировании. В статье представлена конструкция антропоморфной руки с 21 степенью свободы, применимой для использования в качестве протеза. Представлена схемотехническая реализация системы контроля за состоянием приводов руки, а также проведён обзор способов управления конечностью при её использовании в качестве протеза.

медицинская электроника, антропоморфный протез, профилактическая медицина, роботизированные системы, интерфейс мозг-компьютер.

В последние десятилетия наблюдается бурный рост использования технологий робототехники в различных сферах человеческой жизнедеятельности. Одно из таких направлений – протезирование. Появившись в середине прошлого столетия, бионические протезы, основанные на мышечном контроле, заняли большую часть рынка искусственных конечностей. Однако, миоэлектрические методы управления протезами не позволяют человеку в полной мере взаимодействовать с окружающим миром, так как не обеспечивают необходимую подвижность конечности (низкое число степеней свободы), и имеют не естественный для человека метод управления (принудительное сокращение мышц). В связи с этим требуется разработка новых конструкций искусственных конечностей, схожих по строению с человеческой анатомией, а также систем управления, более близких для человека.

В последние годы ведётся активное создания подобных систем. Например, университетом Джона Хопкинса был разработан протез, обладающий 22 степенями свободы и инвазивно соединённый с мышечными волокнами человека, для более точного контроля за конечностью [1]. Данная рука имеет диапазон движений, схожий с человеческим, однако имеет всё так же миоэлектрическую систему управления, и является крайне дорогой.

Как показало исследование [2], лишь 15 % от всех представленных в открытом доступе разработок протезов управляются с помощью электроэнцефалографии, то есть с помощью сигналов мозга, в то время как большая часть управляется сигналами мышечных сокращений. И даже представленные разработки, основанные на управлении с помощью ЭЭГ, имеют низкое число степеней свободы, и как следствие – ограниченный диапазон движений.

1 Конструкция антропоморфной роботизированной руки

Рука человека имеет 27 степеней свободы: по 4 в каждом пальце, по три на разгибание и сгибание и по одной на отведение и приведение; большой палец сложнее и имеет 5 степеней свободы, оставляя 6 степеней свободы для вращения и перемещения запястья [3]. В ходе работы была разработана конструкция пальца роботизированной руки, представленная на рис. 1. В ней каждая фаланга связана с последующей при помощи пружин скручивания.

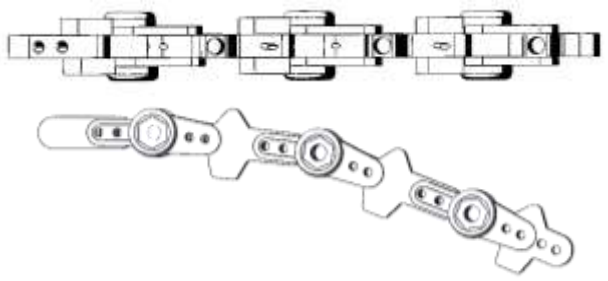
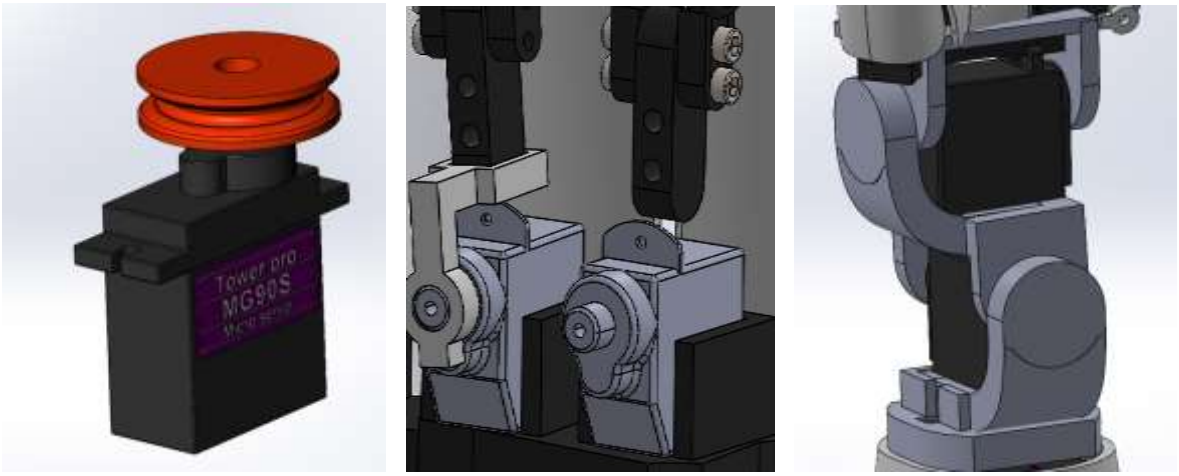


Рис. 1. Конструкция пальца

Фаланги приводятся в движение с помощью нитей, закреплённых на сервоприводах, как показано на рис. 2, а. Сервоприводы расположены в предплечье. Для сокращения дистальных фаланг применяются сервоприводы *mg90s*, которые обеспечивают силу сжатия в 1,8 кг, а для сокращения проксимальных фаланг – сервоприводы *DS-939MG,* которые обеспечивают силу сжатия в 2,5 кг. С помощью диска, закреплённого на выходе редуктора привода, вращательное движение преобразуется в линейное. В дальнейшем планируется использование линейных приводов для сокращения проксимальных фаланг, с целью уменьшения занимаемого ими объёма.

Приведение и отведение пальцев осуществляется напрямую, с помощью закрепления основания пальца непосредственно на редукторах сервоприводов, установленных в кисти, как показано на рис. 2, б. Запястье реализовано с помощью механизма, представленного на рис. 2, в. В нём сервоприводы *mg*995 с усилием 15 кг, связаны напрямую с основными деталями, что позволяет развить наибольшее усилие.



(а) (б) (в)

Рис. 2. Механизмы: а) преобразования вращательного движения привода в поступательное; б) приведения и отведения пальцев; в) механизм запястья

2 Схемотехническая реализация системы управления

Структурная схема системы управления приводами руки приведена на рис. 3. Управляющие команды приходят на контроллер руки через протокол Bluetooth. Контроллер, в свою очередь, следит за тем, чтобы ток, потребляемый сервоприводами, не превысил определённого значения.

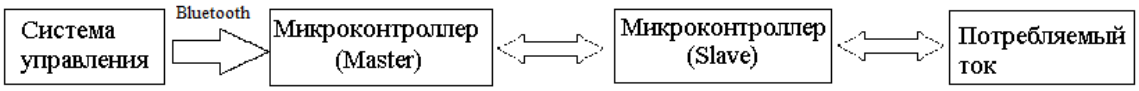


Рис. 3. Структурная схема системы управления

Для измерения тока, протекающего через каждый сервопривод, используется токовый шунт. Измерение тока происходит путем измерения падения напряжения на шунте. Например, при заданной величине максимально допустимого тока в $J_{\text{макс}} = 1$ А и сопротивлении шунта в 0,02 Ом падение напряжения на шунте будет составлять:

$$U_{\text{изм}} = I \cdot R = 1\ \text{А} \cdot 0{,}02\ \text{Ом} = 20\ \text{мВ}.$$

Далее, полученное значение напряжения необходимо сравнить со значением, которое не допустимо превышать. После измерения, сигнал поступает на вход АЦП микроконтроллера *AtTiny24*. Он имеет разрядность 10 бит. Однако, сигнал с амплитудой 20 мВ не получится сравнить с установленным значением. АЦП имеет диапазон измерений $U_{\text{макс}} = 3{,}3$ В, то есть при 10 битах разрядности получаем шаг квантования:

$$U_{\text{кв}} = \frac{U_{\text{макс}}}{2^{10}} = \frac{3{,}3\ \text{В}}{1024} = 0{,}003\ \text{В} = 3\ \text{мВ}.$$

Тогда на диапазон 0...20 мВ, который соответствует изменению тока от 0 до 1 А получим число шагов:

$$n = \frac{U_{\text{изм}}}{U_{\text{кв}}} = \frac{20\ \text{мВ}}{3\ \text{мВ}} = 7\ .$$

Разрядность измерения тока составит:

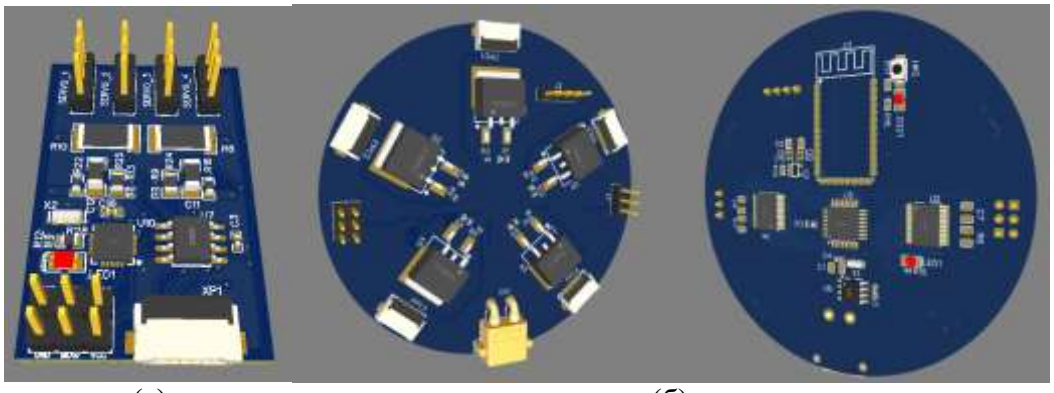
$$k = \frac{J_{\text{макс}}}{n} = \frac{1\text{А}}{7} = 143\ \text{мА}.$$

Для увеличения точности, необходимо усилить измеренный сигнал, перед тем как подавать его на вход АЦП. Для этого воспользуемся операционным усилителем (ОУ). В качестве ОУ используем микросхему *LM358ADR*, которая имеет два ОУ. Рассчитаем усиление:

$$U_{\text{вых}} = U_{\text{вх}} \cdot \left(1 + \frac{R1}{R2}\right) = 0{,}02 \cdot \left(1 + \frac{220\ \text{кОм}}{1{,}2\ \text{кОм}}\right) = 3{,}68\ \text{В}.$$

Спроектирована печатная плата (рис. 4, а), включающая себя микроконтроллер *AtTiny24* и две микросхемы сдвоенного ОУ, что позволяет измерять ток со всех 4 приводов каждого пальца. В сумме для всей руки будет использоваться 5 плат.

После обработки сигналов на микроконтроллере, посылается сигнал на основную плату контроля (рис. 4, б), на которой главный процессор на базе *AtMega328* размыкает ключ на полевом транзисторе, если это лог. 0, и замыкает ключ, если это лог. 1, тем самым обеспечивая защиту приводов от перегрузки по току.



(а) (б)

Рис.4. Внешний вид спроектированной платы:
а) измерения тока через сервоприводы; б) платы контроля

3 Система управления протезом

В работе также рассмотрены пути проектирования системы управления разработанной роботизированной рукой. Для применения её в качестве протеза необходим способ управления, наиболее близкий к естественному контролю человеческими конечностями, то есть основанный на передаче электрических импульсов внутри конечностей.

Прохождение нервных импульсов в конечностях человека происходит через двигательные нейроны, которые получив сигнал от мозга, передают его к исполнительным органам – мышцам. Сам нейрон состоит из тела и отростков – аксона и дендритов, которые дифференцированы по строению и функциям. Аксон является отростком, по которому импульс идет от тела нейрона и передает информацию от мозга. У различных нейронов длина аксона колеблется от микронов до 1,5 м. Именно длинноаксонные нейроны несут функцию связи с эффекторными органами – мышечными клетками, то есть доносят сигнал от мозга к конечностям.

Расшифровать мозговые сигналы достаточно сложно для этого используют специальные методы, такие как электромиография (ЭМГ) и электроэнцефалограмма (ЭЭГ). Первый метод (ЭМГ) предназначен для исследования электрической активности мышц. Путем регистрации биоэлектрических потенциалов, возникающих в скелетных мышцах человека и животных при возбуждении мышечных волокон. Так же в ЭМГ входит электронейрография (ЭНМГ) – исследования передачи нервных импульсов по организму, качества передачи и быстроты отклика на биоэлектрическую стимуляцию. Это исследование требуется для помощи людям с нейродегеративными заболеваниями или при изучении ИМК, который применим и для антропоморфной механической руки. На основе данного метода можно понять и предположить процесс передачи информации и приведения конечности в движение, что помогает в разработке все более эффективных и интуитивно управляемых протезов конечностей.

Второй метод – электроэнцефалограмма (ЭЭГ) – предназначен для изучения и регистрации электрических потенциалов мозга в процессе его жизнедеятельности. Регистрирующие электроды располагаются в определенных областях головы так, чтобы охватить все участки головного мозга. Таким образом, получаемая запись ЭЭГ является суммарной электрической активностью множества нейронов, представленных потенциалами дендритов и тел нервных клеток. Все это отражает функциональную активность головного мозга.

В ходе работы разработана, спроектирована и протестирована работа конструкции и системы управления антропоморфной роботизированной руки, проанализированы возможности создания ИМК методом регистрации и обработки ЭЭГ.

Список используемых источников

1. An Overview of the Developmental Process for the Modular Prosthetic Limb (Johns Hopkins APL Technical Digest, Volume 30, Issue 3, pp. 207–216, 2011)

2. Jelle ten Kate, Gerwin Smit & Paul Breedveld (2017): 3D-printed upper limb prostheses: a review, Disability and Rehabilitation: Assistive Technology, DOI: 10.1080/17483107.2016.1253117

3. EIKoura G, Singh K (2003) Handrix: Animating the human hand. Eurographics/SIGGRAPH Symposium on Computer Animation, eds Breen D, Lin M (The Eurographics Association, Geneva), pp 110–119.

УДК 004.387:621.3.087.93
ГРНТИ 50.09.49

МНОГОРАЗРЯДНЫЙ ПАРАЛЛЕЛЬНЫЙ ЦИФРОАНАЛОГОВЫЙ ПРЕОБРАЗОВАТЕЛЬ ПЕРВОГО ТИПА

А. Э. Гиниятуллин[1], **Ю. А. Никитин**[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский филиал ФГУП НИИР-ЛОНИИР

Основными проблемами при построении параллельных цифроаналоговых преобразователей (ЦАП) являются конечная точность реализации аналоговых элементов (матрицы R-2R, ключей тока – напряжения) во всем выходном диапазоне частот, токов и напряжений. Применение нониусного ЦАП первого типа позволяет обойти или резко уменьшить указанные противоречия.

цифроаналоговый преобразователь, матрица R-2R, ключи тока, ключи напряжения, шаг квантования, арифметический сумматор, аналоговый сумматор, нониус, мерная шкала.

В современном мире технологий существует проблема преобразования цифрового сигнала (кода) в аналоговый сигнал, так как необходимо сохранять высокую точность и быстродействие данного процесса. Для решений подобного рода задач целесообразно использовать параллельные ЦАП, а именно нониусный метод, где исходный сигнал (код) разделяется на 2 группы (старшие и младшие разряды), которые обрабатываются параллельно независимо друг от друга. Таким образом у нас нет необходимости искать ЦАП с достаточно большой точность так как это может нести за собой повышение вероятности ошибки и меньшее быстродействие, будет достаточно двух, которые обладают куда меньшей точностью, но в сумме мы получаем такую же точность без потери остальных параметров [1].

Пример ЦАП, который может обеспечить подобные параметра – ЦАП на матрицах *R-2R*. В таких ЦАП значения разрядов создаются в схеме, состоящей из резисторов с сопротивлениями *R* и 2*R*, называемой матрицей постоянного импеданса, которая имеет два вида включения: прямое – матрица токов, и инверсное – матрица напряжений.

Применение одинаковых резисторов позволяет существенно улучшить точность по сравнению с обычным взвешивающим ЦАП, так как сравнительно просто изготовить набор прецизионных элементов с одинаковыми или близкими параметрами. Наличие таких матриц позволяет добиваться достаточно большой точности с малой вероятностью ошибки, при обеспечении достаточной точности резисторов. Как пример можно рассмотреть схему ЦАП компании *ANALOG DEVICES AD5790* (рис. 1).

В данном ЦАП для формирования 14 старших бит используется лестничная структура *R-2R* матрицы, а для формирования 6 младших бит 63 параллельные источника напряжения, которые подключаются по мере необходимости (рис 2).

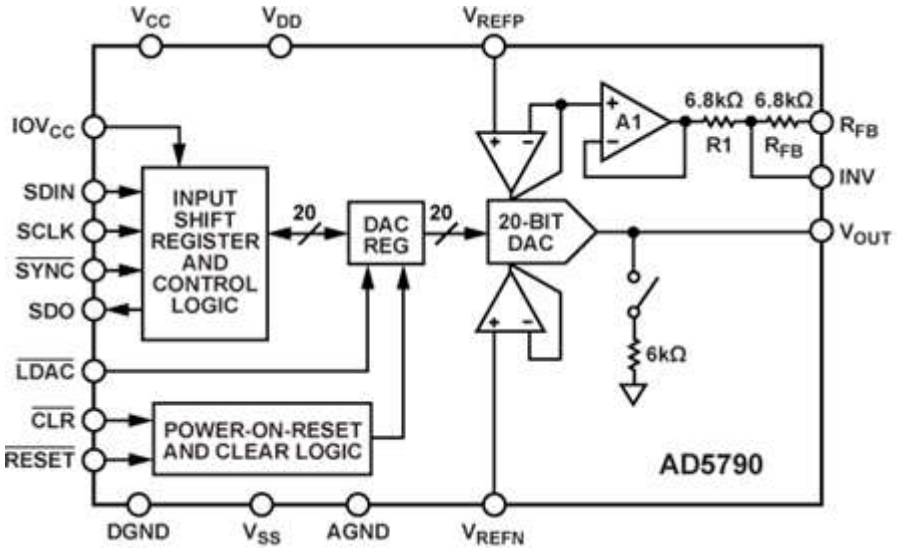


Рис. 1. Схема 20 битного ЦАП AD5790

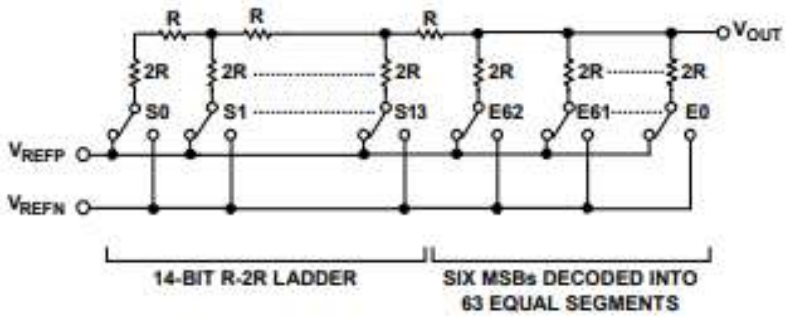


Рис. 2. внутреннее строение 20 битного ЦАП

Аналогичная ситуация обстоит и ЦАП той же компании, но имеющего 18 бит на выходе *AD5780* (рис. 3 и рис. 4).

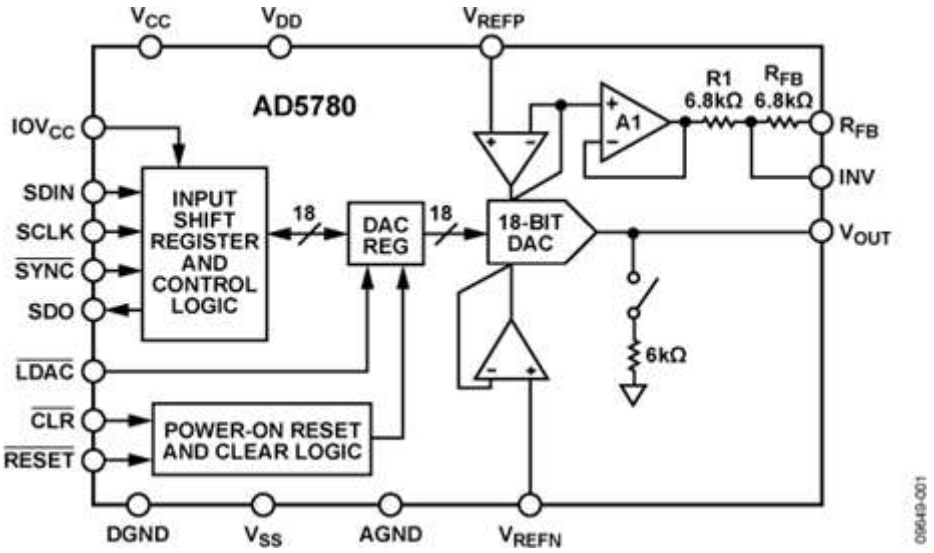


Рис. 3. Схема 18 битного ЦАП AD5780

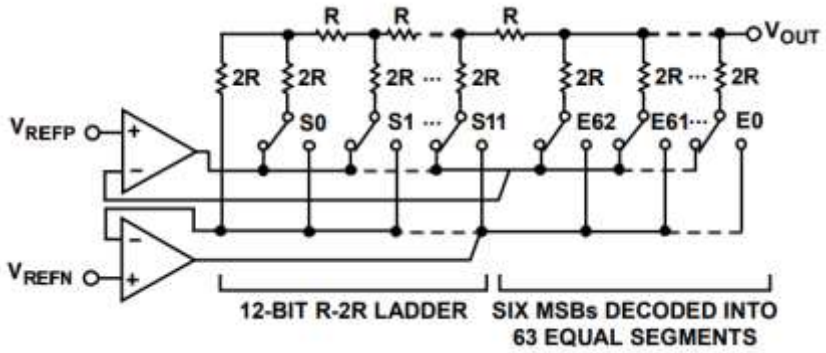


Рис. 4. внутреннее строение 18 битного ЦАП

Работу нониусного ЦАП [1] можно описать следующим образом: имеется арифметический сумматор (1), на входы которого поступают α старших разрядов и β младших разрядов цифрового управляющего слова $\boldsymbol{X}$, причем младшие β разрядов перед этим подверглись цифровому умножению в $\boldsymbol{a}^{\alpha}$ раз (сдвиг влево на α разрядов). Выходная шина арифметического сумматора 6 подключена к входной шине управления ЦАП 1, к другому входу которого подключен выход источника опорного сигнала $\boldsymbol{Y}_1$. Выход ЦАП 1 соединен со входом аналогового сумматора (2), к другому входу которого подключен выход ЦАП 2, на входную шину управления которого поданы $\boldsymbol{a}^{-\alpha}\boldsymbol{N}$ младших разрядов управляющего слова $\boldsymbol{X}$, которые подверглись цифровому умножению в $\boldsymbol{a}^{\alpha}$ раз (сдвиг влево на α разрядов), а другой вход ЦАП 2 соединен с выходом источника опорного сигнала $\boldsymbol{Y}_2$. На выходе аналогового сумматора (2) имеем выходной аналоговый сигнал $\boldsymbol{Z}_0$.

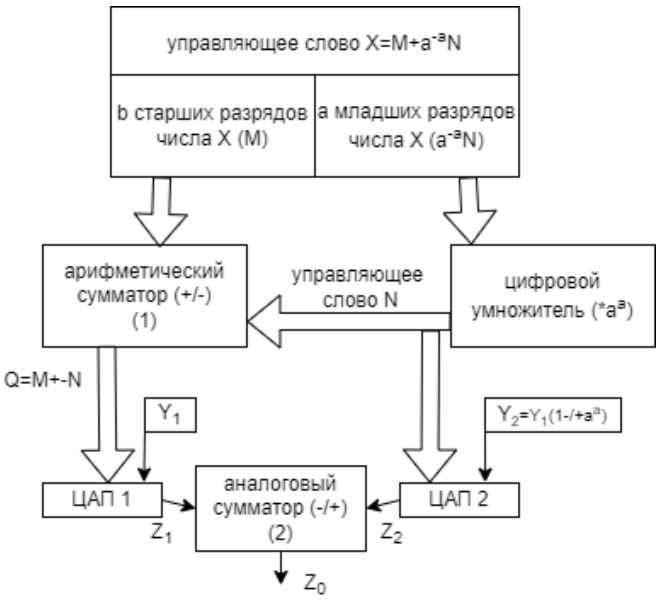


Рис. 5. структурная схема параллельного нониусного ЦАП

Для данного вида ЦАП, чтобы сохранялась точность результата с низкой вероятность ошибки, необходимо связывать опорные сигналы Y_1 и Y_2 жестким соотношением $\boldsymbol{Y_2 = Y_1(1 \mp a^{-\alpha})}$, где $\boldsymbol{a}$ – основание системы счисления, α – число разрядов, на которое сдвинут код управления $\boldsymbol{a^{-\alpha}N}$.

Знак + или – мы выбираем исходя из операции, которая выполняется в арифметическом сумматоре (1): если мы складываем значения *M* и *N*, то зависимость опорных сигналов имеет следующую формулу: $\boldsymbol{Y_2 = Y_1(1 - a^{-\alpha})}$. И на оборот, если в сумматоре (1) мы вычитаем из числа *M* число *N*, то имеем следующую формулу: $\boldsymbol{Y_2 = Y_1(1 + a^{-\alpha})}$. При отклонении от этого правила вероятность ошибки будет повышаться.

Наличие дельта-сигма АЦП разрядности 24 бита [4] и 32 бита [5] и цифровых потенциометров разрядностей 8 и 10 бит разных номинальных значений сопротивлений позволяет на современной элементной базе строить прецизионные ЦАП сверхвысокой разрядности и(ли) сверхбыстродействующие ЦАП высокой разрядности.

Список используемых источников

1. Никитин Ю. А. Способ нониусного цифроаналогового преобразования. Пат. 2703228 Российская Федерация; заявитель и патентообладатель Никитин Ю. А. № 2019107698; заявл. 18.03.2019; опубл. 15.10.2019

2. www.analog.com/media/en/technical-documentation/data-sheets/ad5790.pdf

3. www.analog.com/media/en/technical-documentation/data-sheets/ad580.pdf

4. https://www.ti.com/lit/ds/symlink/ads131e08s.pdf?ts=1643122592538&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FADS131E08S

5. https://www.ti.com/lit/ds/symlink/ads1262.pdf?ts=1643208175077&ref_url=https%253A%252F%252Fwww.ti.com%252Fsitesearch%252Fdocs%252Funiversalsearch.tsp%253FlangPref%253Den-US%2526searchTerm%253Dads1262%2526nr%253D346

УДК 621.396.673
ГРНТИ 29.35.19

ИССЛЕДОВАНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК РАМОЧНОЙ ТРЕУГОЛЬНОЙ СТРУКТУРЫ

Н. И. Глухов, Э. Ю. Седышев, С. И. Федоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе представлены результаты моделирования и эксперимента, а также их сравнение, треугольной рамочной антенны для выявления зависимостей влияния геометрических характеристик (длины ребра, длины отрезка питания) на её электродинамические характеристики.

СВЧ, антенна, треугольная антенна.

Антенна – это неотъемлемая часть любой радиотехнической системы. Основные проблемы требующие решения при проектировании антенны, это её частотные характеристики и как следствие геометрические размеры, значения КСВ, а также поляризация.

Отличным вариантом антенны СВЧ для использования в переносных малогабаритных устройствах, а также для связи модулей ОИС СВЧ, являлась бы малогабаритная широкополосная антенна с круговой поляризацией. В данный момент антенной, отвечающей всем этим запросам, является лишь спиральная антенна. Также в данный момент популярным типом антенн являются фрактальные антенны, стоит заметить, что на данный момент из них выделяются древовидные антенны решающие основную проблему фрактальных антенн – коэффициент усиления.

Следует заметить, что предлагаемая в данной работе структура является скорее не фракталом, а серией вписанных фигур. Также в дальнейшем подразумевается получение круговой поляризации на данной структуре.

Данная статья является продолжением работы, представленной на конференции ПКМ-2021. В ней содержалось общее описание причин выбора данной структуры для дальнейшего исследования, а также описание эксперимента для 10см макета.

После того как был синтезирован десятисантиметровый макет, и получены его характеристики на лабораторном стенде, следовало понять, как изменение геометрических размеров антенны влияет на изменение её электродинамических показателей.

Последующее моделирование производилось в среде MMANA-GAL.

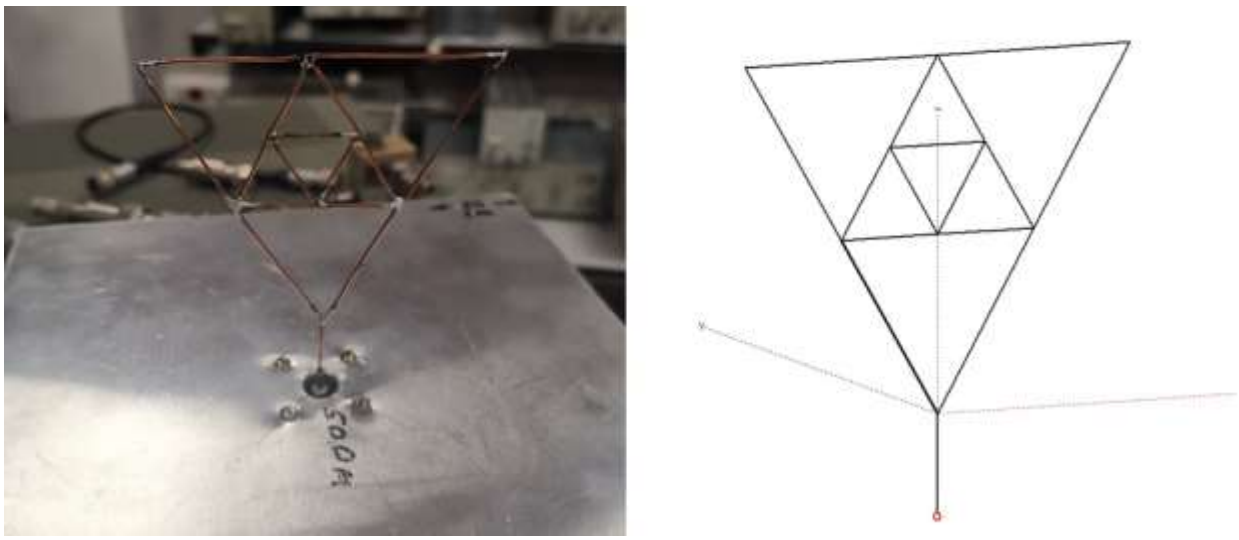


Рис. 1. Синтезированная модель 8 см антенны и её аналог в среде *MMANA-GAL*

Была создана модель, представленная на рис. 1. Представляющая из себя серию треугольников с отрезком питания.

Первой задачей было определить влияние длины отрезка питания на показатели антенны. Для этого в среде MMANA-GAL было рассчитано три модели с длинами отрезков 26, 22 и 20 мм (рис. 2)

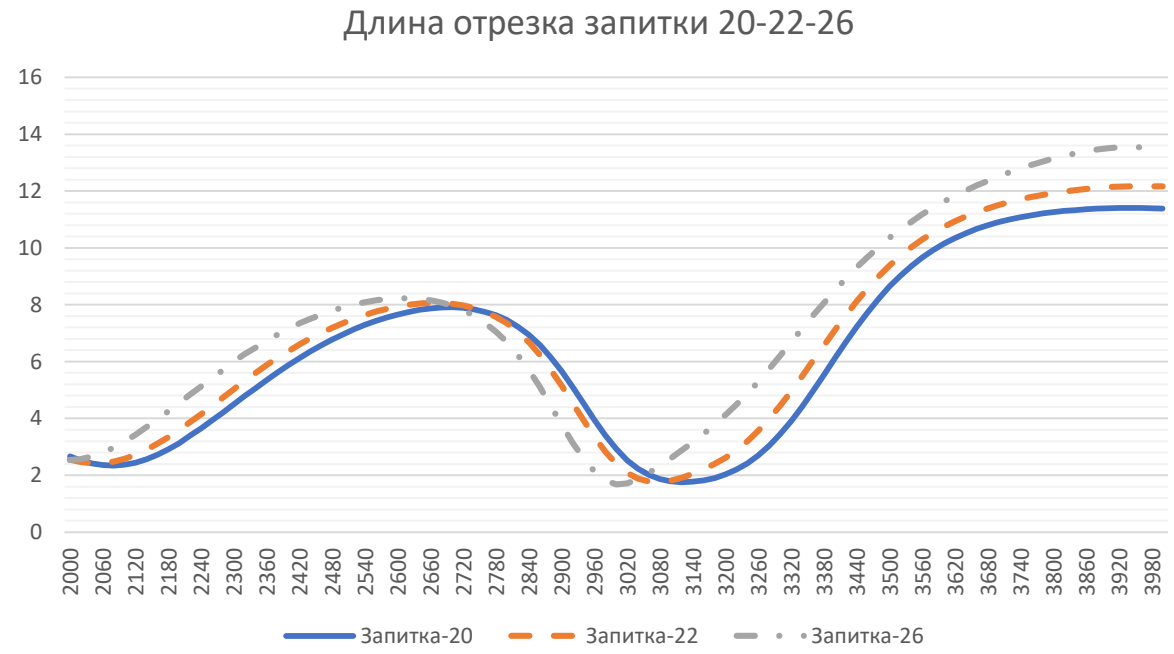


Рис. 2. Три модели с длинами отрезков 26, 22 и 20 мм, рассчитанные в среде MMANA-GAL

Из-за незначительного отличия, и дальнейшего облегчения синтеза модели был выбран отрезок длинной 20 мм.

Следующим шагом, следовало определить влияние длины ребра треугольника на показатели антенны. Для сравнения были выбраны модели с 8-ми, 10-ти и 12-ти сантиметровыми рёбрами (рис. 3).

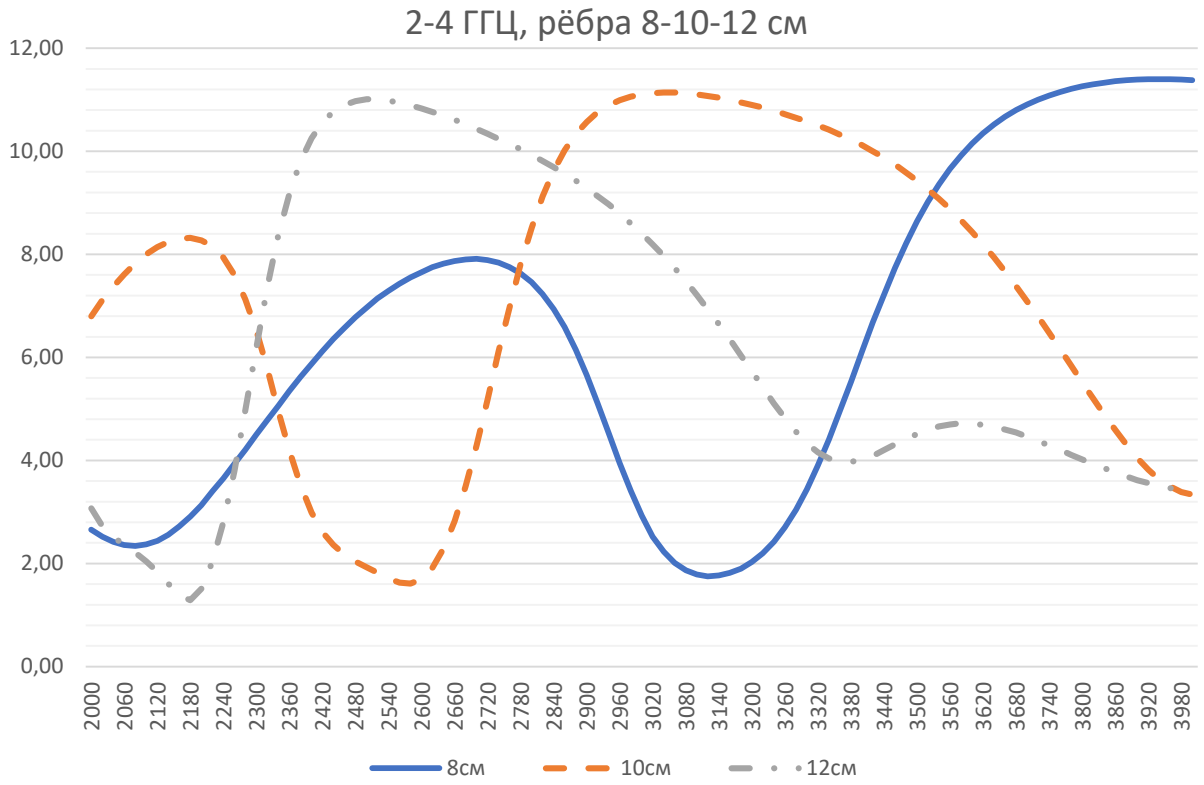


Рис. 3. Модели с 8-ми, 10-ти и 12-ти сантиметровыми рёбрами, отрезок 2–4 ГГЦ

Графики в пределах 2–4 ГГЦ были получены для дальнейшего сравнения с экспериментом, но уже по полученным данным можно понять, что ожидаемое смещение в сторону НЧ, при увеличении длины ребра, происходит с незначительным изменением формы графика и ещё меньшим изменением максимальных и минимальных значений КСВН.

Для лучшего сравнения разницы в зависимостях КСВН от длины ребра и частоты были выбраны треугольники со сторонами 8 и 10 см, а также был увеличен отрезок исследуемых частот с 2–4 ГГЦ до 2–8 ГГЦ (рис. 4).

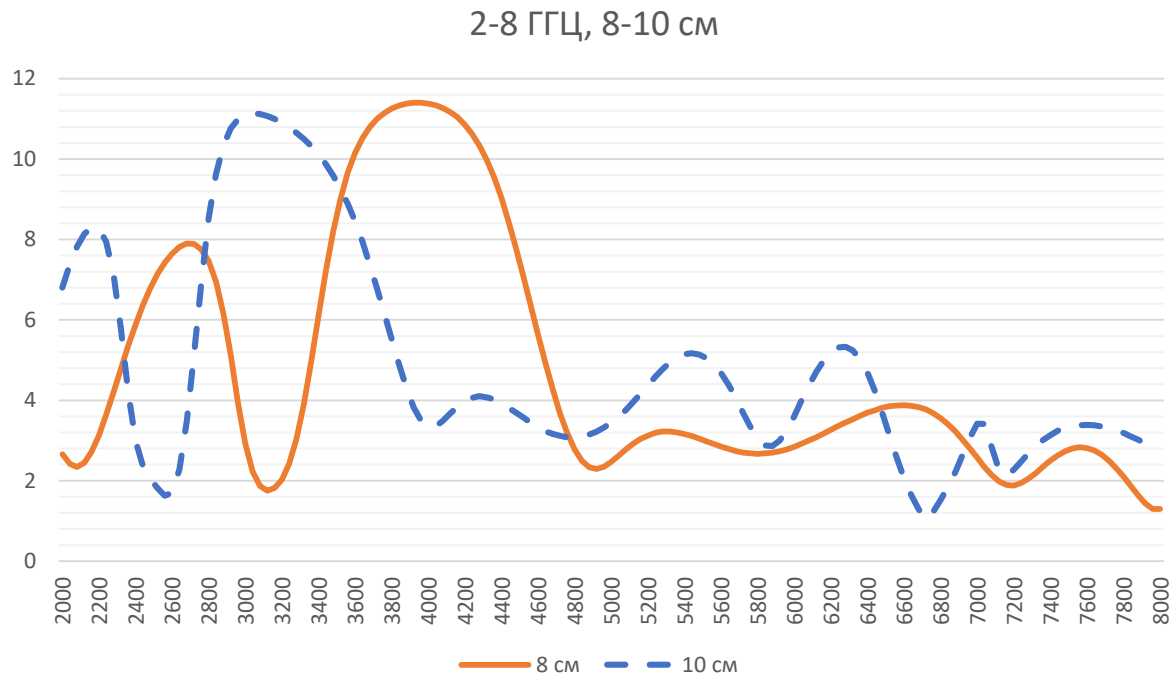


Рис. 4. Треугольники со сторонами 8 и 10 см, отрезок 2–8 ГГЦ

По графику получаем – минимумы КСВН для восьмисантиметровой антенны 3.12 и 8 ГГЦ, для десятисантиметровой – 2.56 и 6.72 ГГЦ, что соответствует длинам волн ~ 9,6 и 3,5 см для восьми см и ~ 11,7 и 4,46 см для десяти см.

Далее была синтезирована модель восьмисантиметровой антенны (рис. 1) для изучения на лабораторном стенде.

Первой задачей было проверить зависимость КСВ реальной антенны от длины отрезка питания.

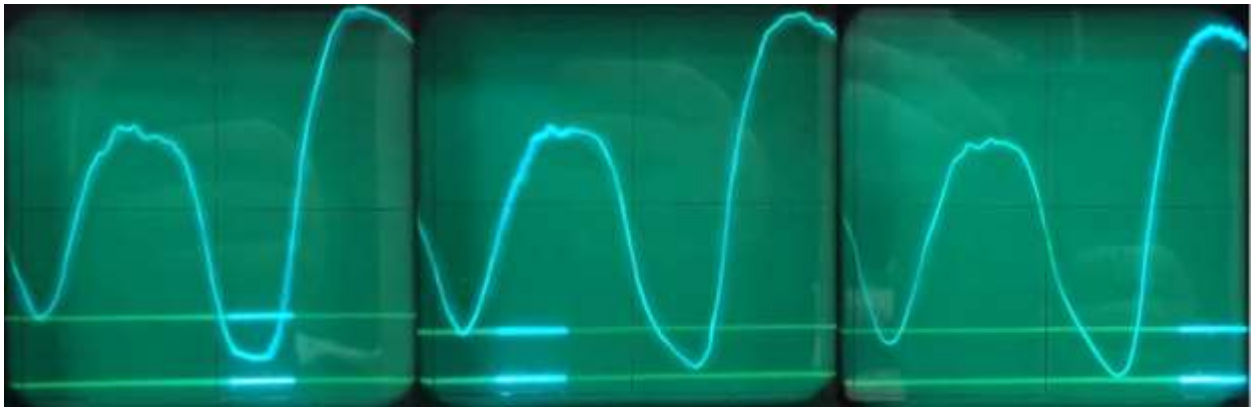


Рис. 5. Слева-направо отрезки питания 26-22-20 см

По результатам измерений были получены следующие данные (рис. 5):

- Длина 26 мм, минимумы: 2.156 ГГц – КСВ 2, 3.148 ГГц – КСВ 1.6;
- Длина 22 мм, минимумы: 2.23 ГГц – КСВ 1.8, 3.35 ГГц – КСВ 1.4;

•Длина 20 мм, минимумы: 2.245 ГГц – КСВ 1.7, 3.325 ГГц – КСВ 1.21.

Следовательно, хотя нельзя было наблюдать прямой зависимости изменения частот минимумов КСВН от длины отрезка, однако явно изменялись сами значения КСВН.

Следует заметить, что изменения КСВН могли быть вызваны неточностями в земле антенны. Было решено провести измерения с другим экраном, который приведён на рис. 1.

По итогам второго эксперименты была получена зависимость, представленная на рис. 6.

Длина отрезка питания 20 мм, минимумы: 2.147 ГГц – КСВ 3.23, 3.04 ГГц – КСВ 2.6 соответственно.

После наложения графиков получим рис. 7.

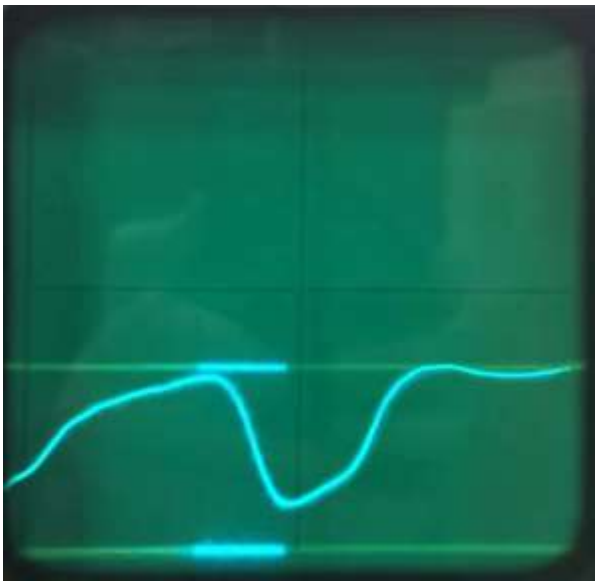


Рис. 6. Зависимость КСВН от частоты для треугольника со сторонами 8 см и отрезком питания 20 мм с новым экраном

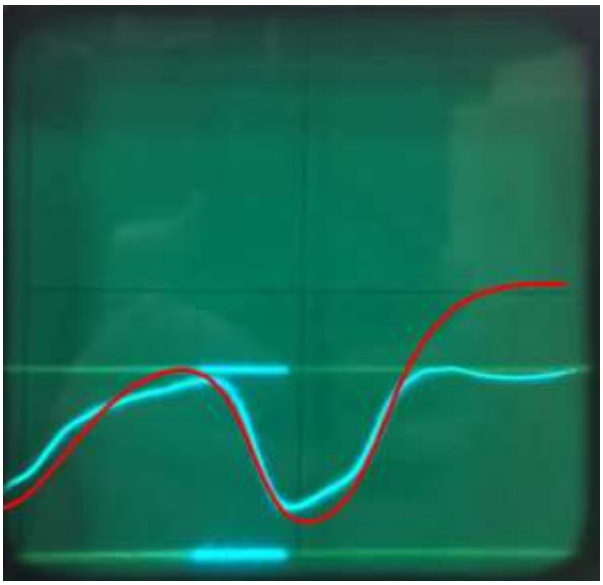


Рис. 7. Наложение графиков эксперимента и моделирования на отрезке 2–4 ГГЦ

Последним, следовало сравнить зависимость КСВ от частоты с различным количеством вписанных треугольников (рис. 8).

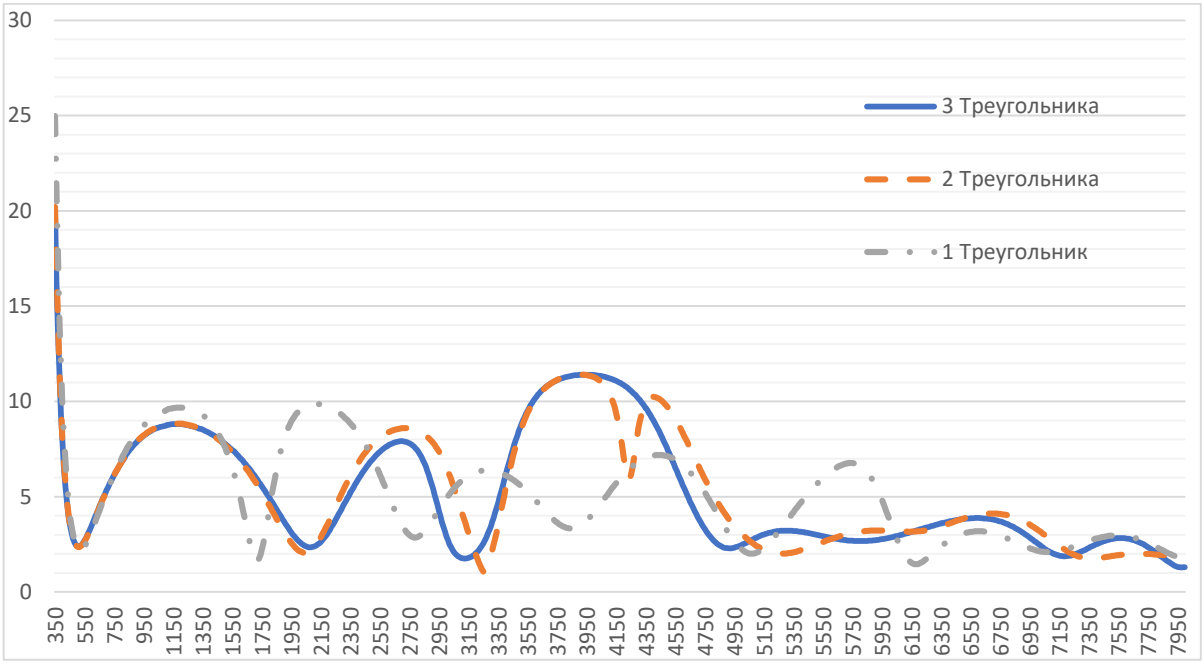


Рис. 8. Сравнение зависимости КСВ от частоты
с различным количеством вписанных треугольников

По результатам моделирования, можно увидеть, что увеличение количества вписанных треугольников ведёт к изменению зависимости КСВ (к примеру, постепенное слияние 2-х максимумов в один в области 4 ГГЦ, или смещение минимумов в область НЧ без вписанных треугольников).

К тому же можно заключить, что при увеличении частоты антенна с максимальным количеством вписанных треугольников имеет наилучшие электродинамические характеристики.

В результате данного исследования было проведено моделирование и макетирование треугольной рамочной антенны. Получена сходимость результатов эксперимента и моделирования.

Определено наличие влияния отрезка питания на характеристики антенны. Установлено влияние геометрических размеров на электродинамические характеристики антенны, а также влияние количества вписанных фигур на зависимость КСВ при увеличении частоты. Требуется дальнейшее, более точное описание влияния количества вписанных фигур на КСВ, а также выявление способов уменьшения КСВ (различные виды питания антенны и т. д.).

Дальнейшим развитием работы планируется рассмотрение способов получения круговой поляризации на данной или подобной структуре.

Список используемых источников

1. Бочаров Е. И., Ветров В. В., Седышев Э. Ю., Усатова И. А. Планарные излучатели объёмных интегральных схем СВЧ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2016. С. 176–181.

2. Банков С. Е., Давыдов А. Г., Папилов К. Б. Малогабаритные печатные антенны круговой поляризации // Журнал радиоэлектроники. 2010. N 8. С. 2.

3. Алли Р. А., Седышев Э. Ю. Частотные свойства древовидных фрактальных антенн // X Всероссийская научно-техническая конференция "Электроника и микроэлектроника СВЧ". Сб. докладов. Санкт-Петербург. 31 мая – 4 июня 2021 г. СПб.: СПбГЭТУ «ЛЭТИ». 629 с.

4. Фальковский О. И. Техническая электродинамика : учебник. 2-е изд., стер. Санкт-Петербург : Лань, 2009. 432 с.

5. Фейнмановские лекции по физике. Т. II (3 – 4) / Фейнман Ричард, Лейтон Роберт, Мэтью Сэндс; перевод с английского]. Москва: изд-во АСТ, 2021. 496 с.

6. Потапов А. А. Фрактальная электродинамика. численное моделирование малых фрактальных антенных устройств и фрактальных 3d микрополосковых резонаторов для современных сверхширокополосных или многодиапазонных радиотехнических систем // Радиотехника и электроника. 2019. Том 64, № 7. С. 629–665.

УДК 621.396.67
ГРНТИ 47.45.99

СИНТЕЗ И КОНСТРУИРОВАНИЕ МИКРОВОЛНОВЫХ ФИЛЬТРОВ

Н. И. Голубенко, А. Р. Кубалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлен алгоритм проектирования полосковых эллиптических структур дециметрового и сантиметрового диапазонов. Представлена методика создания микроволнового золотарёвского фильтра путем параллельного соединения двух решёток связанных линий одинаковой и неодинаковой электрических длин с применением теории стержневых фильтров. Рассмотрен числовой пример расчета микрополосковых эллиптических фильтров, реализованных на решетках связанных полосков с использованием теории стержневых фильтров.

фильтр Золотарёва-Кауэра, узкополосный фильтр, стержневой фильтр, микроволновый фильтр, связанные микрополосковые линии, многопроводная линия, электромагнитное моделирование, метод конечных элементов

Представлена методика создания микроволнового золотарёвского фильтра путем параллельного соединения двух решёток связанных линий

и использования теории стержневых фильтров. В предыдущих методиках синтеза выходы и входы частотно-разделительных устройств находились на одной и той же стенке корпуса, что вызывало серьезные проблемы при синтезе данных устройств. В описанных ранее методах синтеза микроволновых эллиптических фильтров данный вопрос решался подключением к фильтру вспомогательных шлейфов соединительных линий, что значительно ухудшало электрические характеристики цепи (например: затухание, КСВН, плотность тока на поверхности проводника и т. д.), а также увеличивало массогабаритные показателей фильтра.

В предлагаемой к ознакомлению методике расчета фильтра описан иной, новый метод включения цепи в СВЧ тракт за счёт использования четырёх, а не двух, как было предложено ранее, трансформирующих секций и подсоединения к цепи еще двух дополнительных портов. Таким образом, в статье представлена четырёхпортовая структура фильтра с практически полностью совпадающими характеристиками затухания при четырёх различных способах включения данного фильтра в СВЧ тракт.

В соответствие с техническим заданием выбирается фильтр-прототип нижних частот (ФПНЧ) из многочисленных схем ФПНЧ, рассчитанных в таблицах справочника Рудольфа Зааля [1]. Применяя частотное преобразование от ФПНЧ к полосовому фильтру (ППФ) и преобразование Ричардса, то есть воспользовавшись двойным частотным преобразованием Ричардса, осуществляется переход от ФПНЧ на сосредоточенных элементах к полосовому фильтру на резонаторах одной электрической длины (рис. 1).

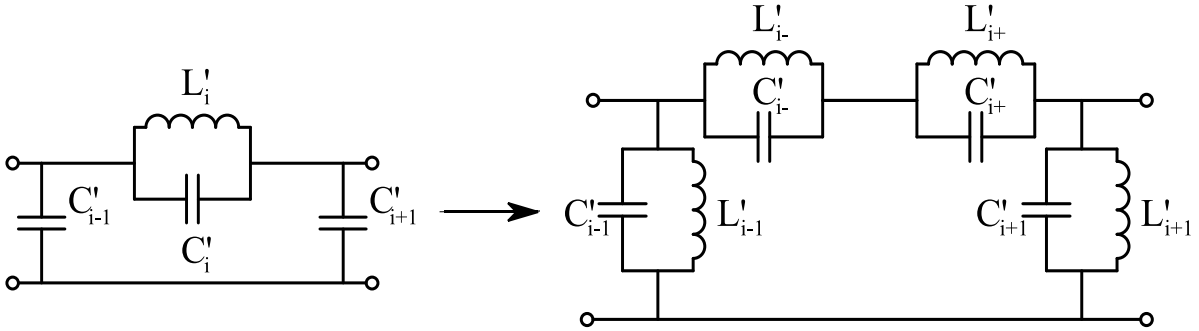


Рис. 1. Частотное преобразование подсхемы ФПНЧ Золотарёва-Кауэра в подсхему полосового фильтра Золотарёва-Кауэра

Если полная электрическая длина резонатора будет эквивалентна π, то величина θ_0 ограничивается как $\pi/6 \le \theta_0 \le \pi/3$. Определив θ_0 (при этом θ_0 обычно выбирается эквивалентной $\pi/4$), следует перейти от конструкции из короткозамкнутых и незамкнутых шлейфов к конструкции из двухсторонне закороченных полуволновых шлейфов неодинаковой длины со скачком волнового сопротивления в соответствующем сечении θ_0. Входные

нагрузки первоначальной и видоизмененной схем будут значительно согласовываться друг с другом только в довольно узкой частотной полосе (примерно до 3–5 %). Таким образом, требуемую схему можно создать путём в параллельного объединения двух лестничных подсхем *A* и *B*, состоящих из закороченных шлейфов. Электрическая длина при центральной частоте f_0 элементов подсхемы *A* будет равна θ_0 и электрическая длина на центральной частоте f_0 элементов подсхемы *B* будет равна $\pi - \theta_0$ (рис. 2).

Подсхемы *A* и *B* при переходе от электрического расчета к конструктивному представляют собой параллельно соединённые в точке скачка волнового сопротивления закороченные на землю связанные линии. Рассчет параметров многопроводных линий передачи практически выгодно осуществлять, используя матрицы нормированных проводимостей (нормированных сопротивлений) или нормированных ёмкостей. Значения элементов матриц определяются из соответствующих уравнений [2, 3]. Для синтеза физически возможной конструкции цепи для подсоединения нагрузок ко входу и выходу фильтра в подсхему *A* вводят единичные элементы, которые практически при конструктивном расчёте представляют собой встречно-стержневую связанную линию (чья электрическая длина равна θ_0), закороченную на землю в точке скачка волновых сопротивлений внутренних стержней и подключённую к нагрузке с незакороченной стороны. На основании известной теории многопроводных линий, два дополнительных узла вводятся в матрицу подсхемы *A*.

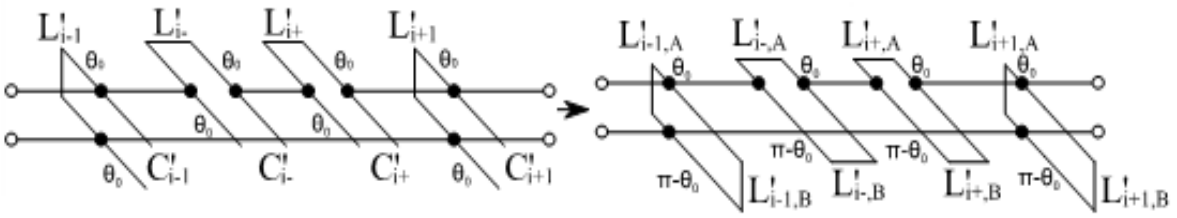


Рис. 2. Узкополосное преобразование подсхемы золотарёвского ППФ

В двухпортовых фильтрах количество узлов в подсхеме *B* не поменяется. Такая конструкция имеет только одно решение – она позволяет включить устройство в СВЧ тракт лишь только когда и выход и вход находятся с лишь одной стороны. Поскольку в описываемой структуре шлейфы подсхемы *B* в свою очередь замкнуты на землю, возможно модифицировать её путем внесения в подсхему *B* дополнительных двух единичных элементов соответствующей электрической длины $\pi - \theta_0$ (рис. 3).

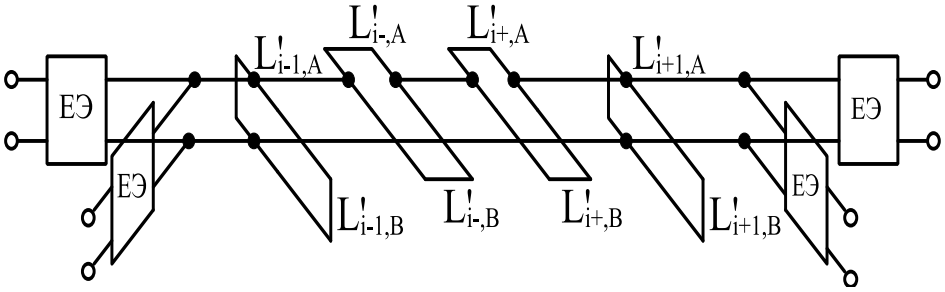


Рис. 3. Схема модифицированного золотарёвского фильтра с четырьмя портами

Геометрические размеры связанных линий определяются с использованием графиков Гетзингера [4] или методом электромагнитного моделирования.

На рис. 4 изображена структура микроволнового ступенчатого золотарёвского фильтра третьего порядка, реализованного путём включения в схему четырех портов. Его исходные данные: центральная частота f_0 = 2 215 МГц, относительная ширина полосы пропускания ω = 1,1287 %, ширина полосы пропускания Δf = 25 МГц, $\theta_0 = \pi / 4$ подключаются для работы взаимосоответствующие пары портов: П1-П2, П2-П3, П3-П4, П1-П4, когда же любой из портов П2, П1 не включен в тракт, он должен работать в режиме короткого замыкания, когда любой из портов П4, П3 не включен в тракт, он будет работать в режиме холостого хода.

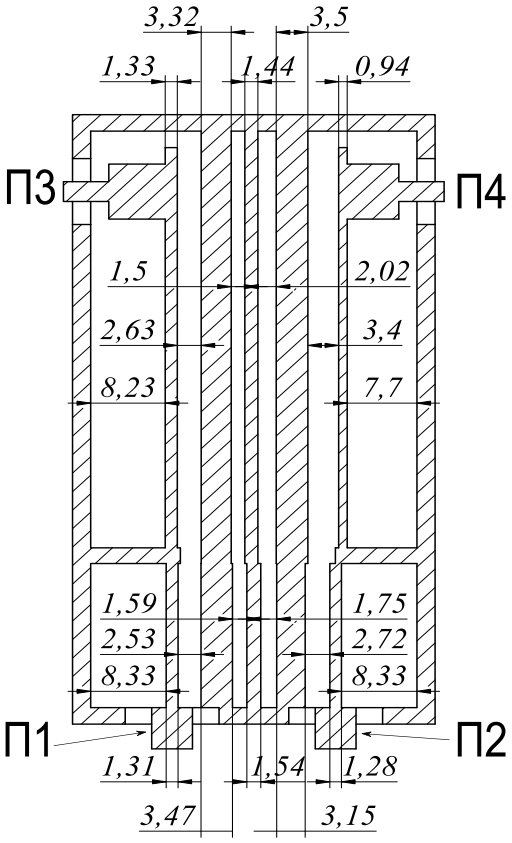


Рис. 4. Конструкция эллиптического фильтра с включением четырёх портов

В электромагнитном модуле программы HFSS была сформирована трёхмерная структура фильтра для анализа с использованием алгоритма конечных элементов. Результаты анализа при четырех различных типах подсоединения портов к тракту отображены на рис. 5. Результаты теоретических исследований микроволнового ступенчатого фильтра Золотарева-Кауэра, реализованного с введением в цепь четырех портов показали, что характеристики затухания устройства практически полностью совпадают при различных методах включения его в СВЧ тракт.

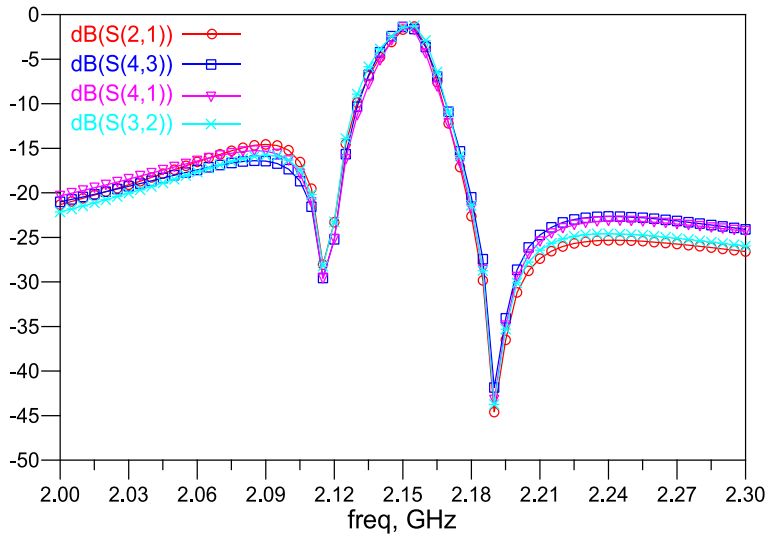


Рис. 5. Результаты электродинамического моделирования затухания фильтра

Список используемых источников

1. Зааль Р. Справочник по расчету фильтров. М.: Радио и связь, 1983. 752 с.

2. Jia-Sheng Hong, Lancaster M. J. Microstrip filters for RF/Microwave applications. N. Y.: John Wiley & sons. Inc., 2001. P. 482.

3. Кубалова А. Р., Томашевич С. В. Анализ и синтез микроволновых эллиптических фильтров. СПб: Издательство СПбГУТ, 2013. 368 с.

4. Getsinger W. J. Coupled rectangular bars between parallel plates // Microwave Theory and Techniques, IEEE Transactions on. 1962. Vol. 10. Pp. 65–72.

УДК 535.317.24, 621.326
ГРНТИ 29.31.15, 29.31.26, 47.14.07

МЕТОДИКА РАСЧЕТА ПЕРВИЧНОЙ И ВТОРИЧНОЙ ОПТИКИ ПОЛУПРОВОДНИКОВЫХ ИЗЛУЧАЮЩИХ ДИОДОВ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАДАННОГО СВЕТОРАСПРЕДЕЛЕНИЯ

В. В. Гришин, Е. Д. Петрова, О. Б. Тёрушкина, М. Д. Трофимушкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Задачей оптических расчетов при проектировании полупроводниковых светоизлучающих диодов (светодиодов) является получение оптической системы, которая позволяет вывести максимально возможное количество световой энергии от первичного источника (p-n-перехода, на котором происходит рекомбинация электрон-дырочных пар с выделение энергии оптического диапазона, пропорциональной ширине запрещенной

зоны) в заданный угол. Традиционно эта задача решается установкой полимерной линзы на кристалл полупроводника.

Использование алгоритмов расчета первичной оптики светодиодов позволяет численно решить задачи определения профиля купола линзы при проектировании светодиодов с целью повысить их энергетическую эффективность, обеспечить требуемое распределение светового потока, излучаемого полупроводниковой структурой. В работе рассмотрены существующие методы такого анализа, проведена оценка их точности.

светодиоды, полупроводниковая техника, оптика, световой поток, освещённость.

На данный момент электроника, основанная на полупроводниковой технологии, приблизилась к пределу скорости передачи сигнала, поскольку полупроводниковый транзистор, лежащий в основе таких логических схем, не позволяет получить частоты свыше 100 ГГц [1]. Это мотивировало инженеров искать новые пути развития электроники связи, в результате чего в устройствах современной фотоники носителем сигнала служит волна оптического или ИК-диапазона электромагнитного спектра. Предел передачи оптических линий связи гораздо выше. Например, мультиплексация линий передачи сети Интернет в оптоволокно позволяет вести передачу на терагерцовых частотах, что выше «кремниевого» предела на 3 порядка [4]. Кроме того, фотонные элементы позволяют работать с более низкими энергозатратами, а также избегать радиопомех. Одним из вариантов технической реализации является использование высокоэффективных излучающих диодов инфракрасного диапазона. Общая структура и принципы работы диодов подробно изложены в [2] и [3].

Проблемами передачи сигнала с помощью полупроводниковых излучателей оптического диапазона являются потери, связанные с полным внутренним отражением в кристалле, а также высокие требования к светораспределению конечного изделия, соблюдение которых не представляется возможным на уровне кристалла [2]. Одним из вариантов решения проблемы является использование линзы с куполом сферической формы. В таком случае форма диаграммы направленности задаётся расстоянием от плоскости монтажа кристалла до вершины линзы. Несмотря на широкое применение, такие линзы не всегда способны обеспечить желаемое распределение светового потока, излучаемого кристаллом [3].

Оптика, рассчитываемая в ходе проектирования и изготовления светодиода, необходима для создания наиболее концентрированного излучения в нужном угловом диапазоне, контроля яркости получаемого света и повышения эффективности устройства. Проектирование оптики требует соответствующих методик, разработка и практическое применение которых является целью данной работы.

С момента создания светодиодных устройств была необходимость в направленной концентрации их излучения в определённом пространственном диапазоне. Частично эта проблема была решена с использованием преломляющих линз, установленных поверх излучающего элемента. Чаще всего для данных целей применяются обычные полусферические линзы. Они уменьшают потери на полном внутреннем отражении и формируют нужное распределение светового потока, однако являются достаточно неэффективным решением в этом вопросе, а расчёт для них, как правило, не проводится. Необходимо сделать выделяемую энергию более полезной, чем она есть в среднестатистическом устройстве. Для движения в эту сторону нами была поставлена задача разработать такой алгоритм определения формы линзы светодиода, чтобы испускаемое через неё излучение соответствовало требуемым конструкторским параметрам, т. е. выполнялось соответствие полученной диаграммы направленности излучения заданной. В этом методе кристалл полупроводника представляется как Ламбертовский источник света, т. е. источник, излучающий световой поток равномерно во все стороны. Такое приближение позволяет с большой точностью получить необходимую диаграмму направленности несмотря на то, что в реальности кристалл излучает неравномерно.

В ходе выполнения работы был проведён анализ научной и специализированной литературы, описывающей принципы работы светодиодов, ход лучей через преломляющую поверхность и применение законов оптики. Также был произведён анализ уже существующих приборов и методов по получению необходимого светового потока через подбор формы линзы. Далее по заданной диаграмме направленности был определён угол, на который нужно изменить первоначальный угол падения, путём последовательного вычисления пространственного угла и дальнейшего пересчёта его в угол преломлённого луча. После этого с определённой долей приближения были определены касательные в нужных точках пространства и сформирована искомая поверхность линзы светодиода. Наконец было проведено сравнение заданной и полученной в ходе расчётов диаграмм направленности, после чего был сделан вывод об их сходстве и высокой точности метода.

Первостепенно была решена задача нахождения формы первичной оптики, позволяющая вывести максимально возможное количество энергии от первичного источника излучения – полупроводникового кристалла. Получить данный результат возможно при использовании полимерной линзы требуемой формы, которая в свою очередь позволяет как сформировать необходимую диаграмму направленности светового потока, так и обеспечить требуемое значение мощности излучения кристалла. По имеющимся данным о входящем и требуемом выходящем световых потоках были рассчитаны необходимые углы выходящих лучей. Затем для каждого из них был

определён угол наклона касательной плоскости к преломляющей поверхности линзы, обеспечивающий данный угол выхода. Также с использованием интерполяции определили искомую форму линзы, которая соответствует требованиям. Используя законы оптики, мы рассчитали элементы с соответствующим функционалом и подходящие к требуемым условиям.

Таким образом, в ходе работы были изучены методы расчёта первичной оптики при проектировании полупроводниковых излучающих диодов. В процессе анализа информации по соответствующей теме были выделены наиболее оптимальные методики. Были рассмотрены основные этапы, требования к световыводящим частям светодиодных устройств, необходимые исходные данные для расчётов параметров первичной оптики светодиодов. Следуя данным алгоритмам, можно быстро получить наиболее точное представление распространения светового потока в оптической системе, что позволяет провести моделирование и подобрать наиболее подходящую элементную базу для формирования требуемой оптики при любой длине волны излучения. Следующим этапом работы является проведение расчёта первичной и вторичной оптики для полупроводникового излучателя по сформулированному методу сопоставления потоков излучения по обе стороны границы раздела «полимерная линза-внешняя среда». Согласно методу строятся модели оптической системы, обеспечивающей формирование заданной диаграммы направленности излучения. При этом физическая реализуемость характеристик рассчитываемого полупроводникового излучателя позволяет говорить о возможности экспериментальной проверки полученных данных.

Список используемых источников

1. Досколович Л. Л., Моисеев М. А. Расчёт преломляющих оптических элементов для формирования диаграммы направленности в виде прямоугольника // Оптический журнал. 2009. Т. 76, № 7. С. 70–76.

2. Берг А., Дин П. Светодиоды / Пер. с англ. Под ред. А. Ю. Юновича. М.: Мир, 1979. 220 с.

3. Коган Л. М. Полупроводниковые диоды: современное состояние // Светотехника. 2000. № 6. С. 11–15.

4. Якушенков П. О. Фотонные интегральные схемы // Фотоника. 2017. № 8. С. 58–67.

УДК 621.396.677.75
ГРНТИ 47.45.29

АНТЕННАЯ РЕШЁТКА НА ДИЭЛЕКТРИЧЕСКИХ СТЕРЖНЯХ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ

М. В. Державин, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе приведено сравнение зеркальных параболических антенн и диэлектрических рупоров. Рассматриваются основные проблемы применения антенн этих типов в спутниковых системах связи. В результате моделирования создан макет единичного диэлектрического стержня, проведён эксперимент, сделаны выводы о возможности объединения таких антенн в решетку, целесообразности и перспективах применения предложенной конструкции в системах спутниковой связи.

СВЧ, диэлектрическая антенна, спутниковая связь.

СВЧ антенны востребованы на сегодняшний день в системах спутниковой связи. Имеющиеся проблемы применения параболических антенн и диэлектрических рупоров приводят к поиску новых структур, например, к антенной решётке на диэлектрических стержнях, целесообразность синтеза которой рассматривается в данной статье.

Для спутникового телевидения используются два основных диапазона: Ku-диапазон (10,7–12,75 ГГц) и С – диапазон (3,5 – 4,2 ГГц). Европейские спутники вещают преимущественно в Ku-диапазоне. Российские и азиатские спутники ведут вещание в обоих частотных диапазонах.

У зеркальной антенны электромагнитное поле концентрируется за счёт отражения волны от металлической поверхности параболического зеркала, называемого рефлектором. В качестве приемника волны обычно выступает небольшая антенна, располагаемая в фокусе зеркала.

Зеркальные параболические антенны обладают громоздкими размерами (0,5–3 м) и большой массой от 3 до 100 кг.

Рупорные антенны представляют собой конический или пирамидальный рупор, соединенный с круглым или прямоугольным волноводом. В частности, облучатель параболической антенны является маленькой рупорной антенной. При равном коэффициенте усиления уровень боковых лепестков рупорной антенны меньше, чем у параболического зеркала, значит, достижим более низкий уровень шума. Коэффициент использования поверхности у рупорных антенн ниже, чем у параболических, а главным их недостатком

является конструкция. Рупорные антенны слишком тяжелые и поставить их на поворотный механизм затруднительно, также усложняются требования к месту и способу установки этих антенн.

Из описанного выше можно сделать вывод, что имеющиеся проблемы применения параболических антенн и рупоров заключаются в больших габаритах и массе, а также в трудностях с установкой и юстировкой.

В связи с обозначенными проблемами предлагается исследовать возможность использования антенной решетки на диэлектрических стержнях.

Диэлектрическая антенна состоит из одного или нескольких конусообразных диэлектрических стержней диаметров около полуволны и длиной 2–10 длин волн. Каждый стержень возбуждается четвертьволновым активным вибратором. Энергия к вибраторам подводится коаксиальным фидером или волноводом.

Принцип работы диэлектрической антенны заключается в следующем: поверхность раздела между двумя средами с резко различными электрическими свойствами вызывает движение электромагнитных волн вдоль поверхности раздела. Такой поверхностью может быть поверхность раздела между проводником и изолятором или двумя изоляторами с разными диэлектрическими проницаемостями, к ним относятся диэлектрические стержни. Если внутри круглого диэлектрического стержня поместить источник электромагнитных колебаний, то такой диэлектрический волновод будет канализировать электромагнитную энергию вдоль всей своей длины. Потери на излучение будут тем меньше, чем резче различаются материалы стержня и окружающая среда по диэлектрической проницаемости.

Для проверки возможности и целесообразности реализации ФАР на диэлектрических стержнях был произведён расчёт поперечного сечения по формуле 1 [3] (для одной частоты диапазона спутниковой связи). Также произведем расчет поперечного сечения стержня для создания масштабного макета.

$$S = (0.1 \div 0.25)\frac{\lambda_0^2}{\varepsilon - 1}. \quad (1)$$

Для частоты Ku – диапазона получаем:

$$S_{\min} = 90 \text{ мм}^2$$
$$S_{\max} = 225 \text{ мм}^2,$$

для C – диапазона имеем:

$$S_{\min} = 610{,}03 \text{ мм}^2$$
$$S_{\max} = 1525 \text{ мм}^2$$

Из расчёта видно, что габариты единичного стержня для частот спутниковой связи будут малы.

Рассчитанные габариты масштабного макета диэлектрической стержневой антенны С–диапазона приведены ниже:

– длина стержня для макета: 360 мм
– диаметр свободный: 35 мм
– диаметр приёмный: 38 мм

Материал: фторопласт ($\varepsilon = 2$).

Конструкция стержня проработана в программном обеспечении КОМПАС-3D с учётом рассчитанных характеристик.

На рис. 1–2 изображены 3D модели диэлектрического стержня.

Рис. 1. Диэлектрическая стержневая антенна, выполненная в программном обеспечении КОМПАС-3D

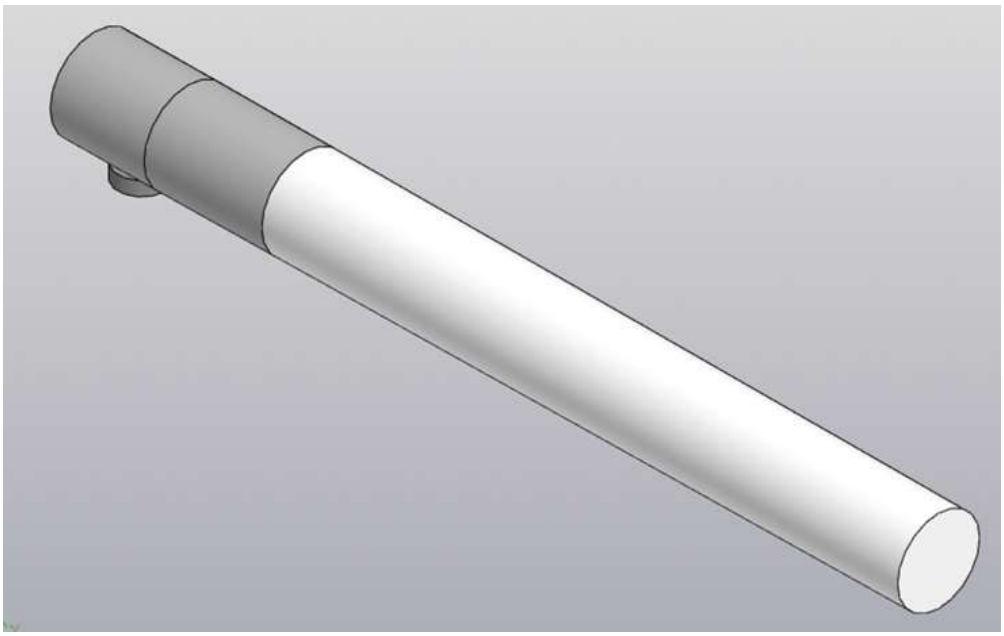


Рис. 2. Диэлектрическая стержневая антенна, выполненная в программном обеспечении КОМПАС-3D

Далее был изготовлен масштабный макет (рис. 3). На торец стержня, вблизи которого расположен активный вибратор, была одета металлическая обойма, выполняющая функцию рефлектора.

Рис. 3. Синтезированный масштабный макет

Первый эксперимент с показанным на рис. 3 макетом показал, что длины рефлектора вдоль стержня недостаточно, поэтому длина коаксиального отрезка была увеличена. Полученный макет представлен на рис. 4.

Рис. 4. Синтезированный масштабный макет с увеличенным рефлектором

Измерительный стенд и результаты измерения представлены на рис. 5 и 6.

Рис. 5. Измерительный стенд синтезированного макета диэлектрической антенны

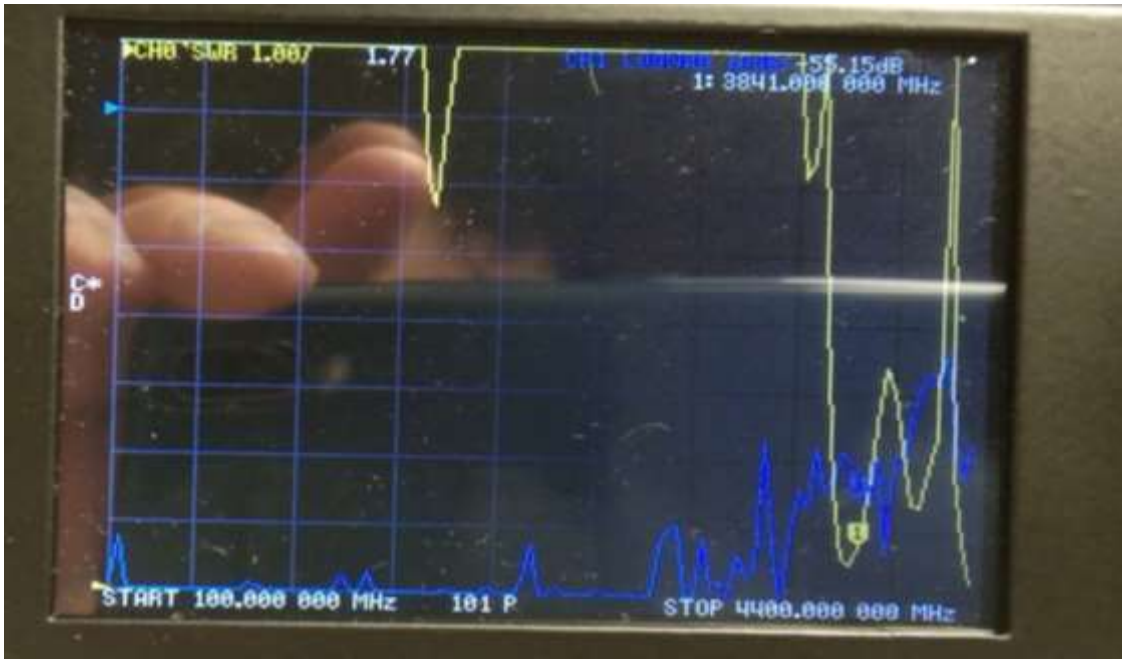


Рис. 6. Результаты измерений КСВ в диапазоне 0,1–4,4 ГГц

Результаты измерений КСВН синтезированного макета на векторном анализаторе в диапазоне 0,1–4,4 ГГц показали, что КСВН макета оказался

равен 1,77 на частоте 3,841 ГГц. Полученные результаты говорят о том, что данная структура является хорошим излучателем. Согласно принципу электродинамического подобия, данная структура будет работать и в диапазоне спутниковой связи. Сужение стержня к его концу приведёт к уменьшению уровня боковых лепестков и большему коэффициенту усиления. Объединение таких структур в антенную решётку целесообразно для дальнейшего сужения диаграммы направленности. Стоит также отметить, что в диапазоне спутниковой связи диэлектрическая антенная решётка будет иметь малые размеры и вес по сравнению с параболическими и рупорными антеннами (включая диэлектрические рупора), что является ее очевидным преимуществом.

Список используемых источников

1. Павлов И. Д., Караев Я. В., Кот М. А. Сверхширокополосная диэлектрическая стержневая антенна // Известия вузов России. Радиоэлектроника. 2020. Т. 23, № 2. С. 38–45.

2. Воскресенский Д. И., Гостюхин В. Л., Максимов В. М., Пономарев Л. И. Устройства СВЧ и антенны / Под редакцией Д. И. Воскресенского. Изд. 3-е, исп. и доп. М.: Радиотехника, 2008.

3. Благовещенский В. П. Основы радиотехники сверхвысоких частот. Ленинград: Судпромгиз, 1952. 420 с.

УДК 621.372.54
ГРНТИ 47.45.99

ВХОДНОЙ ДЕЛИТЕЛЬ МОЩНОСТИ ДЛЯ ДИПЛЕКСЕРА В ОБЪЕМНОМ ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

В. Н. Дорохин, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрен способ реализации делителя мощности для диплексера в объемном интегральном виде. Предложена структурная схема, а также создан рабочий макет Т-делителя.

СВЧ, делитель мощности, объёмная интегральная схема.

В данной работе исследуется способ реализации делителя мощности для микроволнового диплексера в объёмном интегральном виде. Создание

такого устройства поможет подвести сигнал ко входам двух фильтров, располагающихся на разных слоях объёмной интегральной схемы.

На рис. 1 представлена принципиальная схема создаваемого нами делителя мощности.

На рис. 2 представлена 3D модель создаваемого делителя мощности, собранная в программе TFlex.

Данная модель (рис. 2) состоит из четырех слоев диэлектрика и пяти проводящих слоёв. Первый и пятый слои это микрополосковые линии, третий слой – симметричная полосковая линия, второй и четвертый слои – земля.

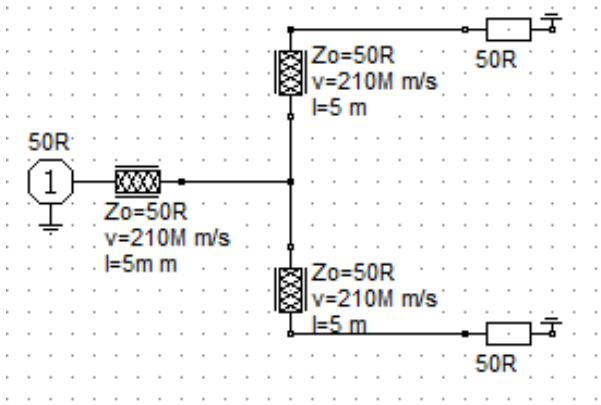


Рис. 1. Принципиальная схема делителя мощности, собранная в программе RFSim99

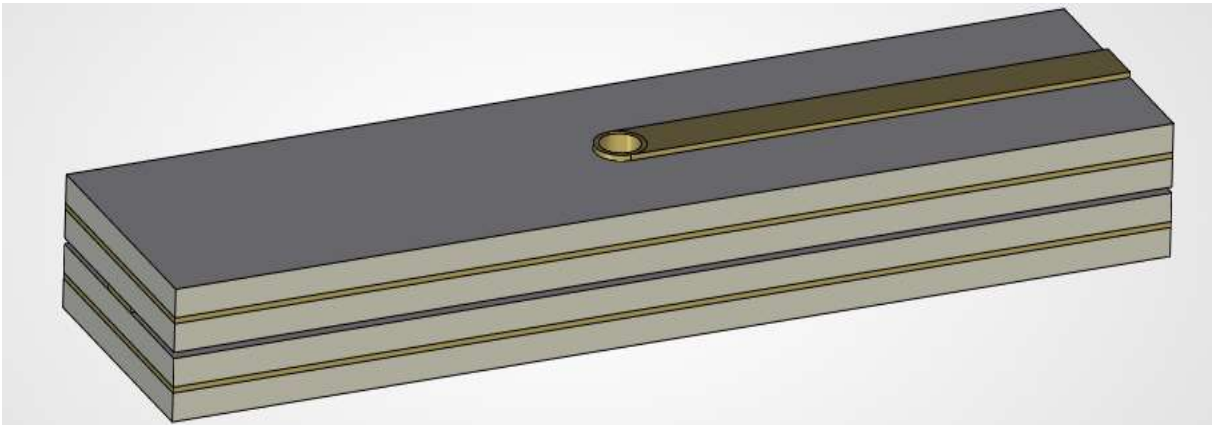


Рис. 2. 3D модель создаваемого делителя мощности, собранная в программе TFlex

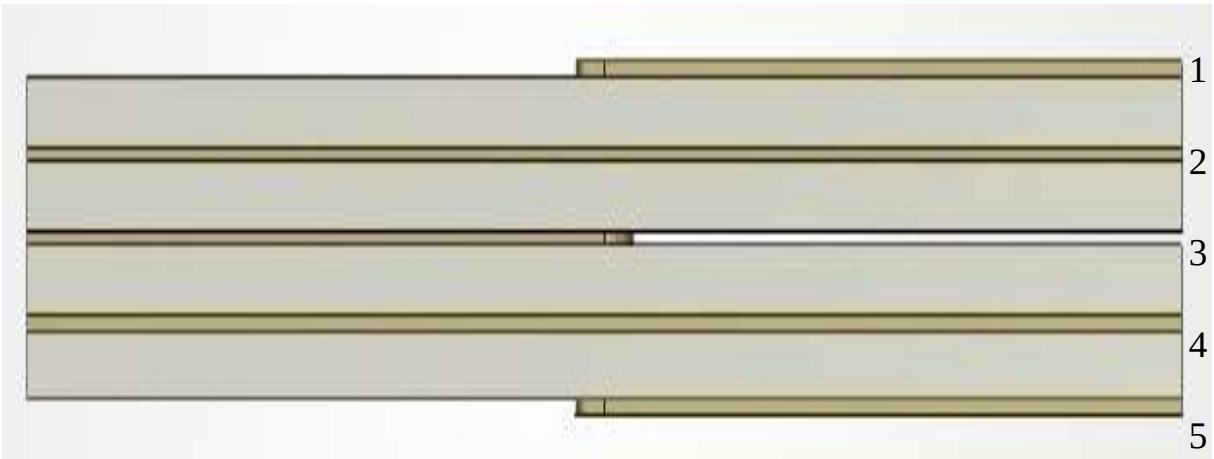


Рис. 3. 3D модель создаваемого делителя мощности, собранная в программе TFlex (вид сбоку)

Подача сигнала на вход делителя осуществляется по симметричной полосковой линии, расположенной в середине объёмной интегральной схемы. Сам делитель представляет собой цилиндрический проводник, напоминающий по структуре своего расположения коаксиальный кабель [1]. На рис. 4 наглядно представлен внешний вид слоев рассматриваемого делителя мощности в объемном интегральном исполнении, сверху – проводящие линии, снизу – земля.

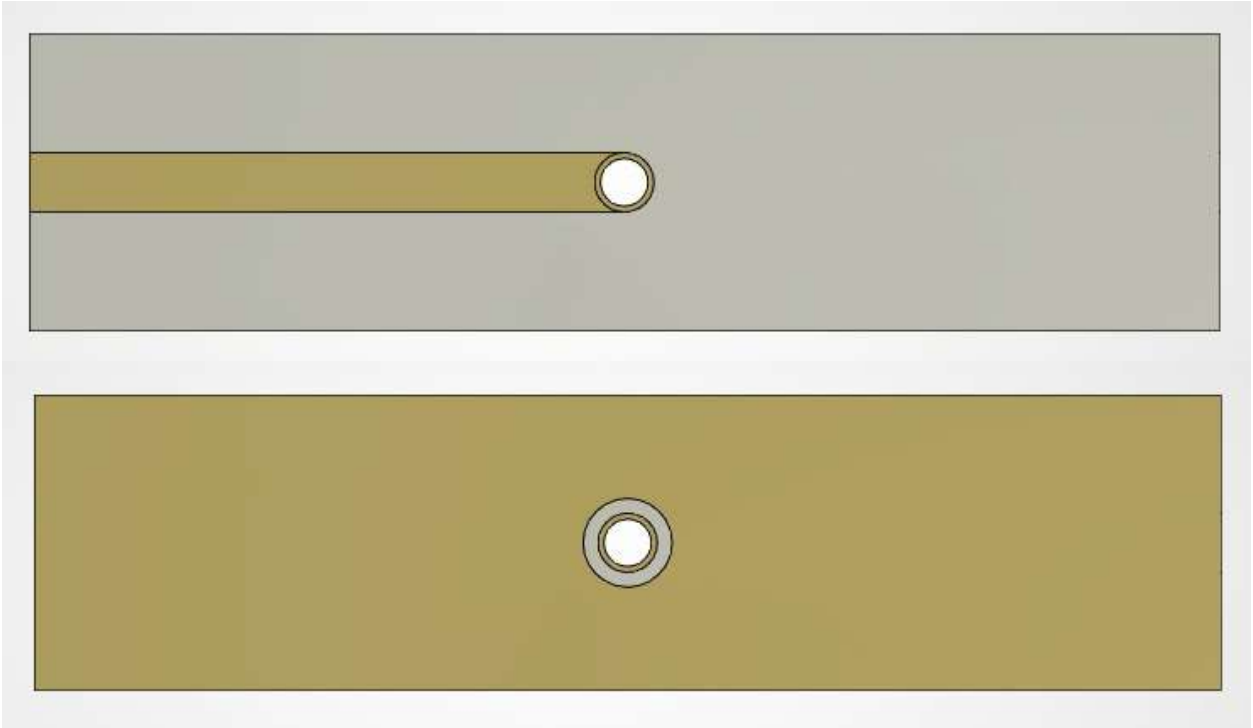


Рис. 4. Внешний вид слоёв делителя мощности

После расчета всех линий передачи в программе RFSim99 была создана схема реального устройства, изображенная на рис. 5 [2].

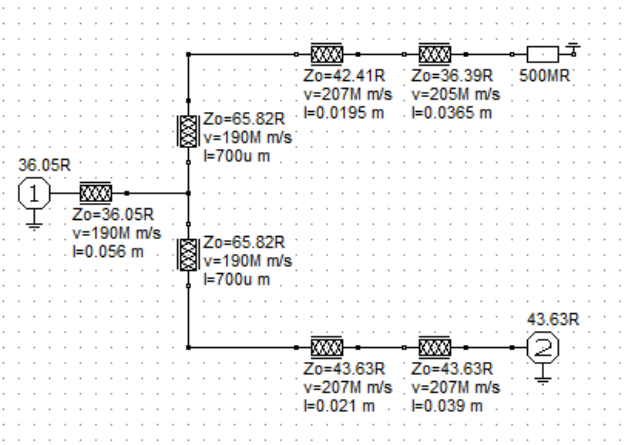


Рис. 5. Реальная модель, собранная в программе RFSim99

А также был произведен анализ частотных характеристик данной модели, изображенных на рис. 6 и 7, из которых видно, что одним из рабочих диапазонов устройства, при нагрузке одного из выходов на холостой ход являются частоты 1 100–2 500 МГц, а при согласованной нагрузке достигается нужное ослабление сигнала в 3 дБ.

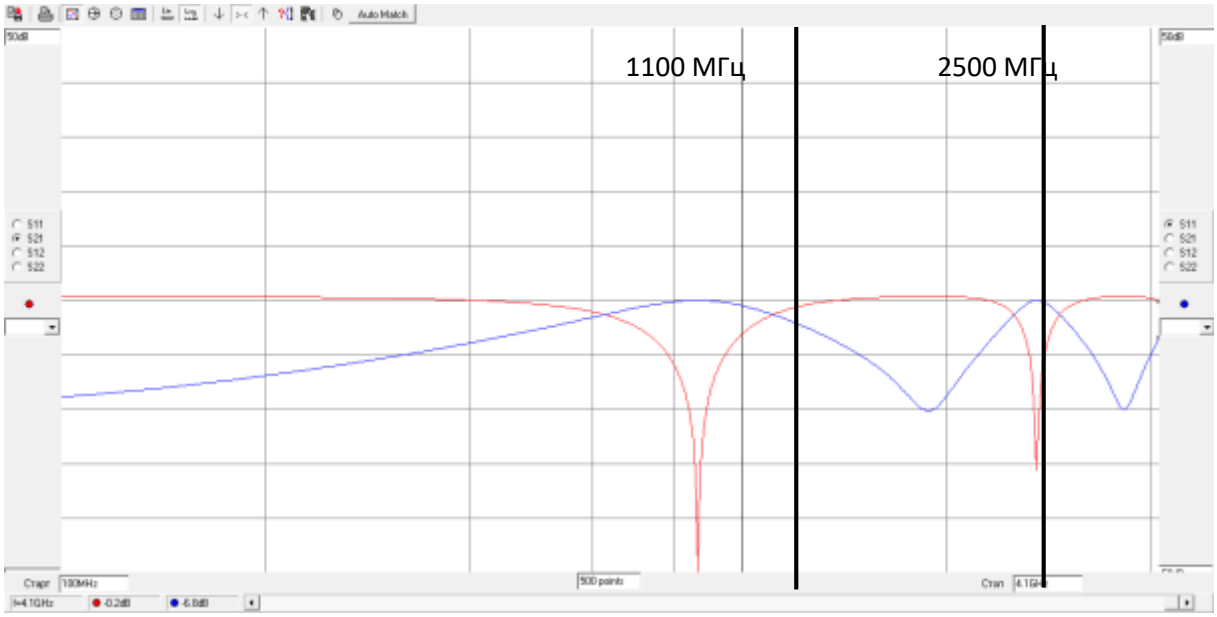


Рис. 6. Частотные характеристики реальной модели в RFSim99 при XX

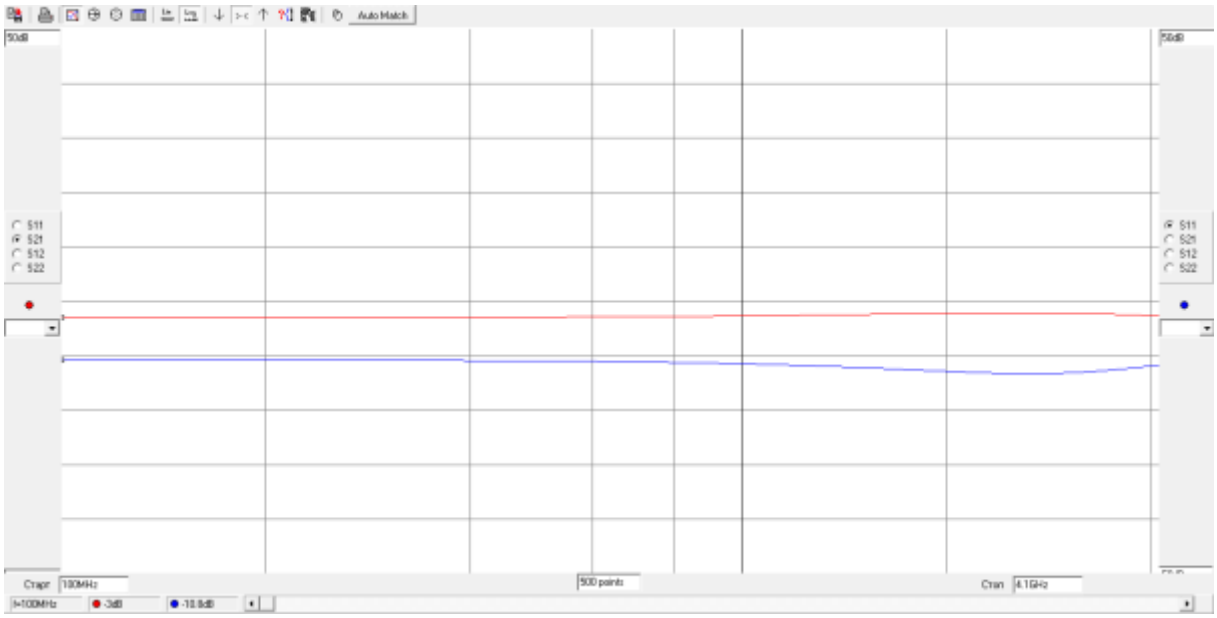


Рис. 7. Частотные характеристики реальной модели в RFSim99
при согласованной нагрузке на обоих выходах

После расчета всех линий передачи в программе RFSim99 был создан рабочий макет устройства, который изображен на рис. 8 [3].

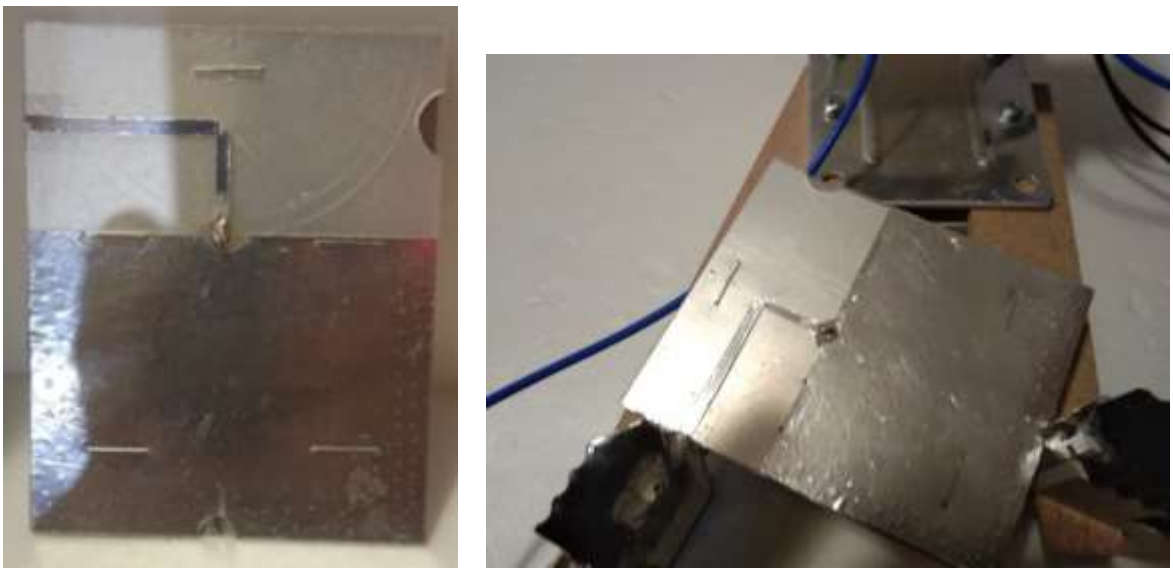


Рис. 8. Рабочий макет делителя мощности в объемном интегральном виде

Для уменьшения затрат на технологические процессы при изготовлении модель устройства была усовершенствована, данный макет состоит из двух слоев диэлектрика и трех проводящих, области земли были размещены на одном уровне с проводящими линиями. Далее на рис. 9 представлены частотные характеристики данного макета (КСВ и ослабления).

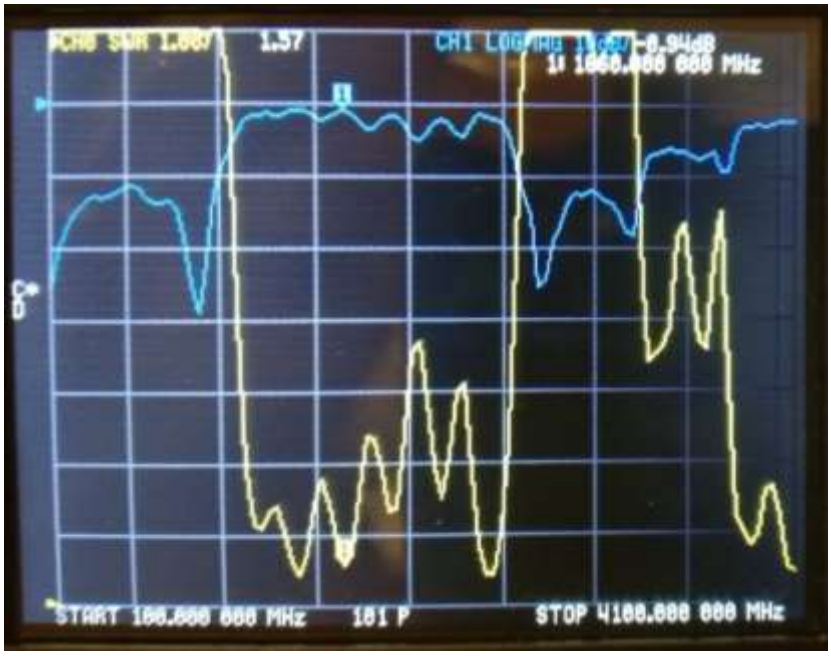


Рис. 9. Частотные характеристики макета делителя мощности

Анализируя получившиеся графики, можно заметить, что данное устройство работает в пределах от 1 100 до 2 600 МГц, что совпадает с ожи-

даниями, ослабление в рабочей полосе варьируется от 1 до 4 дБ, можно сделать вывод что при согласовании второго выхода можно добиться нужного нам ослабления в 3 дБ, что и будет соответствовать делению сигнала на 2.

В результате работы был смоделирован, рассчитан и создан рабочий макет делителя мощности, в дальнейшем планируется использовать данное устройство для реализации диплексера в объемном интегральном виде.

Список используемых источников

1. Гвоздев В. И., Нефедов Е. И. Объемные интегральные схемы СВЧ. М.: Наука. Главная редакция физико-математической литературы, 1985.

2. Вольман В. И. Справочник по расчету и конструированию СВЧ полосковых устройств. Москва: «Радио и связь», 1982.

3. Седышев Э. Ю. Масштабное макетирование объемных интегральных схем СВЧ-диапазона // Актуальные проблемы инфотелекоммуникаций в науке и образовании: Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2012. С. 379–382.

УДК 621.396.67
ГРНТИ 47.45.29

ЭЛЕКТРОДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПЛАНАРНОЙ СИСТЕМЫ ИЗ 4-Х ЩЕЛЕВЫХ ИЗЛУЧАТЕЛЕЙ

Р. И. Дунаева, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрена возможность синтеза планарной антенной системы из 4-х щелевых излучателей, с помощью электродинамического ядра NEC проведено компьютерное моделирование системы. Математически доказана полная работоспособность системы, выявлены основные элементы модели, оказывающие влияние на характеристики системы в целом. Изготовлены масштабные макеты системы и проведена серия экспериментов.

планарная система, щелевой излучатель, электродинамическое моделирование.

Планарная система из щелевых излучателей – одна из самых интересных СВЧ структур [1, 2]. Планарный излучатель обладает свойством конформности, что позволяет с легкостью интегрировать его в объемные интегральные схемы СВЧ, а также получить антенну практически любой формы и размеров. Щелевой планарный излучатель дает возможность разработки

работоспособной структуры в узкой полосе частот. Подбирая источник питания излучателей, решается вопрос с поляризацией антенной системы.

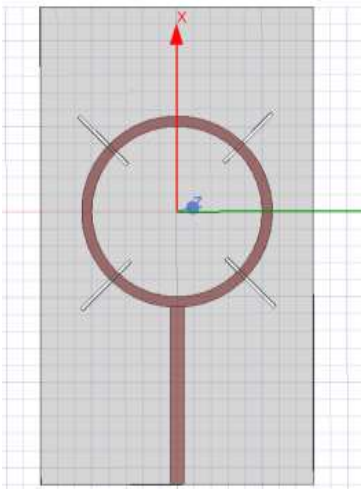


Рис. 1. 3*D*-модель излучателя со щелями на нижней стороне

В результате исследования [3] была получена антенная система, работающая в узком частотном диапазоне, структура которой позволяла теоретически добиться круговой поляризации системы в целом (рис. 1). Электродинамическая модель кольцевого эллиптического резонатора была создана с помощью ЭД пакета Mmana Gal (рис. 2). Доказательство излучающей способности системы приведено на рис. 3.

Рис. 2. Электродинамическая модель кольцевого резонатора

Для получения круговой поляризации антенной системы была выбрана структура «мальтийского креста». Такой излучатель обладает идеальной круговой диаграммой направленности и легко интегрируется в ОИС. В качестве основы был взят квадрат со стороной 10 см и четырьмя ортогональными щелями с длиной щели, примерно равной половине длины волны, и варьируемой шириной щели. Согласно расчетам, рабочая частота данной модели около 3 ГГц (рис. 4).

Важными параметрами, оказывающими существенное влияние на работу всей антенной системы, и, в частности, на КСВн и ширину полосы пропускания, являются ширина щелей и способ их питания. На рис. 5 представлена зависимость КСВн системы от ширины щелей. Как можно заметить, данные характеристики не имеют прямой зависимости. Однако, из графиков видно, что при различных размерах щели, ширина полосы пропускания системы меняется незначительно, система остается узкополосной.

Рис. 3. Макет излучателя со щелями на нижней стороне

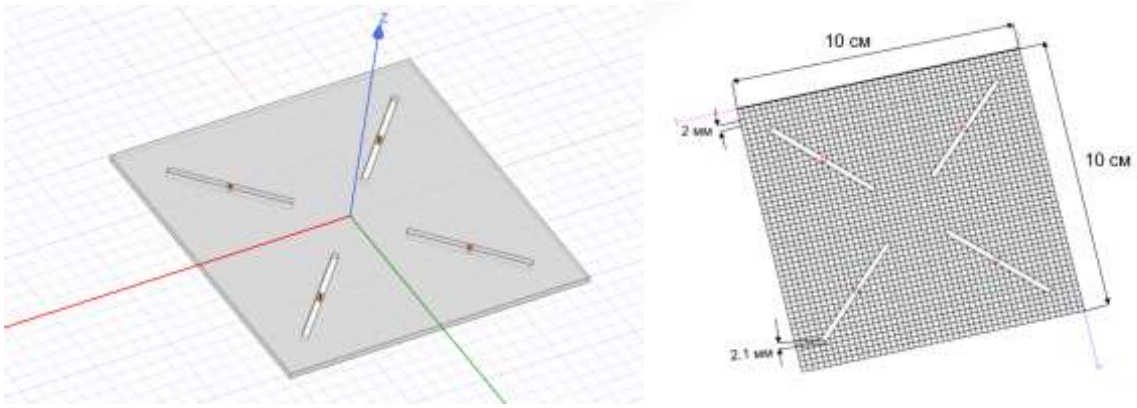


Рис. 4. 3*D* модель и электродинамическая модель щелевой антенной системы

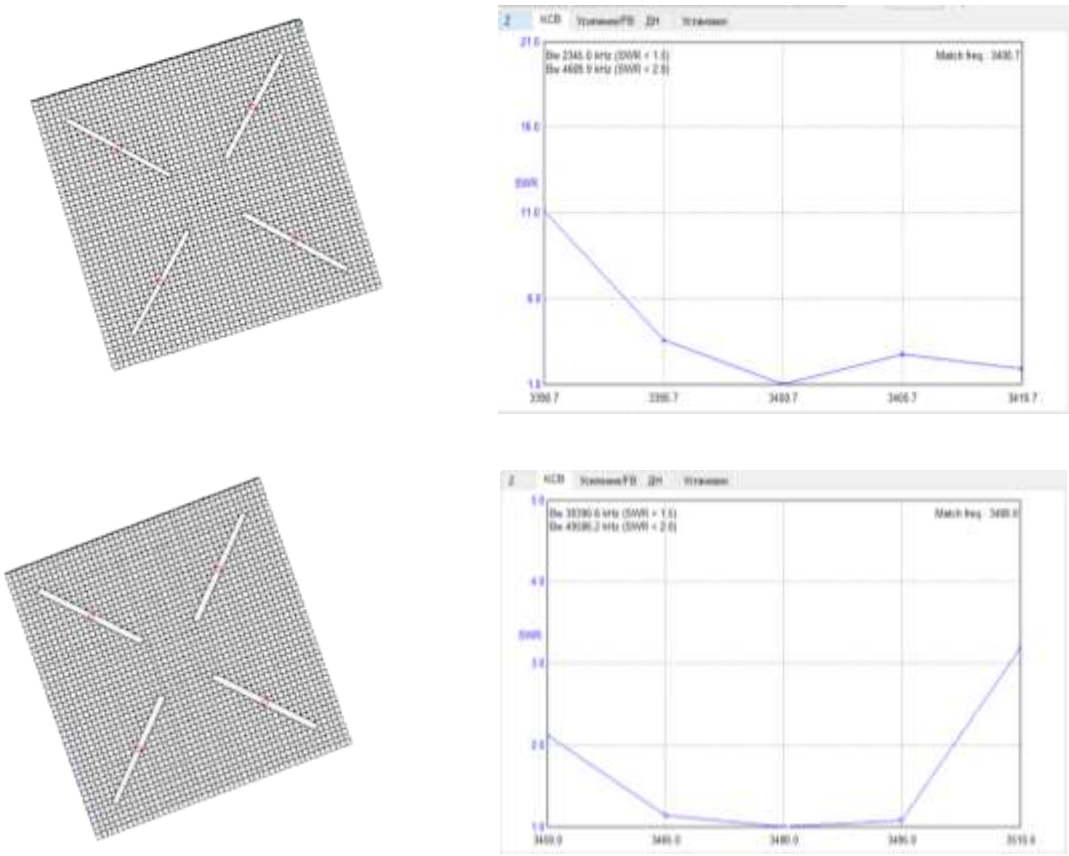


Рис. 5. Зависимость КСВн антенной системы от ширины щели

Еще одним ключевым параметром, влияющим на КСВн антенной системы в целом, является способ питания излучателей [4]. Изменение угла поворота фазы источника питания позволяет значительно улучшить характеристики структуры в одной точке, достигая наименьшего КСВн, однако, согласовать систему в полосе частот, даже узкой, и получить удовлетворительный КСВн очень сложно (рис. 6).

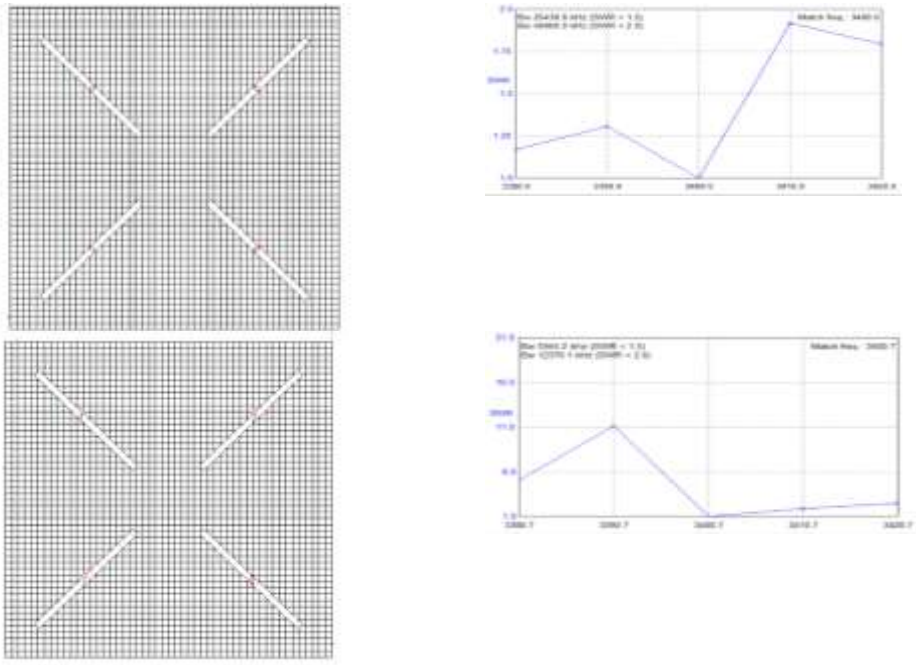


Рис. 6. Зависимость КСВн антенной системы от способа питания излучателей

В результате электродинамического моделирования была доказана работоспособность планарной системы из 4-х щелевых излучателей, а также получена модель с хорошей излучающей способностью, и КСВн, равным 1.9 (рис. 7).

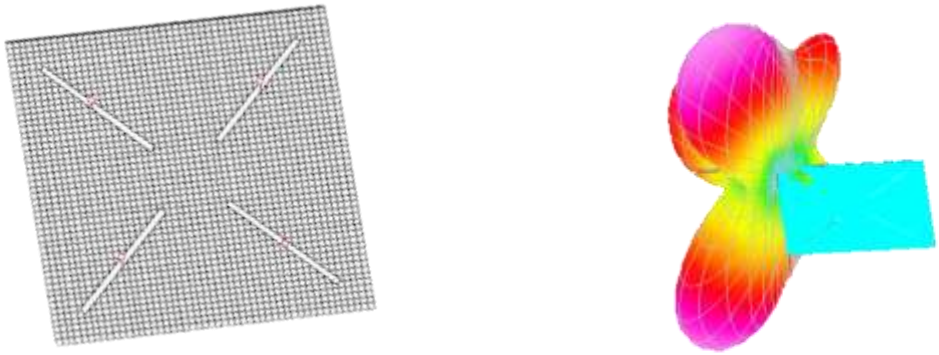


Рис. 7. Электродинамическая модель

Заключительным этапом работы стало создание масштабного макета антенной системы из 4-х щелевых излучателей с питанием на кольцевом эллиптическом резонаторе (рис. 8). Длина щелей соответствует четверти рабочей длины волны резонатора.

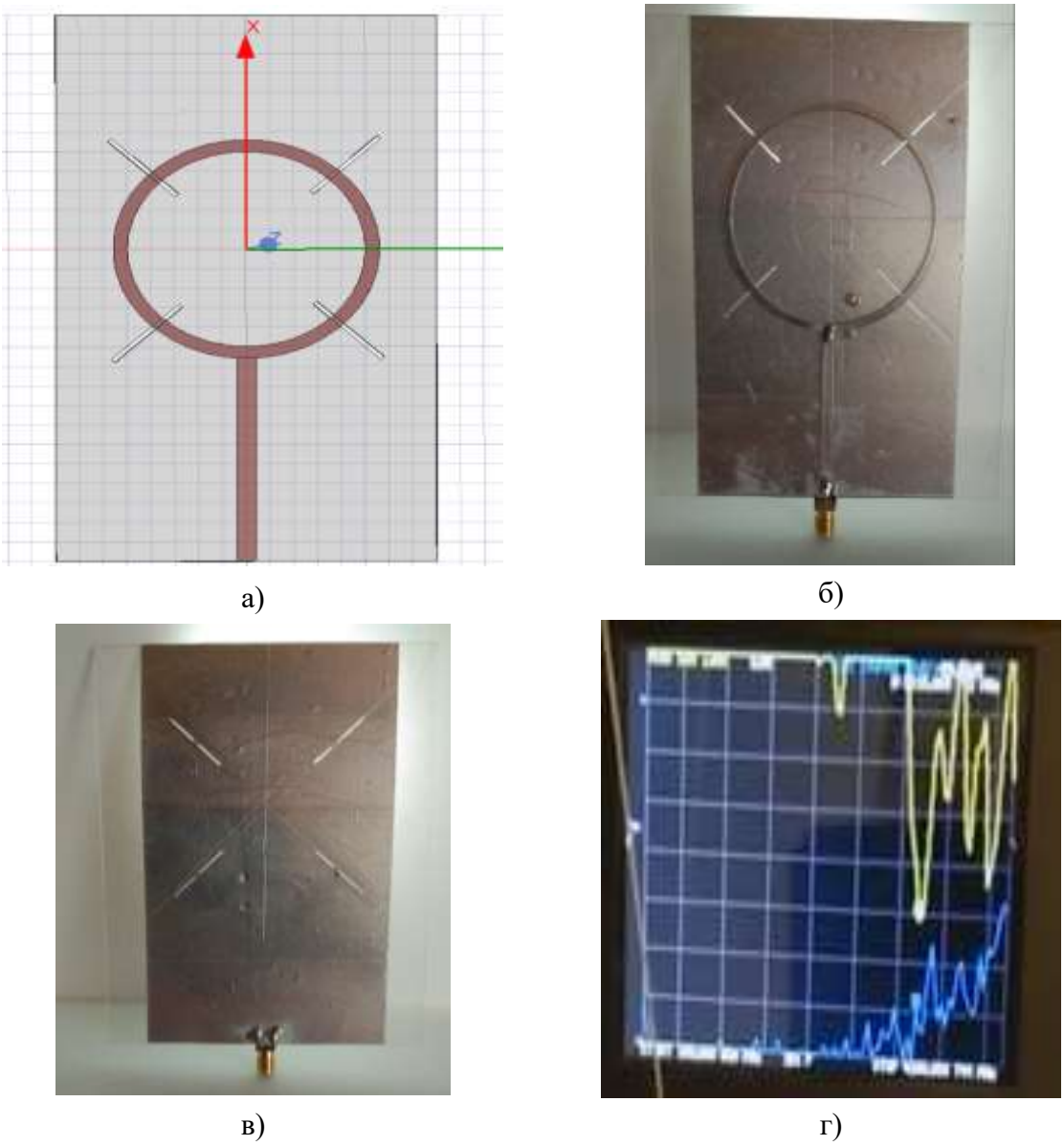


Рис. 8. Макет излучателя на кольцевом эллиптическом резонаторе:
а) 3*D* модель макета; б) макет, вид спереди; в) макет, вид сзади;
г) КСВН макета (желтая линия)

Итогом работы является электродинамическое компьютерное моделирование планарной системы из 4-х щелевых излучателей, синтезирована узкополосная работоспособная структура с хорошей излучающей способностью и КСВн, равным 1,9. Изготовленный масштабный макет планарной щелевой антенной системы с питанием кольцевым эллиптическим резонатором доказывает правильность наших предположений.

Список используемых источников

1. Воскресенский Д. И. Устройства СВЧ и антенны. М.: Радиотехника, 2006. 378 с.
2. Воскресенский Д. И. Проектирование фазированных антенных решеток. М.: Радиотехника, 2012. 744 с.

3. Седышев Э. Ю., Соковых Р. И. Антенная решётка на кольцевом эллиптическом резонаторе.// Электроника и микроэлектроника СВЧ : материалы X всерос. науч.-тех. конф., Санкт-петербург, 31 мая – 4 июня 2021 г. СПб.: СПбГЭТУ «ЛЭТИ», 2021. С. 439–444.

4. Седышев Э. Ю. Комбинированная антенная система. Патент RU78374U1 от 20.11.2008.

УДК 621.372.21
ГРНТИ 47.45.99

ИССЛЕДОВАНИЕ СВОЙСТВ РАСПРЕДЕЛЕННОЙ ЕМКОСТИ НА ПОЛОСКОВОЙ ЛИНИИ

Е. Ф. Иванищева, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматриваются основные характеристики конструктивных емкостей в виде перекрытия планарной линии и коллинеарного торцевого зазора. Произведено макетирование данных конструкций емкостей, приведены результаты математического расчета, компьютерного моделирования и эксперимента. На основании проведенного исследования делается вывод, что реальные эквиваленты предлагаемых конструкций обладают рядом особенностей, присущими связанным линиям.

СВЧ, емкость, микрополосковая линия, частотная селекция.

Сегодня в СВЧ диапазоне разработчикам интегральных схем (ИС) все чаще приходится обращаться к нестандартным формам конструктивных элементов при реализации различных устройств. Это продиктовано в первую очередь повышением степени интеграции ИС в целом. Интегральные фильтры, резонаторы, генераторы и антенны должны быть компактны и конформны. Так как эффективность устройств целиком и полностью определяется элементной базой, то ее арсенал нужно постоянно модифицировать и расширять.

Стоит обратить особое внимание на вопрос исследования свойств планарных конструктивных структур с нетипичной конфигурацией, такие структуры подчас дают довольно интересные и полезные результаты.

В предыдущих работах сотрудников профиля «Микроволновая техника. Объемные интегральные схемы» института магистратуры СПбГУТ эта тематика неоднократно рассматривалась, изучалась и приводила к интересным фактам, которые давали начало для научно-исследовательских работ

на кафедре Электроники и Схемотехники, а также аспирантов и магистрантов лаборатории Синтеза СВЧ устройств.

В статье исследуются конфигурации последовательных конструктивных емкостей в виде перекрытия планарной линии и коллинеарного зазора. Исторически такие конструктивные емкости часто используются в схемах ИС СВЧ. Номинал таких емкостей ограничен, но еще сложнее их подстройка.

Рассмотрим структуру емкости перекрытия в полосковом исполнении (рис. 1).

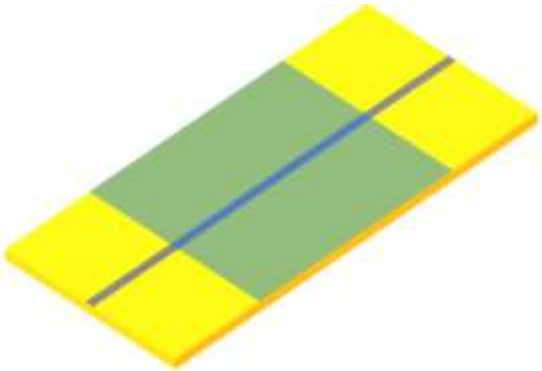


Рис. 1. 3D модель емкости перекрытия в МПЛ исполнении

Как было показано в работе [1] номинал такой емкости варьируется от минимального значения торцевой емкости линии (разрез линии) до максимального значения определяемого максимально возможным перекрытием линии.

С точки зрения топологической связности поля, последовательная ёмкость идеальна в отличии от стандартной параллельной структуры конденсатора на МПЛ [1].

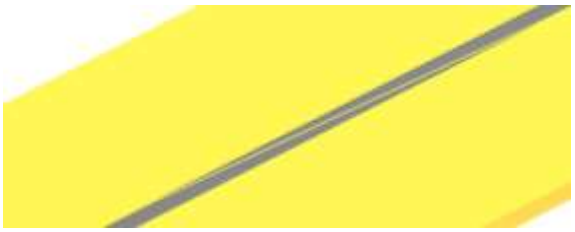


Рис. 2. 3D модель торцевой емкости в МПЛ исполнении

Структура в виде «косого разреза» линии, обеспечивающую торцевую емкость, так же имеет топологическую связность поля за счет небольшого расстояния между торцами. Номинал элемента определяется значением ширины зазора и протяженностью косой линии, разделяющую линию на две части (рис. 2).

В работе рассматриваются две структуры. Для емкости перекрытия выбраны равные отрезки линий с расположением элемента по центру схемы. Для торцевой емкости, образованной косым срезом, выбрано две конфигурации среза, протяженностью в 5 и в 7 см соответственно.

Первым этапом был проведен компьютерный анализ с помощью программы моделирования радиотехнических цепей – **RFSim99**.

Принципиальные схемы устройств были рассчитаны с учетом параметров отрезков линий (рис. 3 а, б, в).

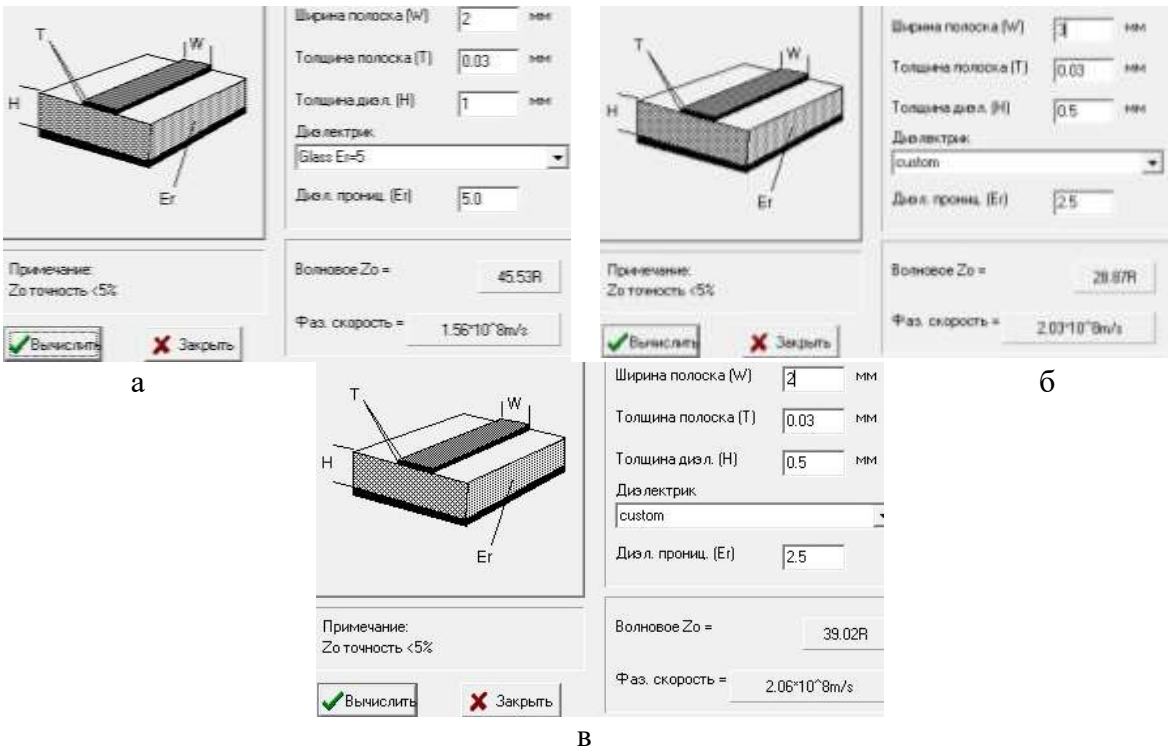


Рис. 3. Расчет параметров отрезков линий: а – схема с емкостью перекрытия, б – макет № 1 с торцевой емкостью, в – макет № 2

Емкость первой схемы легко рассчитывается с помощью формулы для плоского конденсатора:

$$C = \frac{\varepsilon_0 \varepsilon S}{d} = \frac{8{,}85 \cdot 10^{-12} \cdot 2{,}5 \cdot 116 \cdot 10^{-6}}{40 \cdot 10^{-6}} = 128 \text{ пФ}.$$

Схема устройства с емкостью перекрытия (рис. 4) и результат моделирования в диапазоне частот 100 …4 400 МГц (рис. 5).

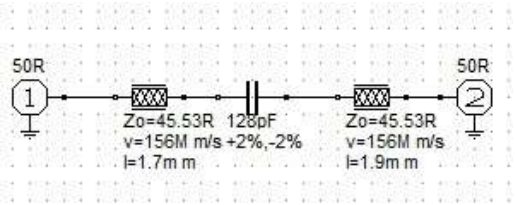


Рис. 4. Макет емкости перекрытия

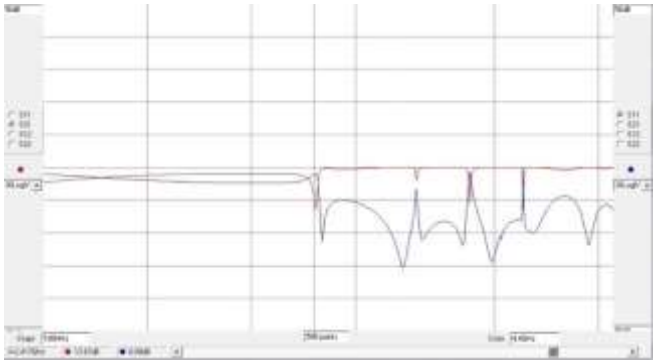


Рис. 5. Результат моделирования емкости перекрытия

Для торцевой емкости воспользуемся формулой планарного конденсатора, состоящего из диэлектрической подложки, и проводящих электродов, разделенных зазором шириной s. [3]

Для удобства расчета произведем преобразование структуры, разделив каждый отрезок линии на блоки и взяв среднее значение для соответствующих взаимодействующих «обкладок» (рис. 6).

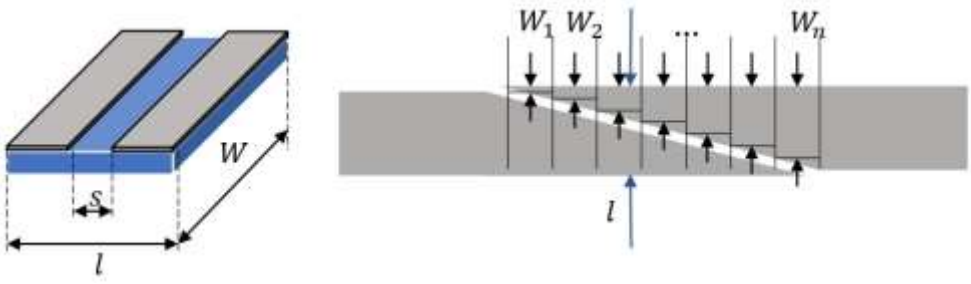


Рис. 6. Результат преобразования структуры торцевой емкости

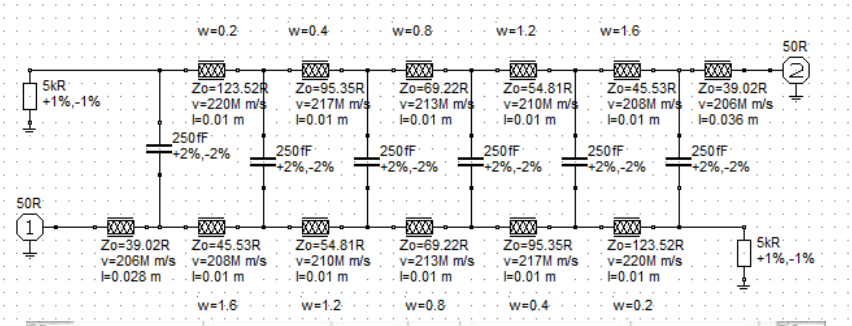
Также необходимо учитывать, что полученные значения имеют приближенный характер и уточнялись при доказательстве работоспособности модели.

Для макета с протяженностью среза 5 см

При ширине полоска = 10 мм, толщиной зазора и шириной полосковой линии имеем торцевую емкость в 250 фФ.

Схемы устройств с торцевой емкостью (рис. 7 а, рис. 8 а) и результат моделирования в диапазоне частот 100 МГц …4 400 МГц (рис. 7 б, рис. 8 б).

а



б

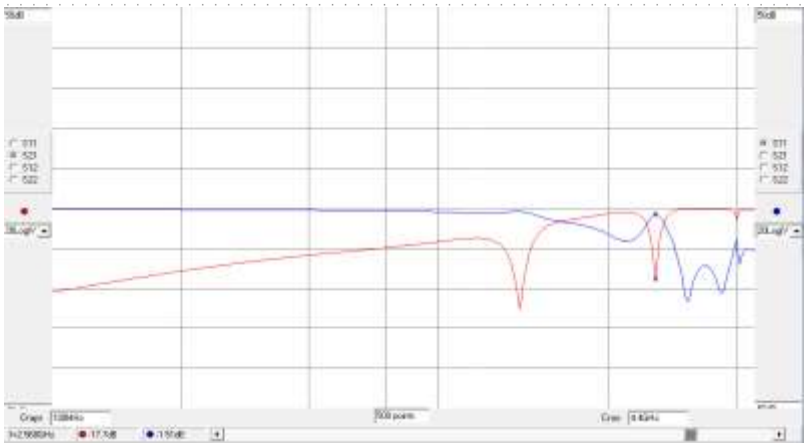


Рис. 7. а – принципиальная схема устройства с торцевой емкостью на 5 см,
б – результат моделирования

Для макета с протяженностью среза 7 см

При ширине полоска = 10 мм, толщиной зазора и шириной полосковой линии имеем торцевую емкость в 269 фФ.

а

б

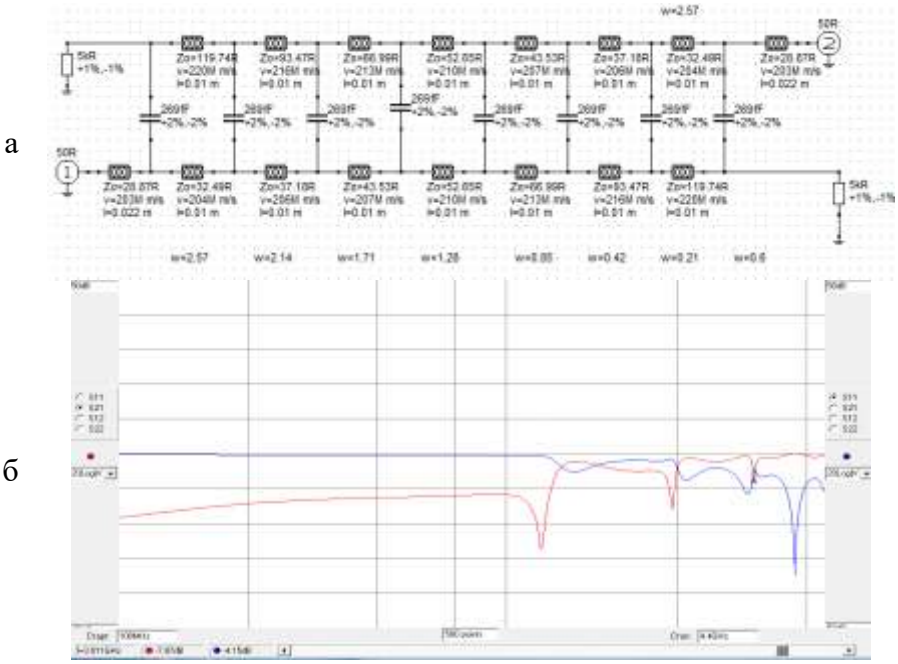


Рис. 8. а – принципиальная схема устройства с торцевой емкостью на 7 см, б – результат моделирования

По полученным результатам моделирования с уверенностью можно говорить о том, что распределенная емкость в линии передачи имеет ярко выраженную резонансную характеристику. Режекция распределенной емкости имеет порядок 20…30 дБ – небольшое ослабление, эквивалент фильтра Баттерворта 3–4 порядка, но простота реализации – не имеет равных.

Далее для сравнения результата моделирования с реальным показателями были разработаны макеты в лаборатории синтеза СВЧ СПбГУТ и проведены измерения КСВН и ослабления на индикаторе (название).

Рис. 9. Макет емкости перекрытия

Макет для схемы с емкостью перекрытия изготовлен на подложке из стекла, металлизация выполнена алюминием, диэлектрическое заполнение конденсатора из полиэтилена (ε = 2,4) (рис. 9). Макет для торцевой емкости изготовлен на подложке из полистирола (ε = 2,5), металлизация выполнена из алюминия (рис. 11 а, б).

Первым измеряем макет с емкостью перекрытия в диапазоне частот от 100 до 4 400 МГц.

На ЧХ наблюдаем пик КСВН на 2 164 МГЦ и ослабление на этой же частоте 11,55 дБ.

Важно отметить, что в правой части частотного диапазона картина ослабления
и увеличения КСВН имеет тенденцию к повторению.

Далее переходим к исследованию макетов с торцевой емкостью.

Первично измерим макеты без разреза, чтобы убедиться в их работоспособности. КСВН первого 1,1, потери на передачу в районе 0,5 дБ. Для второго: КСВН 1,2, потери на передачу 0,5 дБ.

Устройства выполнены на идентичных материалах, ширина полоска первого макета (рис. 11 а) 2мм, протяженность разреза 5 см; ширина второго (рис. 11 б) 3 мм, протяженность разреза 7 см.

Для первого макета рабочий диапазон частот от 100 до 4 400 МГц (рис. 12).

На частоте в районе 2 500 МГц наблюдаем пик КСВН, на этой же частоте ослабление режекции 11 дБ (рис. 12).

Для второго макета рабочий диапазон частот от 100 до 4 400 МГц (рис. 13).

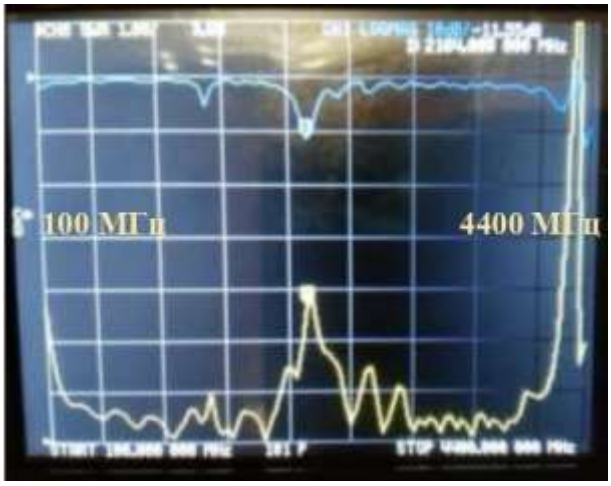


Рис. 10. ЧХ макета емкости перекрытия

а

б

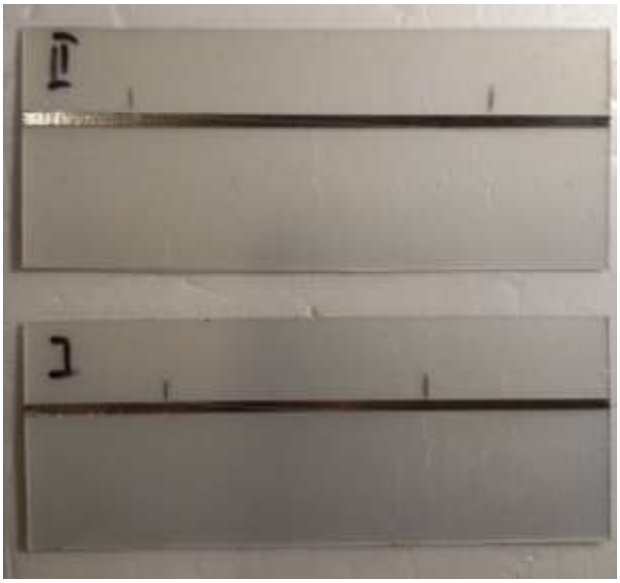


Рис. 11. Макеты торцевой емкости

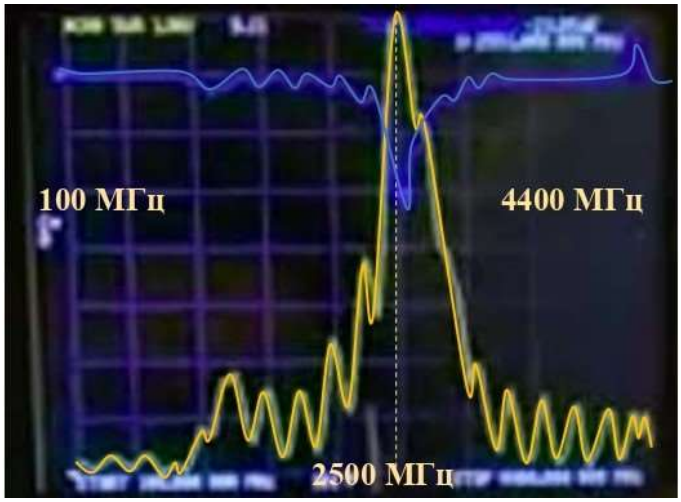


Рис. 12. ЧХ макета № 1 торцевой емкости

В диапазоне 1 300–3 400 МГц видим очевидные фильтровые характеристики, в точке примерно на 2 400 МГц ослабление режекции 35дБ и очень большой КСВН (рис. 13).

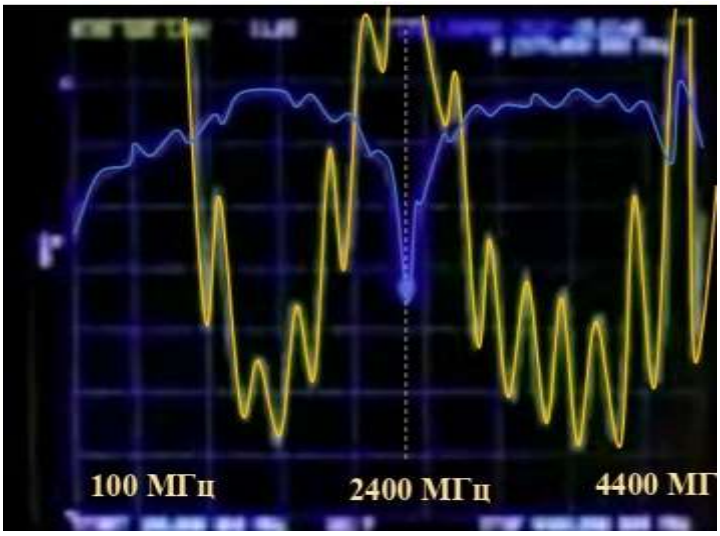


Рис. 13. ЧХ макета № 2 торцевой емкости

Вывод

Полученные в ходе исследования результаты дают нам понять, что изменение конфигурации емкости, в полосковом исполнении, приводит к получению уже не только конструктивного элемента, но к новому устройству с частотно-селективными свойствами.

Такие структуры перспективны в изучении, так как по сути представляют собой нерегулярные связанные линии. Определение геометрических границ возникновения связи по частоте представляет особый интерес.

Список используемых источников

1. Иванищева Е. Ф., Седышев Э. Ю. Моделирование планарной емкости перекрытия в полосковом исполнении // Материалы всерос. научно-метод. конф. ПКМ 2021, СПб, 30 нояб. – 2 дек. 2021 г. . СПб.: СПбГУТ, 2021. С. 77–83.

2. Покровский Н. А., Седышев Э. Ю. Исследование планарной спирали в ОИС СВЧ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 472–476.

3. Вендик О. Г., Зубко С. П., Никольский М. А. Моделирование и расчет емкости планарного конденсатора, содержащего тонкий слой сегнетоэлектрика // Журнал технической физики. 1999. Т. 69, N 4. С. 1–7.

УДК 535.3, 535.317.24, 621.3, 621.316.728
ГРНТИ 29.31.15, 29.31.26, 47.14.07, 47.14.17, 47.14.23

ОСНОВНЫЕ СТРУКТУРЫ ДИОДНЫХ ДРАЙВЕРОВ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ

А. М. Илларионов, В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оптоэлектронные приборы различного назначения представляют особый интерес и открывают всё новые перспективы развития электроники, оптики и схемотехники. Оптические системы передачи информации имеют принципиальные, конкурентоспособные преимущества, такие как высокая информационная емкость оптических каналов связи, малые массогабаритные размеры в сравнении с СВЧ-волноводами, отсутствие взаимных наводок и паразитных связей между функциональными узлами электрической схемы, высокий уровень помехозащищенности и прочее. Обеспечение защиты со стороны электропитания является одним из основных требований для исправной и стабильной работы приборов оптоэлектроники. В работе рассмотрены базовые структуры диодных драйверов. Произведено их моделирование, анализ структурного построения электрических схем, влияния их характеристик на выходной сигнал.

оптоэлектроника, полупроводниковые светодиоды, источник питания, стабилизация, полупроводниковая электроника.

Одной из важных частей оптического оборудования в сфере построения телекоммуникационных систем является лазерный диод, в котором процесс излучения вынужденных световых квантов отличается высокой направленностью и монохроматичностью излучения. Лазерный диод, как правило, используется вместе с драйвером.

Диодным драйвером или источником питания светодиода называется устройство, рассчитанное на потребление постоянного тока, при помощи которого можно подсоединять светодиод или систему из светодиодов к сети переменного тока [1]. При его включении к сети переменного напряжения происходит преобразование переменного напряжение в постоянное, при этом ток уменьшается до рабочего уровня светодиода. В зависимости от свойств и области применения светодиодной схемы драйвер может совершать и другие преобразования сигнала.

Во многих случаях драйверу диода просто необходимо подавать постоянный рабочий ток, что приводит к непрерывной работе лазерного диода с приблизительно постоянной оптической выходной мощностью. Свойства лазерных диодов определяются во многом вольтамперными характеристиками, которые из-за сильной нелинейности описываются низким дифферен-

циальным сопротивлением (высоким значением $\Delta I/\Delta U$). С учетом их сильной зависимости от рабочей температуры электронно-дырочного перехода, необходимо стабилизировать электрический ток в схеме драйвера путем автоматической регулировки приложенного напряжения. Этот режим постоянного тока является функцией так называемого источника тока.

В работе светодиодных систем важным является поддержание заданной величины выходной оптической мощности от тока, протекающего через электронно-дырочный переход, которая является главной оптической характеристикой. Поэтому необходимой составляющей электрической схемы драйвера светодиода является источник тока, с помощью которого возможно практически линейно управлять оптической мощностью излучения светодиодов после выхода на режим генерации [4].

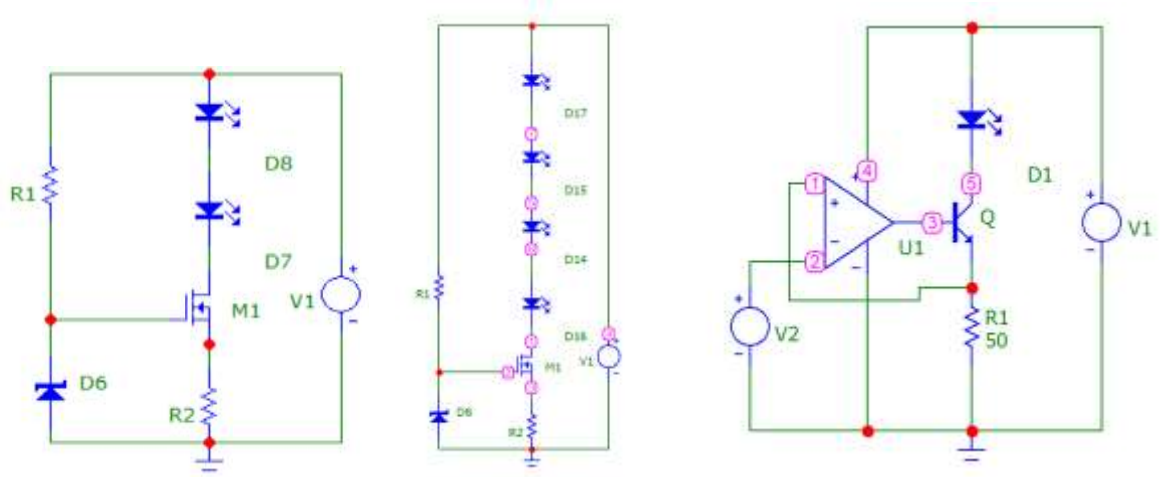
Самая простейшая структурная схема драйвера включает в себя токоограничивающий резистор и защитный диод. Токоограничивающий резистор также иногда называют балластным или подтягивающим резистором. Резистор и регулятор ограничивают прямой ток в цепи до безопасного предела. Такая схема находит применение в схемах, не требующих высокой стабильности мощности светового потока, но она малоэффективна и не может задавать величину силы тока с той же точностью, как линейный регулятор или более сложный драйвер [1].

Существуют конструкции диодных драйверов, которые могут стабилизировать выходную оптическую мощность (режим постоянной мощности) на основе сигнала от фотоприемника, который может быть встроен в корпус лазерного диода. Это особенно актуально для лазерных диодов для передающих систем в оптоволоконных линиях связи.

Во всех конструктивных решениях диодных драйверов следует контролировать приложенное напряжение, поскольку при обнаружении отличного от рабочих значений напряжения устройство может отключить диод, чтобы предотвратить его выход из строя. Схемы стабилизации тока должны обладать большим выходным сопротивлением, чтобы поддерживать постоянное значение тока при подключении нагрузки. Такие электрические схемы обеспечивают поддержание исправной работы светодиодов и обеспечение постоянства значения мощности светового потока. Наиболее распространенным вариантом является использование стабилизаторов тока на основе биполярных (БТ) и полевых транзисторов (ПТ) [2, 3]. Также за счет простоты сбора схемы и её настройки всё чаще применяют схемы на операционных усилителях (ОУ). В работе были проанализированы, выбраны, смоделированы основные схемные решения в проектировании схем стабилизации токовой накачки светодиодов в непрерывном режиме (рис. 1).

Сопротивление *R1* необходимо подбирать с учетом тока стабилитрона (I_{D6}) в соответствие с правилом делителя напряжения для входного контура:

$$R1 = \frac{U_{\text{ип}} - U_{\text{проб}}}{I}.$$



а) б) в)

Рис. 1. Схема компьютерного моделирования:
а) стабилизатора тока на основе полевого транзистора с использованием стабилитрона;
б) передающей части с использованием четырех диодов в качестве нагрузки;
в) стабилизатора тока на ОУ и БТ

Ток, протекающий через лазерные диоды, можно регулировать сопротивлениями *R*1 и *R*2, и изменением порогового напряжения МОП-транзистора. Роль опорного источника напряжения в этой схеме выполняет стабилитрон *D*6, который в пределах рабочего напряжения обеспечивает поддержания заданного уровня тока накачки диодов. Зависимость тока от сопротивления изображена на рис. 2.

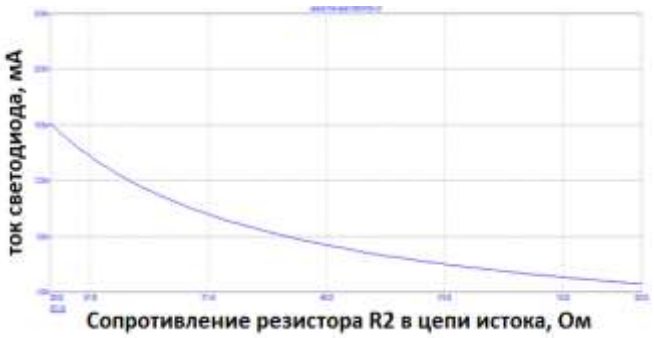


Рис. 2. Зависимость светодиода *I* от сопротивления *R*2

В оптических системах для уменьшения массогабаритных размеров, оптимизации расходов на элементную базу, например, в светодиодной ленте, используется включение нескольких светодиодов. Особенностью практического использования таких схем является подбор оптимального количества светодиодов в последовательном включении, при котором будет поддерживаться постоянная величина тока, мощности светового потока.

В работе был производен расчет схемы с подключением дополнительных светодиодов, как показано на рис. 1, а. Были рассчитаны и подобраны номинальные значения резисторов и минимальное напряжение источника питания для такой схемы стабилизации тока накачки. Произведен экспериментальный подбор оптимального количества светодиодов в линейке. Управляя сопротивлением на резисторах R1 и R2, нужно обеспечить максимально эффективное значение тока на светодиодах. В результате компьютерного моделирования при исходных параметрах элементной базы было получено значение тока $I \approx 30$ мА, наибольшее количество светодиодов, которых можно подключить в линейке при заданном режиме работы – четыре.

При сопоставлении величины токов (рис. 3), протекающих через светодиоды, в схеме было получено, что транзистор перестаёт выполнять функцию источника стабильного тока при наличии в цепи пяти последовательно соединённых светодиодов.

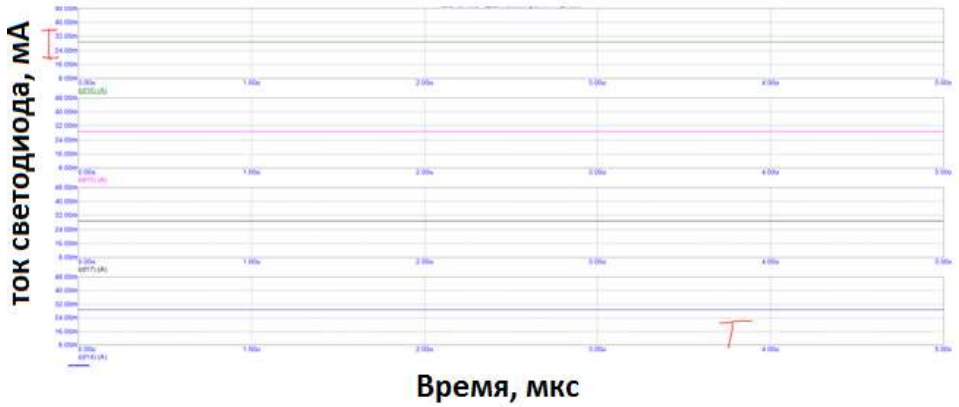


Рис. 3. Значения тока на четырех подключенных светодиодах

Была также рассмотрена работа таких схем на основе биполярного транзистора. При использовании схемы токовой накачки на основе биполярного транзистора источник переменного сигнала должен обладать смещением по постоянному напряжению, так как при напряжении источника переменных сигналов менее напряжения открывания перехода база-эмиттер ($U_{бэ}$) транзистор работает в режиме отсечки, то есть находится в закрытом состоянии. При использовании источника переменных сигналов без наличия постоянной составляющей ток будет протекать через светодиод только при положительных полупериодах входного сигнала. Также при положительных полупериодах часть напряжения падает на переходе база-эмиттер, что является недопустимым при малых входных сигналах. Зависимость тока светодиода от времени при синусоидальном сигнале источника V1 с частотой 1 кГц и амплитудой $U_{max} = 1$ В источника опорного сигнала представлена на рис. 4 а, значение сопротивления резистора $R1 = 100$ Ом. Такие значения параметров элементной базы обеспечивают типовые режимы работы схемы без необходимости сложной настройки оборудования.

Из полученной зависимости видно, чтобы сохранялся стабильным без искажений сигнал в выходной цепи схемы накачки, необходимо обеспечить такое напряжение смещения в схеме, чтобы оно несколько превышало суммарное значение амплитуды входного сигнала и падения напряжения на переходе база-эмиттер (рис. 4, б-в).

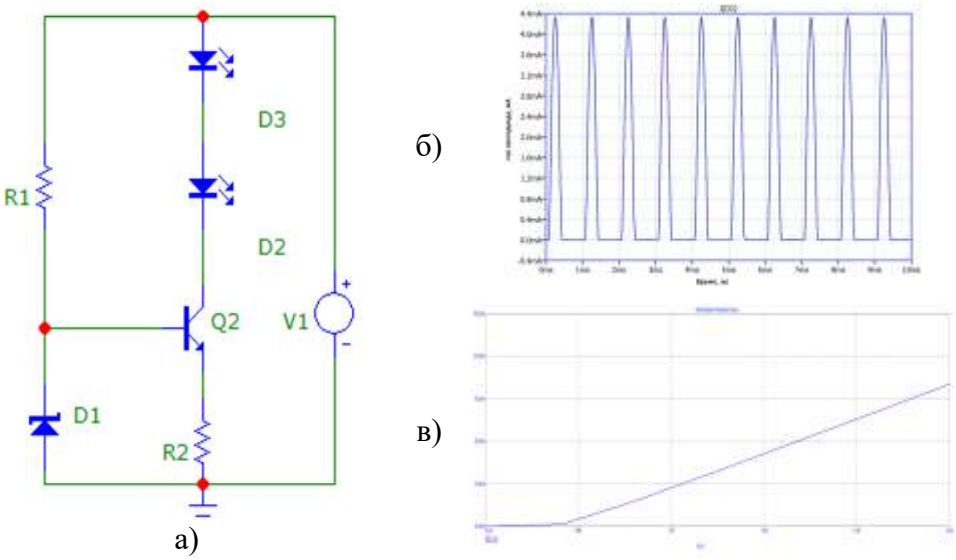


Рис. 4. Схема токовой накачки с помощью биполярного транзистора:
а) принципиальная схема; зависимости тока светодиода:
б) от времени при использовании источника переменных сигналов без напряжения смещения;
в) от опорного источника напряжения

Такое смещение задается с помощью пассивных элементов, устанавливаемых в цепи эмиттера и создающих отрицательную обратную связь по току. Расчет параметров этих элементов производится, исходя из значений постоянной и переменной составляющих, с которыми будет работать проектируемая схема.

Сопоставляя полученные зависимости схем стабилизации накачки на биполярном транзисторе и стабилитроне и на операционном усилителе, можно сделать вывод о том, что при работе даже с переменным сигналом в выходной цепи транзистора в схеме на рис. 1 в величина силы тока поддерживается более постоянной, чем в схемах на рис. 1 а и рис. 4 а. В стабилизаторах на основе ОУ напряжение источника опорного напряжения может быть как меньше порогового напряжения полевого транзистора с изолированным затвором, так и напряжения база-эмиттер, что является одним из преимуществ использования операционных усилителей, также на основе проведенных исследований.

Список используемых источников

1. Гречишников В. М. Схемотехника волоконно-оптических устройств: учеб. пособие. Самара: Изд-во Самарского университета, 2018. 172 с.

2. Алейник А. С., Востриков Е. В., Волковский С. А., Дейнека И. Г., Стригалев В. Е., Мешковский И. К., Основы схемотехники электронных устройств. СПб.: Университет ИТМО, 2021. 149 с.

3. Джонс М. Х. Электроника - практический курс. М.: Техносфера, 2013. 510 с.

4. Chi M., Jensen O. B., Erbert G., Sumpf B., Petersen P. M. Tunable high-power narrowspectrum external-cavity diode laser at 675 nm as a pump source for UV generation // Applied Optics. 2011. V. 50 (1). pp. 90–94.

УДК 621.372.414
ГРНТИ 47.45.99

СИНТЕЗ МИКРОВОЛНОВОГО ГЕНЕРАТОРА НА КОЛЬЦЕВОМ ЭЛЛИПТИЧЕСКОМ РЕЗОНАТОРЕ ПО РАБОЧИМ ПАРАМЕТРАМ

Т. О. Каткова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена изучению конструктива кольцевых резонаторов СВЧ на планарных линиях передачи. В работе сравниваются кольцевые резонаторы на симметричной и несимметричной линиях передач, оценивается добротность двух типов резонаторов, анализируется влияние ширины кольца на основные характеристики. Проведено математическое моделирование, математический расчёт, компьютерное моделирование, масштабное макетирование и эксперимент.

микро-полосковая линия, симметричная линия, кольцевой резонатор, частота резонанса, тангенс угла потерь, добротность, диэлектрические потери.

В работе рассматриваются конструкции кольцевых резонаторов (рис. 1, 2), которые подробно описаны в журнале Электроника и Микроэлектроника [1]. Уже была доказана работоспособность двух макетов на разных типах линии и сняты их спектрограммы (рис. 3, 4).

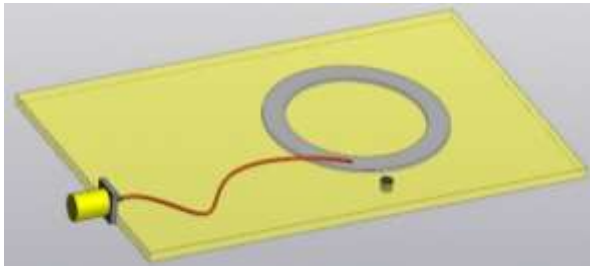


Рис. 1. 3D-Модель СВЧ генератора в микрополосковом исполнении

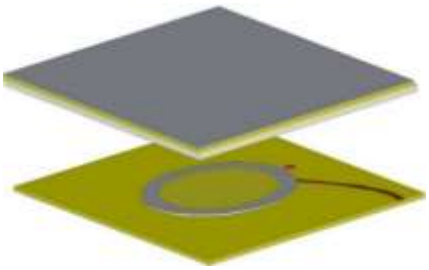


Рис. 2. 3D-Модель СВЧ генератора в объёмном интегральном исполнении

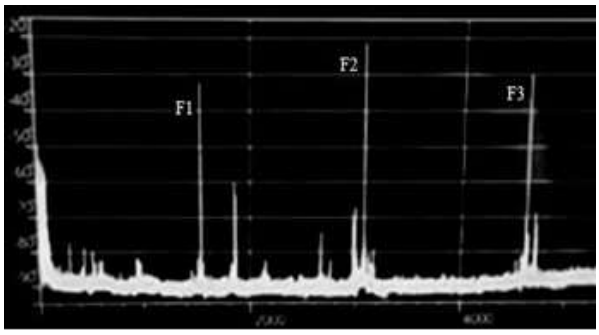


Рис. 3. Спектрограмма СВЧ генератора в микрополосковом исполнении

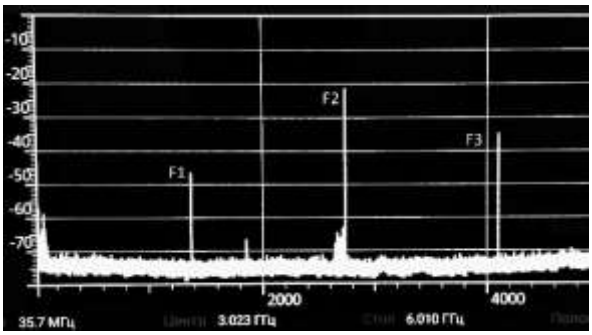


Рис. 4. Спектрограмма СВЧ генератора в объёмном интегральном исполнении

Как и любое устройство, предложенные модели генераторов имеют два основных вида диссипативных потерь: потери в скин-слое проводника и потери в толще диэлектрика. Оценка этих потерь представляет сложную инженерно-техническую задачу. Рассмотрим потери в проводнике и в диэлектрике без учета коэффициента шероховатости поверхностей. Найдя потери проводника и диэлектрика, мы сможем построить в программе RFSimm более точную схему кольцевого генератора [2]. Необходимо учесть сопротивление потерь вносимое проводником (алюминий) и диэлектриком (полипропиленом). Для того чтобы определить поверхностное сопротивление алюминия, необходимо воспользоваться формулой:

$$R = \frac{\rho \cdot l}{t \cdot w}\ , \qquad (1)$$

где ρ – удельное сопротивление алюминия при 20 ℃ [Ом*м], l – средняя длина кольца, t – толщина проводящего слоя, w – ширина полоска.

Из таблицы 1 видно, что величина потерь зависит от ширины полоска. С увеличением данного параметра, уменьшением волнового сопротивления, сопротивление потерь уменьшается.

ТАБЛИЦА 1. Значение потерь в проводнике при различной ширине

Ширина полоска, мм	1,45	2,25	3,8	4,7
Потери в проводящем слое, Ом	0,0189	0,0122	0,0072	0,0047

Чтобы определить значение удельного объёмного электрического сопротивления диэлектрика, требуется найти это значение для используемого материала и перевести в нужные единицы измерения с учётом средней длины модели кольца.

Получив необходимые данные, можно построить схему в программе RFSimm. Общий вид схемы представлен на рис. 5 [3, 4].

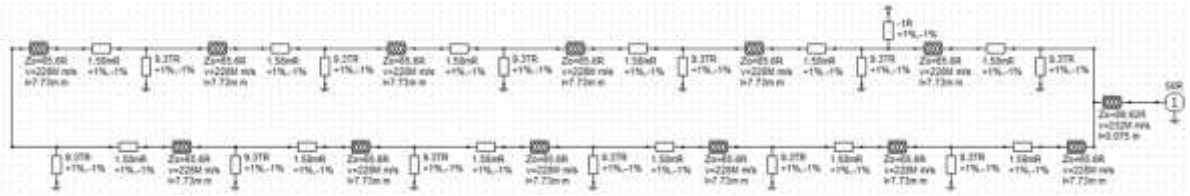


Рис. 5. Пример построения схемы генератора в программе RFSimm

Исследуя компьютерные модели с различными характеристиками, получаем расчётную характеристику S11 с учетом вариаций исполнения резонатора (рисунки 7, 9, 11, 13).

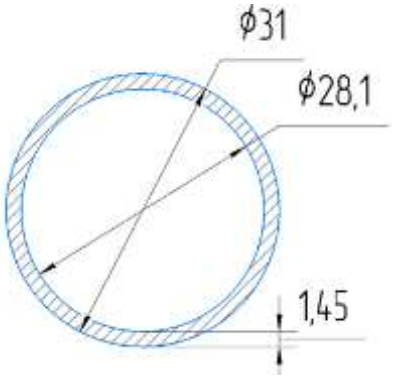


Рис. 6. Модель генератора с шириной полоска w = 1,45 мм и $Z_в$ = 65,6 Ом

Рис. 7. Эмуляция генератора с шириной полоска w = 1,45 мм и $Z_в$ = 65,6 Ом

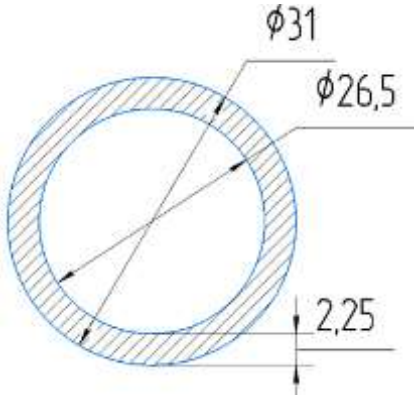


Рис. 8. Модель генератора с шириной полоска w = 2,25 мм и $Z_в$ = 50,4 Ом

Рис. 9. Эмуляция генератора с шириной полоска w = 2,25 мм и $Z_в$ = 50,4 Ом

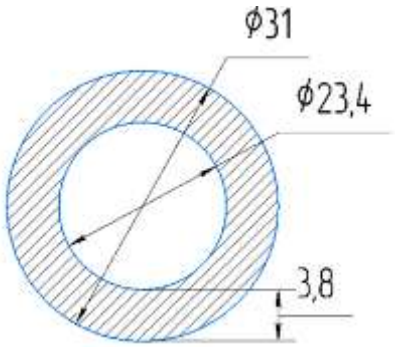


Рис. 10. Модель генератора с шириной полоска w = 3,8 мм и $Z_в$ = 35,1 Ом

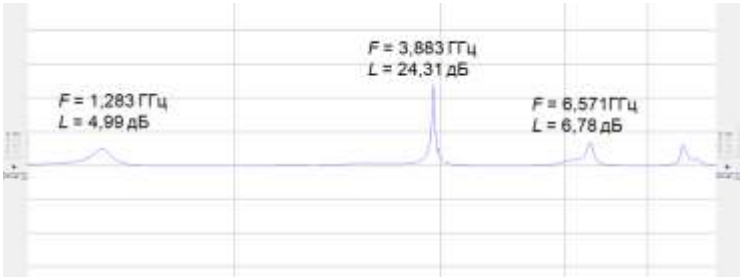


Рис. 11. Эмуляция генератора с шириной полоска w = 3,8 мм и $Z_в$ = 35,1 Ом

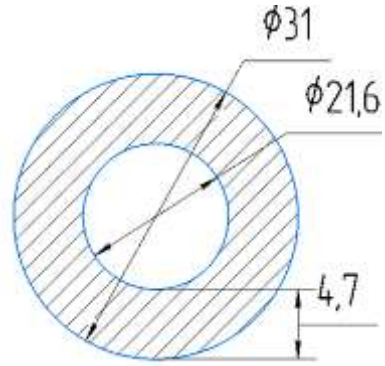


Рис. 12. Модель генератора с шириной полоска w = 4,7 мм и $Z_в$ = 29,92 Ом

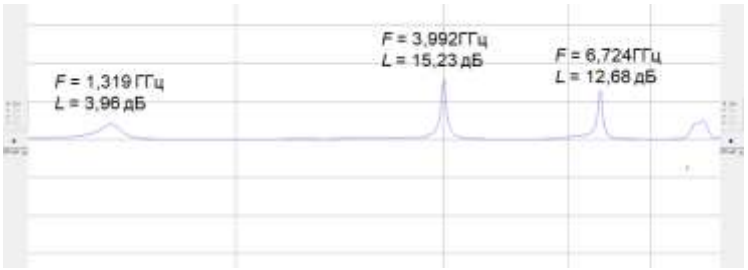


Рис. 13. Эмуляция генератора с шириной полоска w = 4,7 мм и $Z_в$ = 29,92 Ом

Отметим, что у генератора с шириной полоска равной 1,45 мм самая «чёткая» линия генерации – первая. У модели с шириной полоска 2,25 мм линии генерации стали заметно лучше, тут более выраженные 1 и 2 пик. Однако генерация на третей частоте пока остаётся «размазанной» и не чёткой. На рис. 10 модель, которая ближе всего по характеристикам к изготовленному макету (рис. 1). Здесь уже более чистые линии генерации, большие показатели уровня колебаний. Предполагалось, что с уменьшением сопротивления, генерация будет становиться более выраженной и чёткой, но на рисунке 13 видно, что первая и вторая генерации «просели» и только третья увеличилась в 2 раза.

Проведенный анализ предложенных моделей генератора (табл. 2) позволяет заключить, что увеличение выходного сопротивления ослабляет усиление первой гармоники, практически во всех случаях, но улучшает вторую и третью гармоники. Волновое сопротивление больше влияет на форму генерации. С уменьшением волнового сопротивления до 35 Ом улучшается рисунок спектральной линии генерации, пики становятся более «чистыми» и тонкими, дальнейшее уменьшение волнового сопротивления явного улучшения характеристик не показало.

ТАБЛИЦА 2. Выводы

Модель	$R_{вых}$, Ом	I генерация	II генерация	III генерация
$Z_в$ = 65,5 Ом w = 1,45 мм	80,21	1,186 ГГц; 12,88 дБ	3,541 ГГц; 2,1 дБ	6,632 ГГц; 1,69 дБ
	89,92	1,186 ГГц; 10,33 дБ	3,541 ГГц; 2,5 дБ	6,632 ГГц; 1,98 дБ
	109,13	1,186 ГГц; 6,97 дБ	3,541 ГГц; 3,18 дБ	6,663 ГГц; 2,43 дБ
$Z_в$ = 50,4 Ом w = 2,25 мм	80,21	1,236 ГГц; 11,99 дБ	3,76 ГГц; 7,59 дБ	6,421 ГГц; 2,22 дБ
	89,92	1,236 ГГц; 9,93 дБ	3,76 ГГц; 9,82 дБ	6,421 ГГц; 2,38 дБ
	109,13	1,236 ГГц; 6,92 дБ	3,76 ГГц; 15,71 дБ	6,451 ГГц; 2,35 дБ
$Z_в$ = 35,1 Ом w = 3,8 мм	80,21	1,283 ГГц; 5,69 дБ	3,883 ГГц; 19,15 дБ	6,541 ГГц; 5,88 дБ
	89,92	1,283 ГГц; 4,99 дБ	3,883 ГГц; 24,31 дБ	6,571 ГГц; 6,78 дБ
	109,13	1,283 ГГц; 3,76 дБ	3,883 ГГц; 13,32 дБ	6,571 ГГц; 7,73 дБ
$Z_в$ = 29,92 Ом w = 4,7 мм	80,21	1,319 ГГц; 4,36 дБ	3,992 ГГц; 21,73 дБ	6,724 ГГц; 10,16 дБ
	89,92	1,319 ГГц; 3,96 дБ	3,992 ГГц; 15,23 дБ	6,724 ГГц; 12,68 дБ
	109,13	1,319 ГГц; 3,27 дБ	3,992 ГГц; 9,31 дБ	6,693 ГГц; 17,28 дБ
Макет $Z_в$ = 35,95 Ом w = 3,75 мм	90	1,5 ГГц; -33 дБ	3,1 ГГц; -21 дБ	4,62 ГГц; -30 дБ

Чтобы проследить зависимость добротности от варианта исполнения резонатора и, в дальнейшем, управлять ей для получения нужных резонансных частот, с помощью программы SMath Studio были рассчитаны общие погонные потери по формуле (2) [5, 6].

$$\alpha = \alpha_d + \alpha_c\,, \tag{2}$$

где α_d – потери в диэлектрике, α_c – потери в металле.

$$\alpha_d = 0{,}91 \cdot tg\delta \cdot f \cdot \sqrt{\varepsilon}, \tag{3}$$

где $tg\delta$ – тангенс угла диэлектрических потерь, f – частота, ε – диэлектрическая проницаемость подложки.

$$\alpha_c = 545 \cdot \frac{\sqrt{f \cdot \rho}}{w \cdot Z_в}, \quad (4)$$

где w – ширина МПЛ или СПЛ, $Z_в$ – волновое сопротивление, ρ – удельное сопротивление алюминия.

Разница выходит не очень существенная, у МПЛ $\alpha = 2{,}6376 \cdot 10^8$, а у СПЛ $\alpha = 2{,}6375 \cdot 10^8$. Погонные потери помогают выйти на сравнение добротностей двух генераторов.

Научной новизной представленной работы является способ повышения уровня и стабильности генерации за счет изменения добротности структуры, добротность структуры повышается за счет выбора типа линии, ее геометрии и используемых материалов. Итогом работы является более точная эквивалентная схема генератора на кольцевом эллиптическим резонаторе с учётом добротности устройства. Это позволяет в дальнейшем учитывать все характеристики конструкции и материалов, а также точность технологического процесса при серийном изготовлении данных устройств.

Список используемых источников

1. Каткова Т. О., Седышев Э. Ю. Генератор СВЧ на кольцевом эллиптическом резонаторе в объёмном интегральном исполнении // Электроника и Микроэлектроника СВЧ. 2021. Т. 1. С. 430–433.

2. Сазоненко Н.Ю., Седышев Э.Ю. Генератор на кольцевом резонаторе в микрополосковом исполнении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 509–513.

3. Янчук Е. В. Туннельные диоды в приемно-усилительных устройствах. М: Энергия, 1967. 56 с.

4. Седышев Э. Ю., Шомин А. Ю. Исследование возможности одновременного использования нескольких активных двухполюсников при создании СВЧ генераторов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 514–519.

5. Справочник по элементам полосковой техники / под редакцией А. Л. Фельдштейна. М., 1979. С. 200–202.

6. Анпилогов В. Р., Зимин И. В., Чекушкин Ю. Н. Диссипативные потери в микрополосковых линиях и микрополосковых антеннах // Ракетно-космическое приборостроение и информационные системы. 2018. Т. 5, Вып. 3. С. 60–69.

УДК 531.37
ГРНТИ 29.05.09

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ НЕИЗВЕСТНОЙ ПЛАНЕТЫ ПО ДАННЫМ КОСВЕННЫХ МЕХАНИЧЕСКИХ ИЗМЕРЕНИЙ

С. А. Князев, С. Н. Колгатин, Н. Л. Урванцева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе определяются характеристики неизвестной планеты– ускорение свободного падения, а через него – такие глобальные, и, казалось бы, трудно измеряемые параметры как масса и диаметр планеты. Ускорение свободного падения находится из результатов компьютерных экспериментов по скатыванию тела (сплошного и тонкостенного цилиндров и шара) по наклонной плоскости. Масса и диаметр планеты определяются на основании закона всемирного тяготения и дополнительных данных о плотности грунта. Параметры планеты могут варьироваться, создавая банк индивидуальных заданий для отдельных студентов.

неизвестная планета, вывод рабочих формул, ускорение свободного падения, масса и диаметр планеты.

В последнее время среди учащейся молодежи, молодых специалистов, наблюдается падение интереса к физике. Многие считают, что компьютерные науки, управление, экономическое планирование могут осуществляться в отрыве от физической реальности, на основе лишь одного понимания функционирования управляющих систем. Такое мнение представляется нам глубоко ошибочным. Физика не только снабжает обучающихся адекватным математическим аппаратом, но и прививает *мировоззрение*, т. е. систему взглядов на окружающий мир, позволяющую искать объективную причину происходящих явлений и управлять ими на основе истинных законов, воздействовать на причины, а не пытаться управлять следствиями. Законы окружающего мира, будь то устройство компьютера, или колебания курса ценных бумаг, глубоко связаны с объективными законами природы, смысл которых един почти для всех областей знания.

Первая часть работы связана с определением времени, в течение которого тело, в виде цилиндра или шара, скатывается с наклонной плоскости.

Схема виртуального эксперимента

Виртуальная экспериментальная установка состоит из клина, на вершине которого закреплен цилиндр или шар, таймера и таблицы для фиксации результатов измерений (рис.).

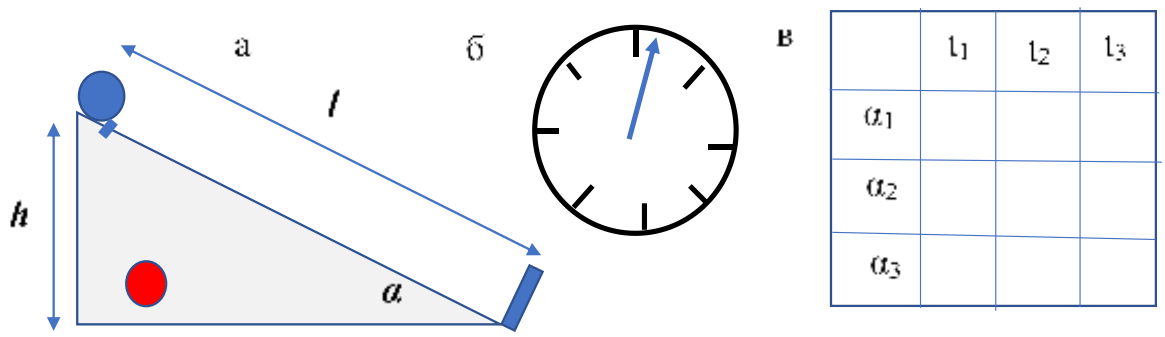


Рисунок. а) клин, б) таймер, в) таблица

Тело, имеющее форму цилиндра или шара в зависимости от номера варианта, закреплено на вершине клина, высота которого равна h, а длина образующей l.

При нажатии курсором мыши на красную кнопку убирается стопор, тело начинает скатываться с наклонной плоскости и одновременно запускается таймер. При контакте тела с нижним стопором таймер останавливается и в таблице высвечивается время движения тела при данном значении угла наклона α.

Во второй части работы студенту необходимо самостоятельно вывести рабочую формулу, связывающую время движения тела по наклонной плоскости с ускорением свободного падения. С этой целью излагается цепочка рассуждений, позволяющая определить ускорение свободного падения из зависимости времени движения бруска по наклонной плоскости в классическом «школьном» варианте.

Закон взаимопревращения механической энергии при отсутствии сил трения имеет сил трения имеет вид: $\frac{mV_1^2}{2} = mgh$, где V_1 – скорость бруска у основания наклонной плоскости, h – высота клина, g – ускорение свободного падения. Откуда следует: $V_1^2 = 2gh$.

Поскольку брусок движется равноускорено, то выполняется равенство: $l = \frac{at^2}{2}$, где a – ускорение, которое является проекцией g на направление наклонной плоскости ($g \sin \alpha$).

Выражение для ускорения свободного падения связано с временем движения бруска t соотношением:

$$g = \frac{2l}{t^2 \sin \alpha}.$$

Далее студенту предлагается вывести рабочую формулу на основании представленной выше цепочке рассуждений.

Скатывание бруска и тела округлой формы с наклонной плоскости имеет принципиальное различие: брусок участвует только в поступательном движении, а цилиндр или шар еще и во вращательном движении. Поэтому закон сохранения механической энергии приобретает вид [1]:

$$\frac{mV_1^2}{2} + \frac{I\omega_1^2}{2} = mgh,$$

где I – момент инерции тела, ω – угловая скорость

Теперь уже скорость скатывающегося тела у основания клина нельзя определить по формуле: $V_1^2 \neq 2gh$ и величина ускорения, определяемая из соотношения $l = \frac{at^2}{2}$, не равна $g \sin \alpha$: $a \neq g \sin \alpha$.

В качестве справочного материала в описании к работе приводится свод основных соотношений: момент инерции сплошного, тонкостенного цилиндров и шара, связь между линейной и угловой скоростями.

После того как будет выведена рабочая формула студентам предлагается обработать полученные результаты – определить величину ускорения свободного падения на данной планете по данным для 3-х значений угла наклона α и оценить погрешность полученного результата.

Для определения массы планеты M и ее диаметра (радиуса R) студентам также требуется самостоятельно вывести формулы для массы планеты M и ее радиуса R.

В качестве справочного материала в описании к работе приводятся необходимые соотношения – закон всемирного тяготения:

$$mg = \gamma \frac{mM}{R^2},$$

где γ – гравитационная постоянная равная 6,67 10^{-11} м^3 кг$^{-1}$ с$^{-2}$, M – масса планеты, m – масса тела, R – радиус планеты.

Связь плотности ρ с массой планеты M, имеющей шарообразную форму:

$$M = \rho \frac{4\pi R^3}{3}.$$

Величина плотности ρ грунта, из которого состоит планета, задается отдельно для каждого из вариантов.

Каждая из бригад получает свое индивидуальное задание – тип используемого тела (сплошной или тонкостенный цилиндр, шар), плотность грунта планеты.

Резюме

В отличии от «традиционных» лабораторных работ, где студентам требуется обработать полученные данные по готовым рабочим формулам, в данном случае им придется самостоятельно вывести эти формулы, что должно способствовать к мобилизации их интеллектуальных способностей, заставить понять связь простейших физических параметров.

Дополнительно, поставленная цель стимулируется и чисто педагогическими задачами – необходимостью снабдить преподавателей, работающих фактически в дистанционном режиме, адекватным инструментарием, позволяющим объективно оценить уровень освоения теоретического материала, исключить возможность «тупого» списывания, заинтересовать неравнодушных студентов.

Список используемых источников

1. Савельев И. В. Курс общей физики. Т. 1. М.: Наука, 1987. Т. 1. 433 с.

Статья представлена на X Юбилейной международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», прошедшей 24–25 февраля 2021 года.

УДК 621.3.088.2
ГРНТИ 29.03.45

ОБРАБОТКА ИЗМЕРЕНИЙ С ПОМОЩЬЮ ПРОЦЕДУРЫ ИНТЕГРИРОВАНИЯ И ДИФФЕРЕНЦИРОВАНИЯ

С. А. Князев, С. Н. Колгатин, Ю. В. Шарихина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На примерах изложения материала по теории погрешностей, лабораторной работы «Движение тел при наличии вязкого трения», метода выделения слабого сигнала на фоне больших помех и анализа энергетического распределения тока вторичных электронов, показано преимущество обработки результатов измерений с помощью процедур интегрирования и дифференцирования по сравнению с традиционными методами.
интегрирование и дифференцирование, погрешности измерений.

процедура интегрирования и дифференцирования.

На вводном занятии по теории погрешностей студенты должны определить «на глазок» размер стержня, демонстрируемого преподавателем. На рис. 1 представлен график зависимости числа поданных студентами голосов за тот или иной размер стержня. Этот график представляет собой ломанную линию и на первый взгляд трудно извлечь какую-либо информацию их этих данных.

С помощью процедуры интегрирования – строится накопительная кривая, где по оси абсцисс отложен размер стерженька, а по оси ординат суммарное число поданных голосов. Это построение превращает результат первого эксперимента в плавную кривую (рис. 2).

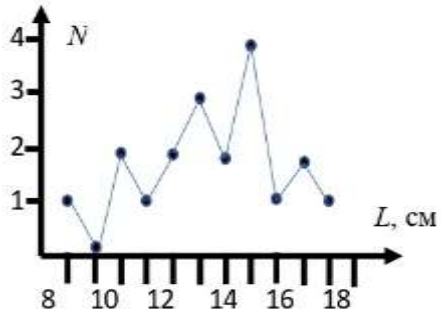


Рис. 1. N – число поданных голосов, L – размеры стержня

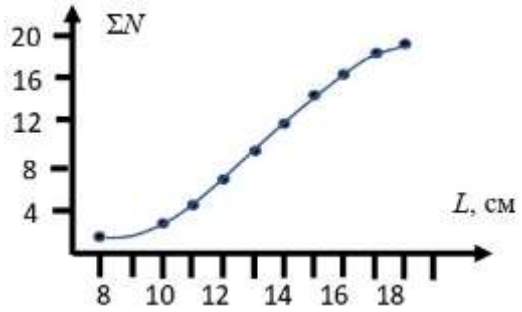


Рис. 2. Накопительная кривая

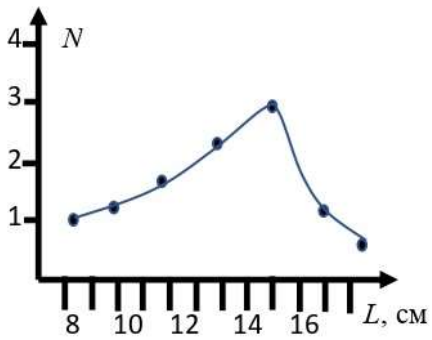


Рис. 3. Зависимость числа поданных студентами голосов от размера стержня $N(L)$

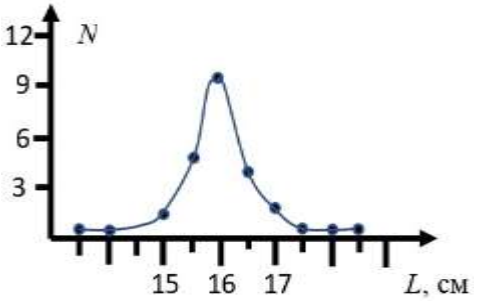


Рис. 4. N – число поданных голосов, L – размеры стержня

Возвращение к зависимости $N(L)$ осуществляется путем дифференцирования парных точек (рис. 3).

На полученной зависимости $N(L)$ четко виден максимум, а асимметрию левой и правой части кривой можно объяснить малым числом опрошенных студентов.

Во втором эксперименте необходимо определить размеры стержня с уже помощью линейки. Результаты этого опыта представлены на рис.4. Использование линейки качественно изменило результат эксперимента – существенно сузился разброс точек относительно максимума этой кривой. Математически, полученная кривая описывается с помощью функции Гаусса: $y = A \cdot \exp(-k(x - x_0)^2$, где x_0 – среднее арифметическое значе-

ние измеряемой величины x, k – коэффициент, определяющий скорость спада экспоненты относительно x_0.

Условия нормировки и доверительная вероятность

Пусть на промежутке от –∞ до +∞ измеряемая величина определена с вероятностью P = 1 или 100 %. Возьмем интеграл от функции e^{-kx^2} в указанных пределах: $\int_{-\infty}^{+\infty}\exp(-k\cdot x^2)dx=\sqrt{\frac{\pi}{k}}$. Тогда:

$$f(x)=\sqrt{\frac{k}{\pi}}\int_{-\infty}^{+\infty}\exp(-k(x-x_0)^2)dx=1.$$

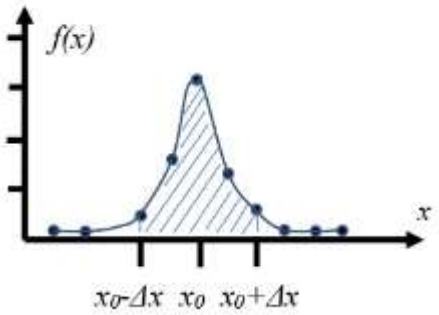


Рис. 5. Гауссово распределение. Область доверительной вероятности

Утверждение о том, что искомая величина x лежит в пределах от $x_0 - \Delta x$ до $x_0 + \Delta x$, должно сопровождаться указанием доверительной вероятности, равной площади под кривой на рис. 5:

$$P=\sqrt{\frac{k}{\pi}}\int_{x_0-\Delta x}^{x_0+\Delta x}\exp(-k\cdot(x-x_0)^2\,dx.$$

Этот факт отражается в выражении для абсолютной погрешности измерения наличием коэффициента Стьюдента $t_{\alpha,N}$, где α – доверительная вероятность $(\Delta x)^2_{общ}=(\Delta x)^2_{сист}+t^2_{\alpha,N}\frac{\sum(x_i-x_0)^2}{N(N-1)}$. Увеличение числа измерений N уменьшает случайную составляющую погрешности, при этом общая погрешность определяется ее систематической компонентой, не зависящей от числа измерений и определяемой только условиями эксперимента и погрешностью измерительных приборов [1].

Существует метод идентификации полезного сигнала на фоне шумов, даже если интенсивность этого сигнала равна или меньше интенсивности шума. Рассмотрим эту ситуацию на примере выделения слабой спектральной линии на уровне шума [2].

Повторные измерения не приводят к идентификации сигнала. При суммировании результатов измерений через некоторое время отчетливо проявляется искомый сигнал (обозначен стрелкой на рис. 6). Его положение строго фиксировано при хаотичном изменении интенсивности фона.

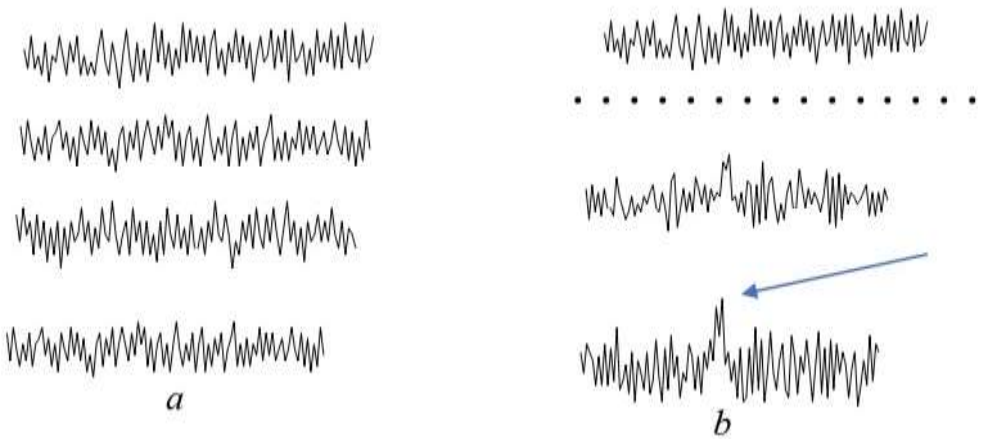


Рис. 6. Шумовая дорожка со слабым сигналом внутри:
a) повторные измерения, b) суммирование повторных измерений

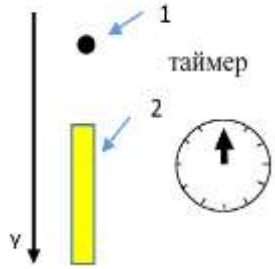
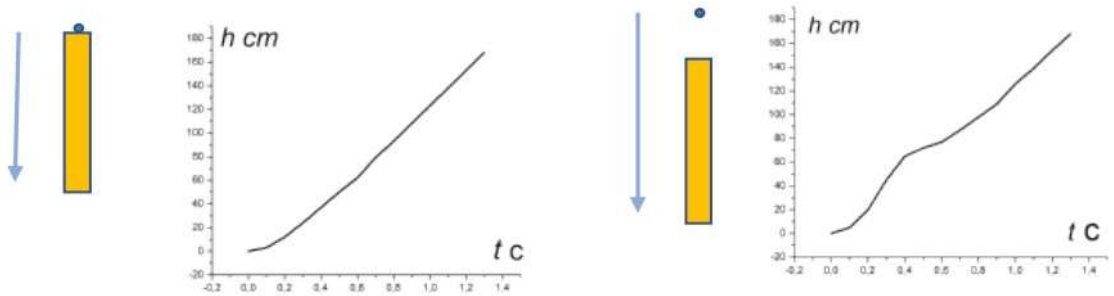


Рис. 7. Схема лабораторной установки

Ещё один пример использования метода дифференцирования – лабораторная работа «Движение тел при наличии вязкого трения» [3]. На рис. 7 приведена схема проводимого эксперимента. Шарик 1, набрав скорость при свободном падении в воздухе, попадает в цилиндрический сосуд 2 с вязкой жидкостью. Автоматическое устройство определяет положение шарика по y через одинаковые интервалы времени Δt. Эксперимент проводится для двух начальных положений шарика – когда он начинает движение непосредственно с поверхности жидкости и с некоторой высоты над поверхностью жидкости. Из рис. 8 видно, что во втором случае на линейной зависимости $h(t)$ наблюдается некий «наплыв».



а) б)

Рис. 8. Зависимость положения шарика от времени в случае,
когда шарик начинает движение с поверхности жидкости (а), и когда шарик успевает пролететь некоторое расстояние по воздуху, прежде чем попасть в жидкость (б)

Дифференцирование зависимости $h(t)$ по времени (переход от координаты к скорости) для двух значений начального положения шарика делает возможным интерпретацию полученных результатов. График полученной зависимости представлен на рис. 9. Можно видеть, что независимо от начального положения шарика через некоторое время его движение в вязкой жидкости становится равномерным.

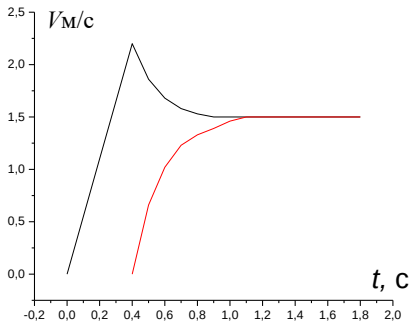


Рис. 9. Зависимость зависимости скорости движения шарика в вязкой жидкости от времени

Эксперимент по электронному дифференцированию кривой задержки вторичных электронов [4]

Схема проведения эксперимента приведена на рис. 10.

Направленный пучок электронов, создаваемый электронной пушкой *1* падает на поверхность образца *2*. Вторичные электроны (ВЭ), рассеянные мишенью регистрируются сферическим коллектором *3*. Если энергия электронов *Ep* в первичном пучке (ток I_0) имеет определенную величину, то в токе ВЭ (ток $I_к$) присутствуют электроны с энергией от 0 до *Ep*.

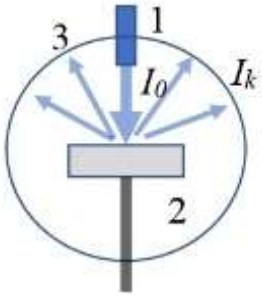


Рис. 10. Схема эксперимента по электронному дифференцированию

Если на коллектор подать запирающее напряжение *Uз*, то на него попадут только электроны, имеющие энергию от *eUз* до *Ep:* $I_k \to \int_{eU_3}^{E_p} N(E)dE$, где *N(E)* – функция распределения вторичных электронов по энергии. Для получения «кривой задержки» на коллектор подается задерживающее напряжение, линейно изменяющееся со временем: *Uз~k·t*. На рис. 11 приведена «кривая задержки» – зависимость тока на коллектор от потенциала коллектора.

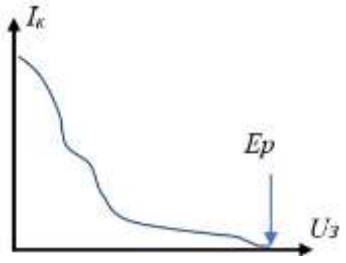


Рис. 11. Кривая задержки

Чтобы найти зависимость *N(E)*, нужно продифференцировать эту кривую по энергии. Для этого на линейно изменяющееся напряжение задержки накладывается переменное напряжение малой амплитуды.

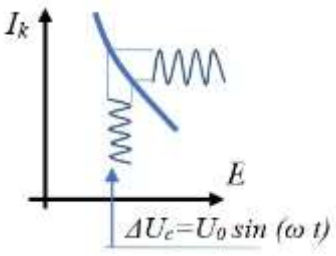


Рис. 12. Электронное дифференцирование «кривой задержки»

Тогда, ток на коллекторе можно представить в виде: $I_k = I_{k0}(U_3) + \frac{dI_k}{dU_c}\sin(\omega t) + \frac{d^2 I_k}{dU_c}\sin^2(\omega t) + \ldots$, где $I_{k0}(U_3)$ постоянная составляющая тока, $\frac{dI_k}{dU_c} \to N(E)$; $\frac{d^2 I_k}{dU_c^2} \to \frac{dN}{dE}$ вторая производная силы тока по напряжению.

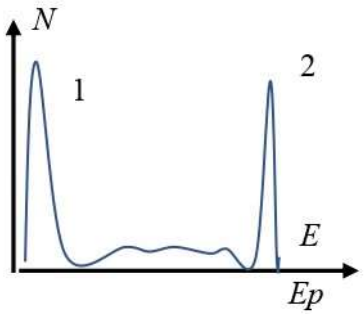


Рис. 13. График зависимости $N(E)$

Дифференцирование тока на коллекторе позволяет выделить на зависимости *N(E)* два участка (рис. 13): (*1*) – пик электронов с малой энергией (вторичные электроны), (*2*) – пик упруго отра между этими пиками наблюдается ряд особенностей, но их идентификация возможна только при повторном дифференцировании (рис. 14).

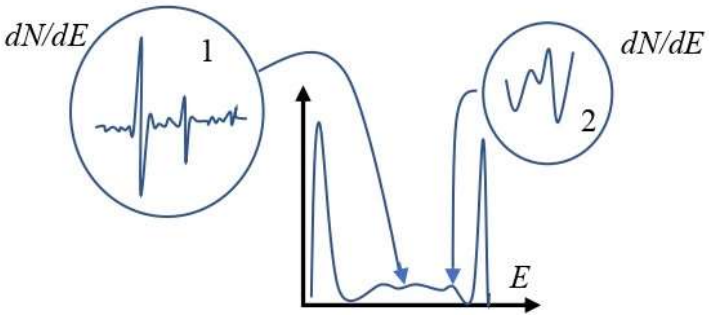


Рис. 14. Результат повторного дифференцирования кривой задержки

Слагаемое $\frac{d^2 I_k}{dU_c^2}\sin^2(\omega t)$, соответствует удвоенной частоте, так как $\sin^2(\omega t) = \frac{1-\cos(2\omega t)}{2}$. Настройкой тракта от коллектора до регистратора сигнала удвоенной частоты с использованием резонансного усилителя и синхронного детектора удается идентифицировать эти особенности. Таким образом, дифференцирование кривой задержки позволяет определить распределение вторичных электронов по энергии, а повторное дифференцирование – выявить данные о химическом составе и электронной структуре поверхности твердых тел.

Список используемых источников

1. Соловьев В. А., Яхонтова В. Е. Элементарные методы обработки результатов измерений. Л.: Изд-во ЛГУ.1977.

2. Yang J., Yang B., Liu M., Cao Y. Detection method of loose parts in nuclear reactor based on eigenvector algorithm // Progress in Nuclear Energy. 2016. Vol. 91. P. 250–255.

3. Шульман А. Р., Фридрихов С. А. Вторично-эмиссионные методы исследования твердого тела. М.: Наука, 1977. 551 с.

УДК 548.74
ГРНТИ 29.01.09

ВОСПРОИЗВОДСТВО КРАЕУГОЛЬНОГО ЭКСПЕРИМЕНТА КВАНТОВОЙ МЕХАНИКИ – ОПЫТА ДЭВИССОНА И ДЖЕРМЕРА ПО ДИФРАКЦИИ ЭЛЕКТРОНОВ

С. А. Князев, С. Н. Колгатин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

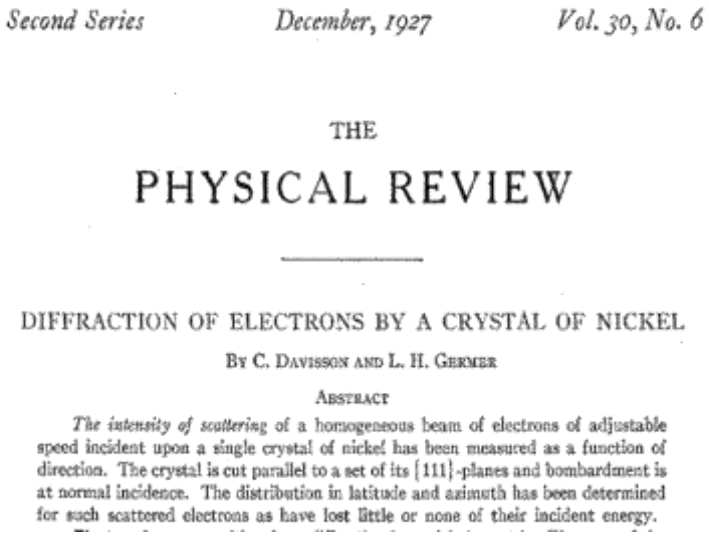
Опыты Дэвиссона и Джермера по дифракции электронов, проведенные в 1927 году, экспериментально подтвердили гипотезу де Бройля о корпускулярно-волновом дуализме, заложив тем самым основу квантовой механики. В данной работе воспроизводится этот эксперимент на современном оборудовании в ультравысоком вакууме с контролем за структурой и химическим составом поверхности рекристаллизованного никелевого образца.

дифракция электронов, корпускулярно-волновой дуализм

В начале 20 века классическая физика зашла в тупик при попытке определения того, что же из себя представляет свет: волны или частицы? Де Бройль решил «примирить» обе концепции на природу света – волновую и корпускулярную. Он высказал гипотезу о том, что свет в зависимости от обстоятельств может проявлять как волновые, так и корпускулярные свойства. Для получения соотношения, объединяющего эти свойства света, он использовал формулу Планка и формулу Эйнштейна, связывающую массу и энергию: $E = mc^2$ и $E = h\nu$, получив при этом соотношение, связывающее корпускулярные (импульс p) и волновые (λ) свойства света: $\lambda = h/p$. Следующим шагом де Бройля – было предположение о том, что данное соотношение носит всеобщий характер: **Каждому волновому процессу можно сопоставить систему квазичастиц, каждой частице соответствует некоторый волновой процесс.**

Эта идея, высказанная де Бройлем в 1924 году, не вызывала особого интереса до 1927 года, когда Дэвиссон и Джермер (Д. и Д.) обнаружили, что классические частицы – электроны способны создавать дифракционную

картину, т. е. обладают волновыми свойствами. Этот эксперимент [1] заложил краеугольный камень в создание принципиально нового направления в развитии физики – квантовой механики. На рис. 1 представлено факсимиле их статьи в журнале «THE PHYSICAL REVIEW».



Second Series *December, 1927* *Vol. 30, No. 6*

THE

PHYSICAL REVIEW

DIFFRACTION OF ELECTRONS BY A CRYSTAL OF NICKEL

By C. Davisson and L. H. Germer

Abstract

The intensity of scattering of a homogeneous beam of electrons of adjustable speed incident upon a single crystal of nickel has been measured as a function of direction. The crystal is cut parallel to a set of its {111}-planes and bombardment is at normal incidence. The distribution in latitude and azimuth has been determined for such scattered electrons as have lost little or none of their incident energy.

Рис. 1. Факсимиле их знаменитой статьи

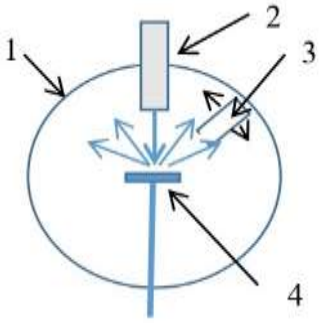


Рис. 2. Схема эксперимента Д. и Д.

1 – стеклянный корпус прибора.
2 – электронная пушка.
3 – цилиндр Фарадея, предназначенный для измерения интенсивности отраженных электронов. Его угловое положение изменялось с помощью двойного карданного подвеса.
4 – никелевая пластина.

Открытие, сделанное Д. и Д. – это результат аварийной ситуации, когда в результате разгерметизации стеклянного корпуса прибора произошло окисление поликристаллической никелевой пластинки. После починки прибора Д. и Д. провели несколько циклов очистки поверхности образца от окислов путем высокотемпературных прогревов в вакууме. В результате этих прогревов никелевая

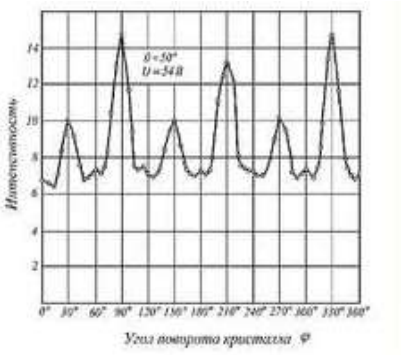


Рис. 3. Угловое распределение интенсивности

пластина изменила свою структуру – из поликристаллической она превратилась в крупноблочную и на угловой зависимости интенсивности рассеяния электронов появились отчетливо выраженные максимумы.

Условие образования дифракционных максимумов: $d \sin \varphi = k\lambda$, длина волны де Бройля: $\lambda = \frac{h}{p} = \frac{h}{mV}$, скорость электронов определяется из соотношения: $\frac{mV^2}{2} = eU$, длина волны электрона, прошедшего ускоряющую разность потенциалов U: $\lambda = \sqrt{\frac{150}{U}}$.

Расчеты положения дифракционных максимумов показали хорошее согласие с гипотезой де Бройля и предопределили начало бурного развития квантовой механики.

Метод дифракции медленных электронов (ДМЭ), созданный Д. и Д., получил широкое распространение и активно используется в настоящее время**.** Имеется много работ и по исследованию никеля методом ДМЭ, но все они выполнены на монокристаллических образцах [2–4]. В данном случае было решено воспроизвести эксперименты Д. и Д. на исходно поликристаллической фольге никеля.

Методика эксперимента по воспроизведению опытов Д. и Д.

Тонкие полоски Ni фольги крепились на стандартном фланце низковольтного дифрактометра. В отличие от многочасовых измерений углового распределения интенсивности рассеянных электронов в опытах Д. и Д., современные дифрактометры позволяют наблюдать полную картину дифракции на люминесцентном экране и фиксировать ее на камеру.

Рис. 4. Низковольтный дифрактометр

Химический состав поверхности образца контролировался методом Оже-электронной спектроскопии. Для очистки поверхности образца и ее рекристаллизации использовался высокотемпературный прогрев в вакууме при давлении остаточных газов ~10^{-7} Па и в атмосфере кислорода при давлении ~10^{-4}Па.

Результаты эксперимента

На начальной стадии (рис. 5) после откачки установки до рабочего вакуума картина ДМЭ отсутствовала, Оже-спектры содержали пики углерода, кислорода и серы. Прогрев образца при температурах 700–1 000^0 С в вакууме и в атмосфере кислорода привел к уменьшению концентрации углерода, серы на поверхности фольги и появлению Оже-пика никеля. После нескольких циклов такой обработки образца возникла слабая дифракционная картина, которая свидетельствовала о появлении на поверхности никеля укрупненных упорядоченных структур разнообразной ориентации, способных создавать достаточно сложную картину дифракции.

Рис. 5. Начальная стадия рекристаллизации Ni

После многократного повторения циклов прогрева образца удалось получить картину ДМЭ, которая свидетельствовала о выходе на поверхность грани (111) со структурой 1×1, повторив тем самым результаты Д. и Д. 90 летней давности (рис. 6).

Рис. 6. Появление упорядоченной структуры на поверхности Ni пластины

Данная работа представляет интерес как с точки зрения материала для раздела «история физики» – воспроизведение в современных условиях эксперимента, утвердившего идею корпускулярно-волнового дуализма, так и материала, который можно использовать в лекциях по курсу общей физики. Помимо этого, разработанная методика рекристаллизации тонких металлических фольг [5] позволяет проводить исследования процессов в нанометровом поверхностном слое, происходящих в результате каких-либо внешних воздействиях, без использования дорогостоящих монокристаллических образцов.

Список используемых источников

1. Савельев И. В. Курс общей физики: в 3-х т. М.: Наука, 1987. Т.1. 433 с.

2. Davisson C., Germer L. H. Diffraction of electron by a crystal of nickel // Phys. Rev. 1927. V. 30, № 6. pp. 705–712.

3. Feinstein L. G. LEED secondary Bragg peaks for Ni(111) // Surf. Sci. 1970. V. 19. pp. 366–370.

4. Nakano H., Nakamura J. Carbide-induced reconstruction initiated at step edges on Ni (111) // Surf. Sci. 2001. V. 482–485. pp. 341–345.

5. Усачёв Д. Ю., Добротворский А. М., Рыбкин А.Г., Адамчук В.К. Структурная стабильность ступенчатых поверхностей никеля // Физика твёрдого тела. 2011. Т. 53. С. 1211–1215.

6. Князев С. А., Корсуков В. Е. Структурные изменения на поверхности платины под воздействием механического растяжения // Физика твёрдого тела. 2005. Т. 47. С. 876–879.

Статья представлена на X Юбилейной международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», прошедшей 24–25 февраля 2021 года.

УДК 537.862
ГРНТИ 29.35.19

УСТАНОВКА ДЛЯ ДЕМОНСТРАЦИИ ВЗАИМОПРЕВРАЩЕНИЯ ЭЛЕКТРИЧЕСИХ И МАГНИТНЫХ ПОЛЕЙ

С. А. Князев, С. Н. Колгатин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Теоретические основы радиосвязи заложены в уравнениях Максвелла: изменяющееся во времени магнитное поле является источником вихревого электрического поля, электрические токи и переменное электрическое поле являются источником вихревого магнитного поля. Данная работа относится к истокам возникновения беспроводной передачи энергии – знаменитым опытам Герца.

опыт Герца, уравнения Максвелла.

Если на две проводящие параллельные пластины подать постоянное напряжение, то между ними возникает постоянное электрическое поле. При подаче на пластины линейно изменяющегося с течением времени напряжения между пластинами образуется, соответственно, линейно изменяющееся с течением времени электрическое поле, которое уже порождает стационарное магнитное поле. На этом процесс взаимопревращения полей заканчивается. Но если теперь на пластины подать напряжение, изменяющееся по закону $U_0 \sin(\omega t)$, то, в принципе, число таких взаимопревращений становится неограниченным, так как при дифференцировании выражений для E и H sin→cos→sin …. Возникает электромагнитная волна [1] (рис. 1, 2).

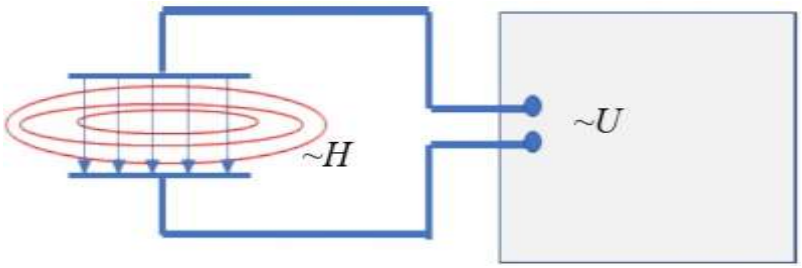


Рис. 1. Схема образования магнитного поля переменным электрическим полем

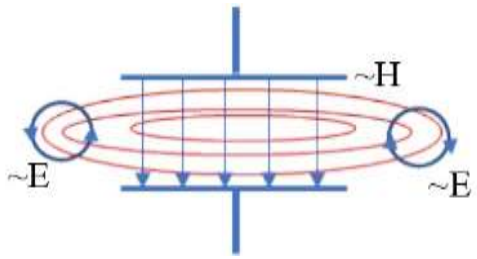


Рис. 2. Схема образования ЭДС индукции в проводящем контуре в переменном магнитном поле

Установка для демонстрации взаимопревращения электрических и магнитных полей

СВЧ генератор *1* подает переменное напряжение высокой частоты на пластины *2*, в результате чего между ними возникает переменное электрическое поле. Вокруг этого поля образуется переменное магнитное поле, вызывающее возникновение ЭДС индукции в каждом витке намотки тороида *3*. Если к концам этой намотки присоединить лампочку *4*, то она загорится. Кстати, это еще одно из взаимопревращений – возникновение электромагнитных световых колебаний (рис. 3).

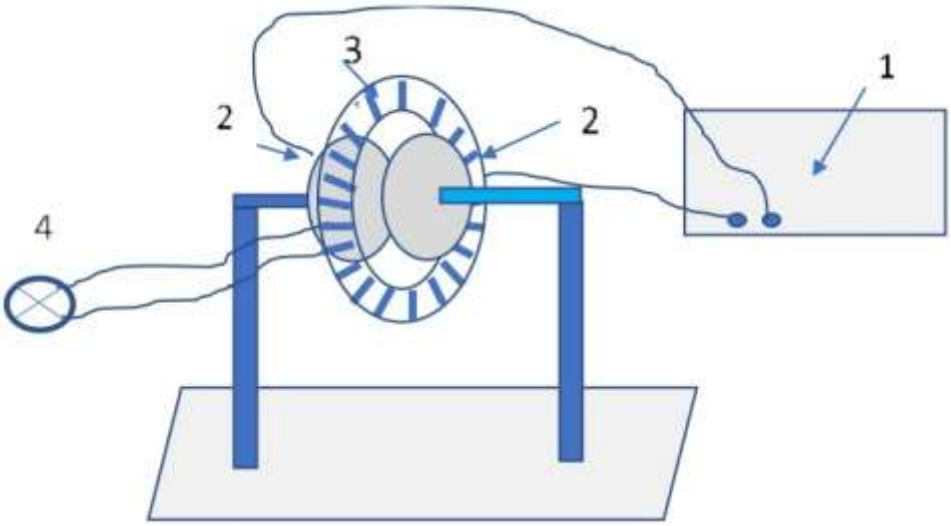


Рис. 3. Лекционная демонстрация

Данная лекционная демонстрация может быть также реализована в виде лабораторной работы с весьма интересным результатом – новым способом определения скорости распространения электромагнитной волны.

Преобразование лекционной демонстрации в лабораторную работу

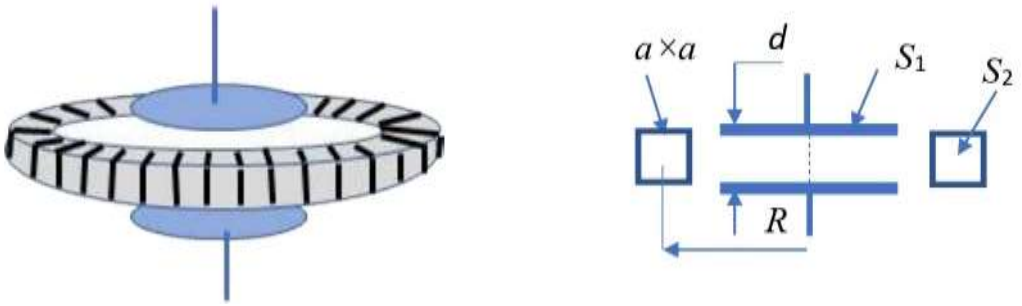


Рис. 4. Схема лабораторной работы

Пусть на пластины подается напряжение высокой частоты:

$$U(t) = U_0 \sin(\omega t). \quad (1)$$

Если считать, что электрическое поле между пластинами является однородным, то напряженность поля E между пластинами определяется соотношением:

$$E(t) = \frac{U_0}{d} \sin(\omega t), \quad (2)$$

где d – расстояние между пластинами.

Вектор электростатической индукции: $D(t) = \varepsilon\varepsilon_0 E(t)$.

Если величину ε принять равной 1, то

$$D(t) = \varepsilon_0 \frac{U_0}{d} \sin(\omega t). \quad (3)$$

3-е уравнение Максвелла в отсутствии токов проводимости имеет вид:

$$\oint H_l dl = \int (\frac{\partial D}{dt})_n dS. \quad (4)$$

Расстояние от оси пластин до осевой линии тороида, обозначенное как *R*, (рис. 3) существенно превышает размеры сечения тороида (*R* >> *a*). Поэтому можно считать, что магнитное поле внутри тороида является однородным. Тогда левую часть соотношения (4) можно представить как:

$$\oint H_l dl = H \cdot 2\pi R, \tag{5a}$$

а правую как:

$$\int (\frac{\partial D}{\partial t})_n dS = \varepsilon_0 \frac{U_0}{d} \omega \cos(\omega t) \cdot S_1, \tag{5b}$$

где S_1 – площадь параллельных пластин.

Из равенства выражений (5а) и (5б) следует:

$$H(r) = \varepsilon_0 \frac{U_0}{2\pi R d} \omega \cdot \cos(\omega t) \cdot S_1. \tag{6}$$

1-е уравнение Максвелла:

$$\oint E_l dl = -\int (\frac{\partial B}{\partial t})_n dS. \tag{7}$$

Если считать, что поперечное сечение тороида имеет форму квадрата со стороной *a* (см. рис. 3), то

$$\oint E_l dl = E \cdot 4a, \tag{8a}$$

где *a* – сторона квадратного сечения тороида.

Вектор магнитной индукции: $B(t) = \mu\mu_o H(t)$.

Если величину μ принять равной 1, то:

$$B = \mu_0 \varepsilon_0 \frac{U_0}{2\pi R d} \omega \cdot S_1 \cos(\omega t). \tag{8b}$$

Тогда:

$$\int (\frac{\partial B}{\partial t})_n dS = \mu_0 \varepsilon_0 \frac{U_0}{2\pi R d} \omega^2 a^2 S_1. \tag{9}$$

Из приравнивания (8а) и (9) следует:

$$\mu_0\varepsilon_0 \frac{U_0}{2\pi Rd}\omega^2 a^2 S_1 \sin(\omega t) = 4aE = U\,, \qquad (10)$$

где U – напряжение, возникающее в одном витке тороида.

С учетом числа витков тороида N:

$$U_{\text{общ}} = \mu_0\varepsilon_0 \frac{U_0 N}{2\pi Rd}\omega^2 a^2 S_1 \sin(\omega t)\,. \qquad (11)$$

В этом выражении помимо геометрических параметров R, d, S_1, напряжения на пластинах U_0 и его частоты ω, числа витков N, которые берутся из внешних данных, присутствуют $\boldsymbol{\mu_0\varepsilon_0}$, что открывает еще один способ определения скорости распространения электромагнитных волн путем замены лампочки на вольтметр переменного тока.

Список используемых источников

1. Савельев И. В. Курс общей физики: в 3-х т. М.: Наука, 1987. Т. 2. 405 с.

Статья представлена на X Юбилейной международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», прошедшей 24–25 февраля 2021 года.

УДК 537.22
ГРИТИ 29.19.23

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЭЛЕКТРОСТАТИЧЕСКИХ ПОЛЕЙ

С. А. Князев, С. Н. Колгатин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе ставится задача по воспроизводству качественной картины взаиморасположения эквипотенциалей для системы плоский конденсатор - проводник с сечением треугольной формы, стоящий на нижней пластине. Студентам предлагается в игровой манере воспроизвести эту картину с учетом того, что вдали от остроугольного проводника совокупность эквипотенциалей представляет собой систему линий, параллельных пластинам, а вблизи острия эти линии должны «просочиться» через зазор между верхней пластиной и вершиной острия. Далее предлагается оценить распределение плотности заряда на верхней и нижней пластинах, а также на поверхности проводника с сечением треугольной формы.

электростатическое поле, эквипотенциали, проводники в электрическом поле.

Основной задачей электростатики является определение потенциала и напряженности электрического поля, создаваемого заряженными проводниками [1]. Для проводников, обладающих высокой степенью симметрии (сфера, цилиндр, плоскость), эта задача решается с помощью теоремы Гаусса. В общем случае распределение потенциала вокруг заряженных проводников описывается уравнением Лапласа. Для решения этого уравнения, как правило, приходится прибегать к численным методам расчета электростатического поля или двумерному моделированию электрических полей.

Задача данной работы состоит в определении качественных изменений картины электрического поля между заряженными пластинами плоского конденсатора при помещении на нижнюю пластину проводника конусообразной формы. В отсутствии проводников между пластинами плоского конденсатора эквипотенциали (ЭП) представляют собой систему параллельных линий, значение потенциала которых изменяется линейно с расстоянием между пластинами. Наличие проводника остроконечной формы приводит к кардинальной перестройке системы ЭП: первоначально горизонтальный «поток» ЭП должен будет «просочиться» через малый зазор между острием и верхней пластиной и затем вновь превратиться в горизонтальный поток (рис. 1).

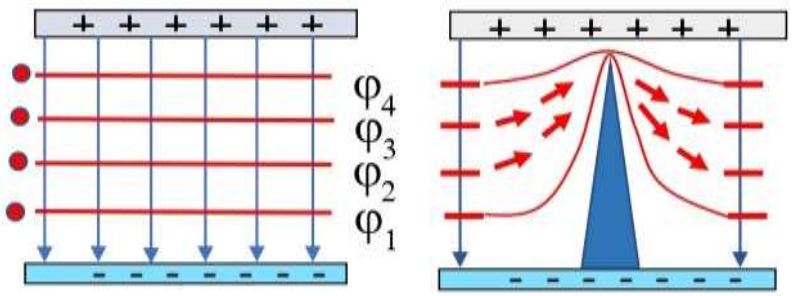


Рис. 1. Картина взаиморасположения ЭП при отсутствии (a) и наличии проводника (b) между пластинами конденсатора

Студентам предлагается в игровой манере воспроизвести качественную картину взаиморасположения ЭП для системы плоский конденсатор-проводник с сечением треугольной формы.

Алгоритм действий, связанных с построением ЭП следующий: по горизонтали пространство между пластинами разбивается на n уровней. Если разность потенциалов между пластинами равна U_0, то вдали от острия поле считается однородным и потенциал от точки к точке слева изменяется на величину U_0/n. Поиск точек, в которых потенциал равен потенциалу исходной точки слева, осуществляется вдоль вертикальных линий, отмеченных пунктиром. При попадании курсора в нужную точку и после клика мышки на ней появляется отрезок линии, соответствующий данной ЭП.

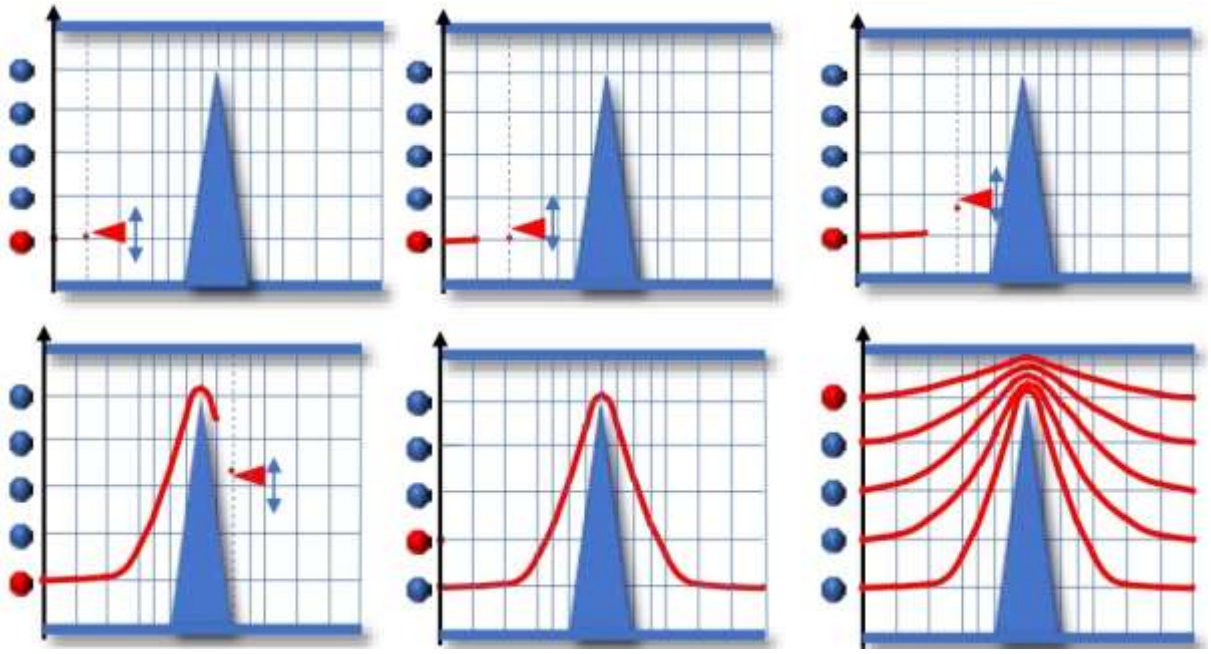


Рис. 2. Последовательность построения системы эквипотенциалей

Шаг № 1: Сначала, с помощью курсора выделяется нижняя точка, потенциал которой отличается от потенциала нижней пластины на величину U_0/n

Шаг № 2: Движением курсора вдоль первой вертикальной линии и периодическим нажатием на кнопку мыши, находится точка, потенциал которой равен потенциалу выделенной точки. При этом появляется отрезок линии, которая является отрезком первой ЭП.

Шаг № 3: Данная процедура повторяется на следующей вертикальной штриховой линии и т. д. Таким образом на экране монитора высвечивается первая ЭП.

Повторением данной процедуры для последующих точек, студент получает общую картину взаиморасположения ЭП между пластинами конденсатора.

Полученная путем многократного повторения процедуры построения по точкам система эквипотенциалей должна прочно закрепить в голове студента мысль о недопустимости нарушения законов электростатики: проводники, находящиеся в электростатическом поле и контактирующие друг с другом, имеют одинаковый потенциал. Вследствие этого, линии ЭП находящиеся вблизи проводников огибают эти проводники, а силовые линии поля направлены по нормали к поводящей поверхности проводника.

Следующий шаг состоит в выяснении того, как перераспределение заряда по поверхностям проводника конусообразной формы и пластин конденсатора приводит к кардинальной перестройке системы ЭП.

Напряженность электрического поля и плотность заряда на поверхности проводников

Теорема Гаусса: $\oint E_n dS = \dfrac{\sum q_i}{\varepsilon_0}$.

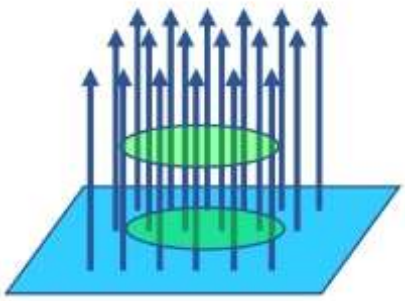


Рис. 3. Связь E и σ

Поскольку вектор E всегда направлен по нормали к заряженной поверхности, а торцевую поверхность интегрирования можно выбрать достаточно малой так, что поле внутри интегрируемого объема можно считать однородным, то $E = \dfrac{\sigma}{\varepsilon_0} = \dfrac{U}{d}$, где σ – поверхностная плотность заряда, d – расстояние между пластинами (рис. 3). На основании этого соотношения, по заданной величине U, студентам предлагается рассчитать напряженность электрического поля и поверхностную плотность заряда на пластинах конденсатора вдали от острия.

Напряженность электрического поля и поверхностная плотность заряда на кончике острия

На рис. 4: R – радиус закругления кончика острия. В дальнейшем, вершина острия заменяется сферой с радиусом r, потенциал которой равен потенциалу нижней пластины φ_0, R – расстояние от центра сферы до ближайшей ЭП, потенциал которой равен φ_1

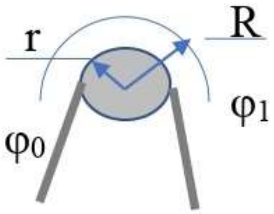


Рис. 4. Модель вершины острия

$$\varphi_0 = \frac{q}{4\pi\varepsilon_0 r} \quad q = \sigma \cdot 4\pi r^2 \quad \text{откуда} \quad \varphi_0 = \frac{\sigma \cdot r}{\varepsilon_0}$$

$$\varphi_1 = \frac{q}{4\pi\varepsilon_0 R} \quad \text{откуда} \quad \varphi_1 = \frac{\sigma \cdot r^2}{R \cdot \varepsilon_0} \quad \text{и} \quad \varphi_1 - \varphi_0 = \frac{\sigma \cdot r(r-R)}{R \cdot \varepsilon_0}.$$

Поверхностная плотность заряда на кончике острия:

$$\sigma = \frac{\Delta\varphi \cdot \varepsilon_0 \cdot R}{r(r-R)}.$$

Напряженность поля на кончике острия:

$$E = \frac{\sigma}{\varepsilon_0} = \frac{\Delta\varphi \cdot R}{r(r-R)}.$$

Напряженность электрического поля и поверхностная плотность заряда на верхней пластине конденсатора

Взаиморасположение силовых линий и эквипотенциальных поверхностей для системы точечный заряд – плоскость мало чем отличается от картины, создаваемой вершиной конуса с полусферическим закруглением и плоскостью. Поэтому возможно заменить конус на сферу с радиусом r и зарядом q. Напряженность поля E_o, создаваемая зарядом q, находящимся на расстоянии h от плоскости в точке x, как это показано на рисунке, определяется методом зеркального отражения.

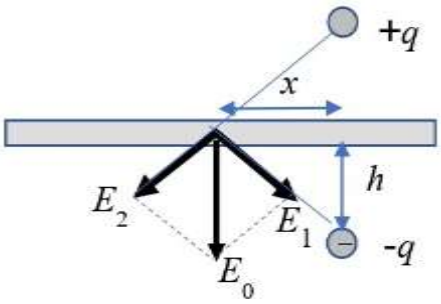


Рис. 5. Метод зеркального отражения

$$E_1 = \frac{q}{4\pi \cdot \varepsilon_0 (h^2 + x^2)} \qquad E_2 = \frac{q}{4\pi \cdot \varepsilon_0 (h^2 + x^2)} \qquad E_0 = \frac{q}{4\pi \cdot \varepsilon_0 (h^2 + x^2)^{3/2}}.$$

«Мертвая» зона у основания конуса

Пусть некая точка находится вблизи основания конуса и имеет потенциал равен φ_a. Тогда $E_{11}=(\varphi_a-\varphi_0)/l_1$, а $E_\perp=(\varphi_a-\varphi_0)/l_2$, где l_1 и l_2 – расстояния до нижней пластины и боковой поверхности конуса.

$$E_{\text{общ}}^2 = E_\perp^2 + E_{11}^2$$

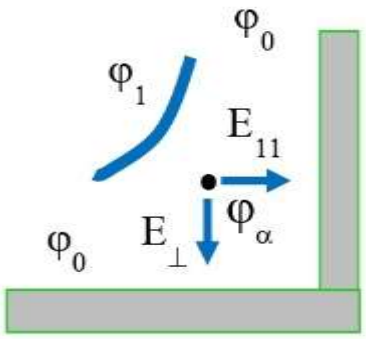


Рис. 6. Поле у основания конуса

Тогда нарушается главное условие: вектор E всегда должен быть $\perp$ поверхности проводника. Отсюда $E_{11} = 0$, $E_\perp = 0$. Но если $E = 0$, то и $\sigma = 0$.

Поскольку эта работа является качественной, то зона, где поле отсутствует, определяется следующим образом: расстояние от угловой точки до первой ЭП делится пополам и эта половина и есть радиус, определяющий «мертвую» зону на нижней пластине и боковой поверхности конуса, как это показано на рис. 7.

На пластинах конденсатора «вдали» от конуса и на боковой поверхности самого конуса величина E определяется как $(\varphi_1-\varphi_0)/l$, где l – расстояние от первой ЭП до поверхности проводника.

В итоге, студент должен воссоздать качественную картину распределения напряженности электрического поля и поверхностной плотности заряда на пластинах конденсатора и поверхности конуса.

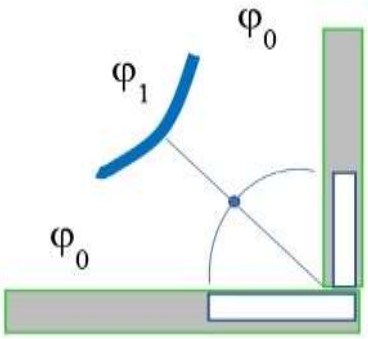


Рис. 7. Область мертвой зоны у основания конуса

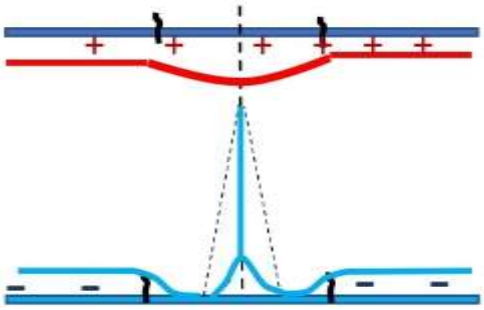


Рис. 8. Картина распределения заряда по поверхности пластин конденсатора и конуса

Основная задача многократного повторения процедуры построения системы ЭП состоит в закреплении с помощью визуального восприятия информации представления о том, что поверхность проводника, находящегося в электростатическом имеет одинаковый потенциал, что достигается неравномерным распределением заряда по его поверхности.

Список используемых источников

1. Савельев И. В. Курс общей физики: в 3-х т. М.: Наука, 1987. Т. 1. 433 с.

Статья представлена на X Юбилейной международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», прошедшей 24–25 февраля 2021 года.

УДК 548.74
ГРНТИ 29.19.11

ДИФРАКЦИЯ НА ГОФРИРОВАННОЙ ПОВЕРХНОСТИ В КИНЕМАТИЧЕСКОМ ПРИБЛИЖЕНИИ

С. А. Князев[1], Б. А. Обидов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Физико-технический институт РАН им. А. Ф. Иоффе

В рамках кинематической теории рассеяния рассматриваются особенности дифракции на поверхностных гофрированных структурах. Показано, что эти структурные дефекты приводят к существенным изменениям интенсивности и формы дифракционных максимумов по сравнению с картиной дифракции от идеальной поверхности.

дифракция, гофрированная поверхность, кинематическое приближение.

Дифракция на атомной цепочке [1]

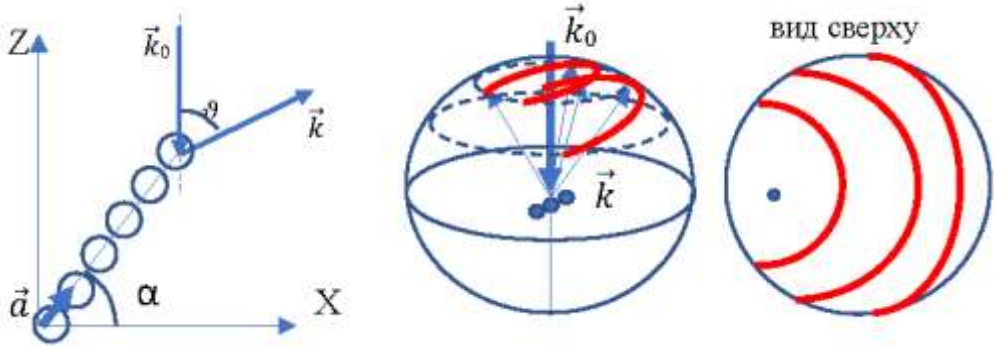


Рис. 1. Дифракция на атомной цепочке

$$A_{\text{общ}} = A_0 \sum_m^N \exp(2\pi i((\vec{k} - \vec{k}_0)\cdot\vec{a}),$$

где $\vec{k}_0(0,0,\frac{1}{\lambda})$ – волновой вектор падающей волны;

$\vec{k}_0(\frac{1}{\lambda}\sin\vartheta\cdot\cos\varphi, \frac{1}{\lambda}\sin\vartheta\cdot\sin\varphi, \frac{1}{\lambda}\cos\vartheta)$ – вектор рассеянной волны;

$\vec{a}(a\cdot\cos\alpha, a\cdot\sin\alpha)$ – трансляционный вектор. $\frac{2\pi a}{\lambda} = B$.

Обозначения: $\sin\vartheta\cdot\cos\varphi = x; \sin\vartheta\cdot\sin\varphi = y; \cos\vartheta = \sqrt{1-(x^2+y^2)}$.

$$I = \left|A_{общ}\right|^2 = A_0^2 \left| \frac{\exp(iBN(x\cdot\cos\alpha + (1+\sqrt{1-(x^2+y^2)}\sin\alpha) - 1}{\exp(iB(x\cdot\cos\alpha + (1+\sqrt{1-(x^2+y^2)}\sin\alpha) - 1} \right|^2 .$$

Дифракция на наклонной плоскости

Переход к рассеянию на наклонной плоскости осуществляется добавлением множителя, связанного с суммированием вторичных волн по направлению оси Y: $\frac{\exp(i\cdot B\cdot N\cdot y)-1}{\exp(i\cdot B\cdot y)-1}$.

Дифракция на гофрированной поверхности

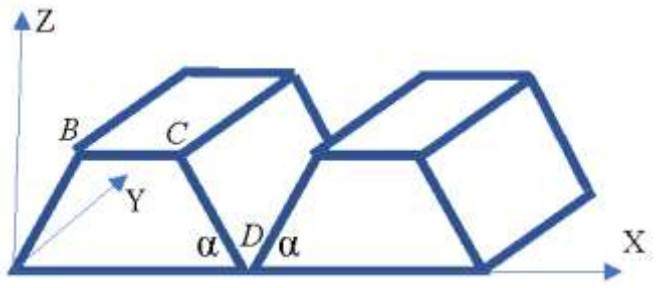


Рис. 2. Гофрированная поверхность

N_1 – число атомов вдоль левой и правой образующих.

N_2 – число атомов на горизонтальном участке.

N_3 – число атомов вдоль оси Y.

Координаты точек в системе координат XZ:

$$B\ ((N_1-1)\cdot a\cdot\cos(\alpha),\ (N_1-1)\cdot a\cdot\sin(\alpha));$$
$$C\ ((N_1-1)\cdot a\cdot\cos(\alpha)+(N_2-1)\cdot a,\ (N_1-1)\cdot a\cdot\sin(\alpha));$$
$$D\ (2\cdot(N_1-1)\cdot a\cdot\cos(\alpha)+(N_2-1)\cdot a,\ 0),$$

где a – постоянная квадратной решетки.

Структура достаточно громоздкого выражения для интенсивности при дифракции на гофрированной поверхности имеет вид:

$$I = |(A_{01}+A_{02}+A_{03})A_{04}\times A_{05}|^2,$$

где A_{01} – суммарная амплитуда рассеяния по левой образующей вдоль оси X:

$$A_0 \frac{\exp(iBN_1(x\cdot\cos\alpha + \sin\alpha(1+\sqrt{1-(x^2+y^2)})) - 1)}{\exp(iB(x\cdot\cos\alpha + \sin\alpha(1+\sqrt{1-(x^2+y^2)})) - 1)}.$$

A_{02} – по участку гофра BC с учетом сдвига в точку B:

$$A_0 \cdot \exp(iB(N_1-1)(x\cdot\cos\alpha+\sin\alpha(1+\sqrt{1-(x^2+y^2)}))\frac{\exp(i\cdot B\cdot N_2\cdot x)-1}{\exp(i\cdot B\cdot x)-1}.$$

A_{03} – по правой образующей:

$$A_0\frac{\exp(iBN_1(x\cdot\cos\alpha-\sin\alpha(1+\sqrt{1-(x^2+y^2)}))-1)}{\exp(iB(x\cdot\cos\alpha-\sin\alpha(1+\sqrt{1-(x^2+y^2)}))-1)}\times$$

$$\times(\exp(iB\cdot((N_1-1)x\cdot\cos\alpha+\sin\alpha(1+\sqrt{1-(x^2+y^2)})))+(N_2-1))x).$$

A_{04} – суммарная амплитуда рассеяния по оси Y, одинаковая для всех образующих гофра:

$$\frac{\exp(i\cdot B\cdot N_3\cdot y)-1}{\exp(i\cdot B\cdot y)-1}.$$

A_{05} – суммарная амплитуда рассеяния между гофрами:

$$\frac{\exp(i\cdot B\cdot M\cdot(2(N_1-1)\cdot\cos\alpha+(N_2-1)))\cdot x-1}{\exp(i\cdot B\cdot(2(N_1-1)\cdot\cos\alpha+(N_2-1)))\cdot x-1}.$$

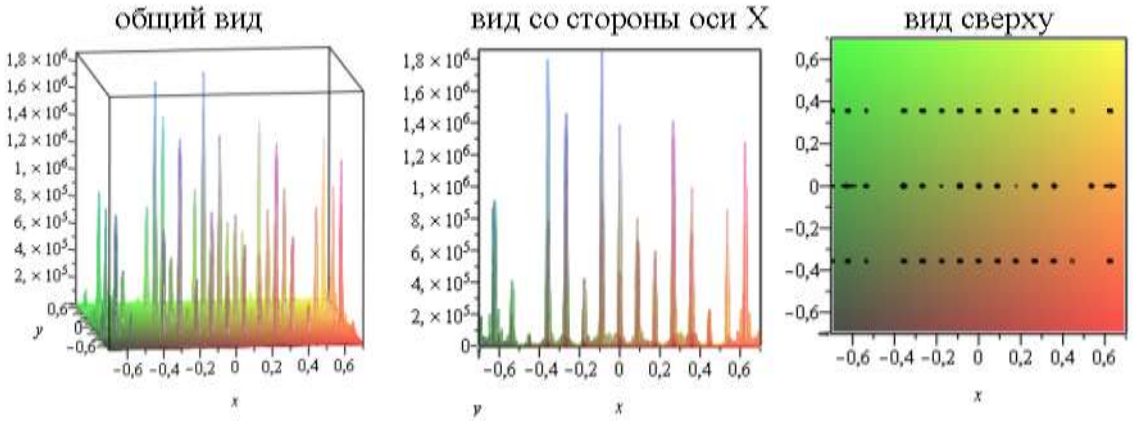


Рис. 3. Дифракционная картина от гофрированной поверхности $N_{1,2}$ = 5, N_3 = 40, N_4 = 6, α = 30° энергия 130 эВ

Для идентификации дифракционной картины, представленной на рис. 3, рассматривается результат наложения картин дифракции от 6 левых боковин, 6 правых боковин и 6 горизонтальных участков гофрированной структуры, расположенных на расстоянии трансляционного вектора между соседними гофрами т. е. результат сложения интенсивностей от различных участков периодической гофрированной поверхности. Красные точки – это

рефлексы, обусловленные дифракцией от горизонтальных участков гофров, а синие и зеленые – от двух боковин. Видно, что угловые положения рефлексов на рис. 3 и 4 практически совпадают. Таким образом угловое положение рефлексов на дифракционной картине соответствует простому наложению картин дифракции от трех составляющих гофра – двух боковин и горизонтального участка.

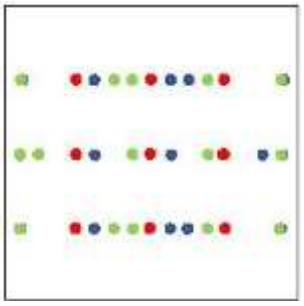


Рис. 4. Наложение картин дифракции от составляющих гофра

Интенсивность картины дифракции и интерференционные эффекты

Интенсивность рефлексов на дифракционной картине, представленной на рис. 3, составляет $A_0^2 \cdot 1{,}8 \cdot 10^6$. Интенсивность рефлексов на дифракционной картине от 6 боковин, представленной на рис. 4, составляет $A_0^2 \cdot 1{,}4 \cdot 10^6$ Дополнительные расчеты показали, что интенсивность дифракционных максимумов от одной боковины составляет $A_0^2 \cdot 4 \cdot 10^4$ Суммирование интенсивности от 6 боковин составит $A_0^2 \cdot 2{,}4 \cdot 10^5$ Суммирование амплитуд от соседних боковин с нулевой разностью фаз дает $I = A_0^2 \cdot 1{,}44 \cdot 10^6$. Таким образом, формирование интенсивности рефлексов на общей картине (рис. 3) обусловлено сложными интерференционными эффектами как между отдельными участками гофр, так и самими гофрами.

Интерференционные эффекты – 1 гофр

Интенсивность дифракционной картины от одного гофра:

$$I = |A_1+A_2+A_3|^2,$$

где A_1, A_2, A_3 – суммарные амплитуды рассеяния от трех составляющих гофра в комплексном виде. Тогда, $I = A^*_1 \cdot A_1 + A^*_2 \cdot A_2 + A^*_3 \cdot A_3 + 2A^*_1 \cdot A_2 + 2A^*_1 \cdot A_3 + 2A^*_2 \cdot A_3 + 2A_1 \cdot A^*_2 + 2A_1 \cdot A^*_3 + 2A_2 \cdot A^*_3$, где $A^*_1 \cdot A_1 = I_1$ – интенсивность от левой боковины, $A^*_2 \cdot A_2 = I_2$ – от горизонтального участка гофра, $A^*_3 \cdot A_3 = I_3$ – от правой боковины. Остальное – интерференционные слагаемые ($I_{int} = I_{com} – (I_1 + I_2 + I_3)$).

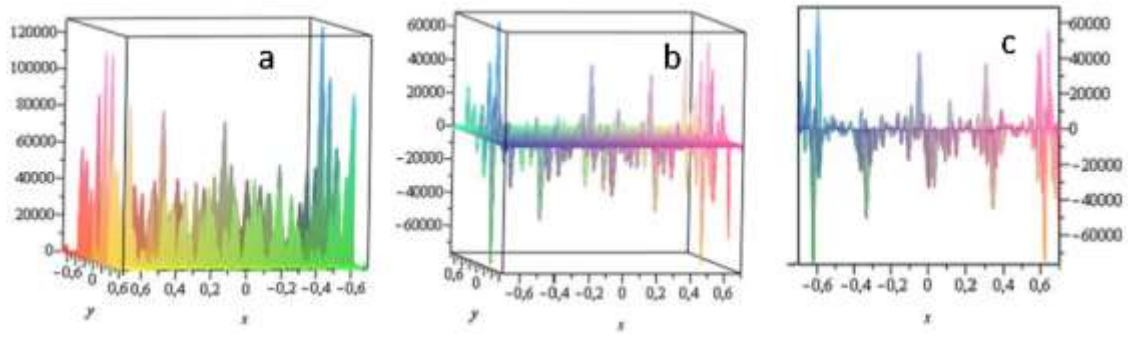


Рис. 5. a – картина дифракции, b, c – вклад интерференционного слагаемого

Интерференционные эффекты – 6 гофр

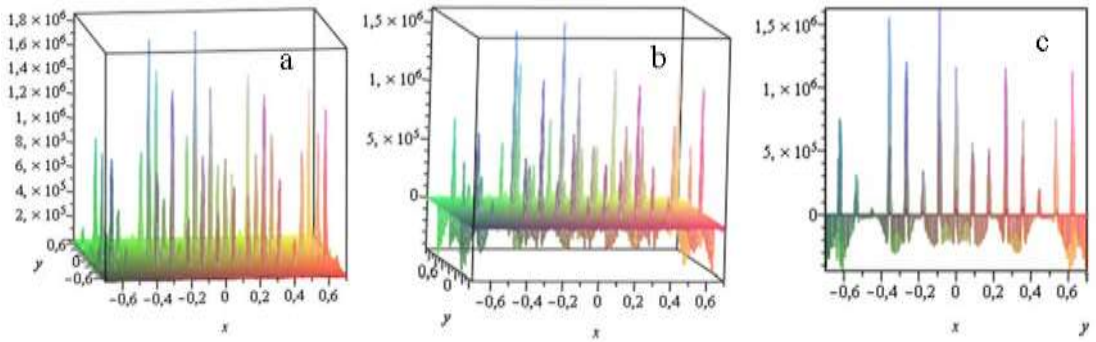


Рис. 6. a – картина дифракции, b, c – вклад интерференционного слагаемого

Из данных, представленных на рис 5, следует, что вклад в интенсивность «+» и «–» компонент интерференционного слагаемого примерно одинаков и сравним с интенсивностью всей картины дифракции. Рис. 6 показывает, что вклад в интенсивность «+» компоненты интерференционного слагаемого оказывает решающее влияние на формирование дифракционной картины.

Изменение угла наклона образующих гофра

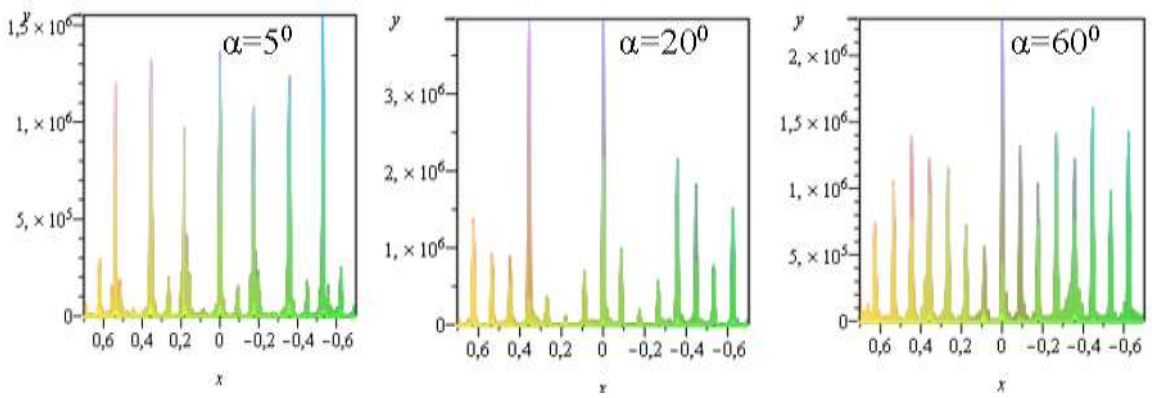


Рис. 7. Профили дифракционной картины от гофрированной поверхности 5×40 – M = 6, 130 эВ при различных значениях угла α

Изменение энергии первичного пучка Ep
(изменение электронной длины волны λ)

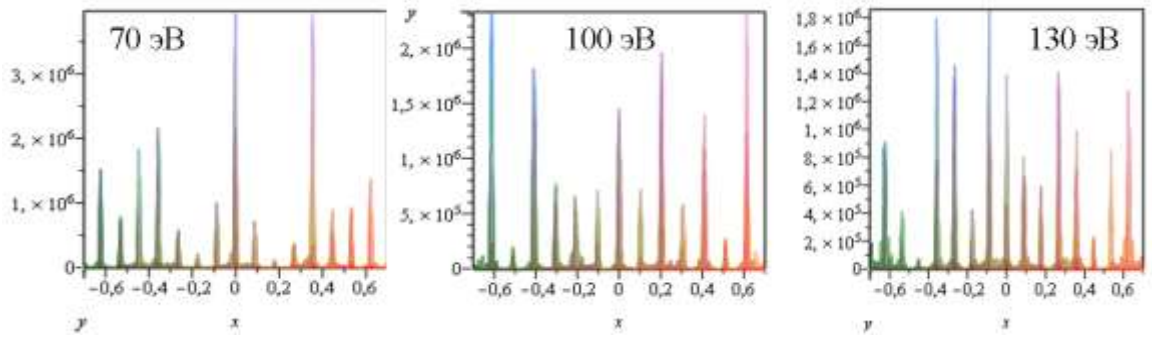


Рис. 8. Профили дифракционной картины от гофрированной поверхности 5×40 от 6 гофр, α = 30° при различных значениях Ep

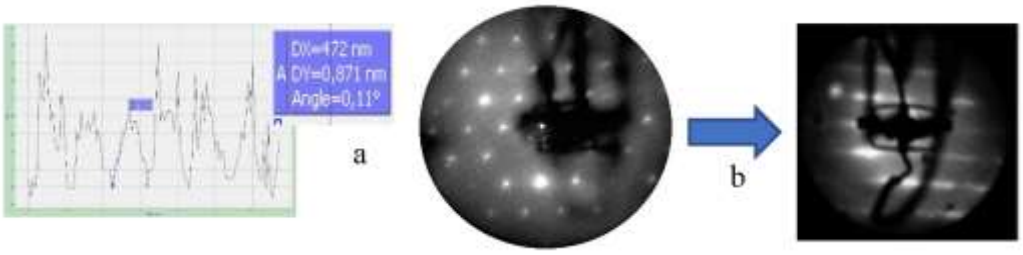


Рис. 9. *a* – профиль поверхности слюды и соответствующая ей картина ДМЭ, *b* – картина ДМЭ от изогнутой полоски слюды

Примеры дифракционных картин от гофрированных поверхностей

На рис. 9 в части *a* представлен профиль поверхности слюды, считающейся эталоном гладкости, полученный в атомно-силовом микроскопе и соответствующая картина дифракции электронов (ДМЭ). Если теперь тонкая полоска слюды подвергается деформации изгиба, то на дифракционной картине (рис. 9, часть *b*) возникают полосы, свидетельствуя об образовании на изогнутой поверхности гофрировки большего масштаба, которая уже приводит к существенной перестройке картины ДМЭ.

Появление частично упорядоченных гофрированных структур наблюдается и в процессе рекристаллизации поликристаллических вольфрамовых лент (рис. 10).

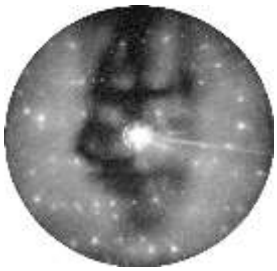


Рис. 10. Картина ДМЭ от W ленты

Заключение

Любая реальная поверхность в нанометровом масштабе не является атомно-гладкой и в этом масштабе представляет собой систему «холмов и впадин», которую, естественно, следует моделировать как гофрированную поверхность.

Расчеты дифракционных картин от таких структур, выполненные в кинематическом приближении, показали многообразие изменений на этих картинах по сравнению с дифракцией на «идеальной» поверхности. Это и существенная разница в интенсивности и форме рефлексов, и образование цепочек из дифракционных максимумов, и резкая смена взаиморасположения рефлексов при незначительном изменении длины электронной волны.

Список используемых источников

1. Пинскер З. Г. Дифракция электронов. М.; Л.: изд-во АН СССР, 1949. 404 с.

УДК 537.533.73
ГРИТИ 29.19.11

ДИФРАКЦИЯ НА СТРУКТУРЕ ИЗ РАЗОРИЕНТИРОВАННЫХ БЛОКОВ В КИНЕМАТИЧЕСКОМ ПРИБЛИЖЕНИИ

С. А. Князев[1], **Б. А. Обидов**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Физико-технический институт РАН им. А. Ф. Иоффе

В рамках кинематической теории рассеяния рассматриваются особенности дифракции на поверхностных структурах, состоящих из отдельных двумерных блоков, лежащих в одной плоскости и разориентированных друг относительно друга. Показано, что интерференционные эффекты, обусловленные межблочным рассеянием, не оказывают существенного влияния на интенсивность рефлексов от каждого из блоков и не приводят к появлению новых дифракционных максимумов. Исключение составляют максимумы зеркального отражения.

кинематическая теория рассеяния, двумерные блоки, межблочное рассеяние.

Кинематика рассеяния на двумерном блоке

Согласно теории рассеяния рентгеновских лучей [1], интенсивность дифракционной картины – это квадрат модуля результирующей амплитуды. На рис. 1 представлена схема рассеяния на двумерной структуре.

$\vec{k}_0(0,0,\frac{1}{\lambda})$ – волновой вектор падающей волны;

$\vec{k}(\frac{1}{\lambda}\sin\vartheta\cos\varphi,\frac{1}{\lambda}\sin\vartheta\sin\varphi,-\frac{1}{\lambda}\cos\varphi)$ – волновой вектор рассеянной волны,

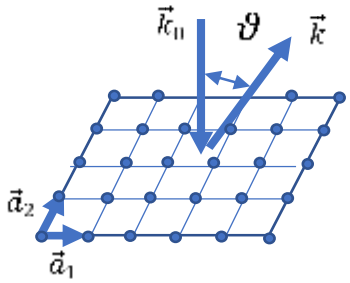


Рис. 1. Кинематика рассеяния на двумерной структуре

где ϑ, φ – углы рассеяния в сферической системе координат;
$\vec{a}_1, \vec{a}_2$ – трансляционные вектора;
λ – длина волны.

Результирующая амплитуда рассеяния определяется соотношением:

$$A_{\text{общ}} = A_0 \sum_{m,n}^{N,M} \exp(2\pi i(\vec{k} - \vec{k}_0, \vec{r}_{m,n}),$$

где $\vec{r}_{m,n}$ – координаты рассеивающих узлов. Выражение для интенсивности имеет вид:

$$I = A_0^2 \left| \frac{1-\exp(iNx)}{1-\exp(ix)} \frac{1-\exp(iMy)}{1-\exp(iy)} \right|^2, \quad (1)$$

где $\frac{2\pi a}{\lambda} \sin\vartheta\cos\varphi = x$, $\frac{2\pi a}{\lambda} \sin\vartheta\sin\varphi = y$; где a – постоянная решетки, N, M – число рассеивающих центров вдоль трансляционных векторов.

«Прямой» блок с элементарной ячейкой в виде квадрата (N, M = 10×10)

Трансляционные вектора направлены по осям X и Y. Интенсивность и угловое расположение рефлексов на дифракционной картине, представленной на рис. 2, определяются соотношением (1).

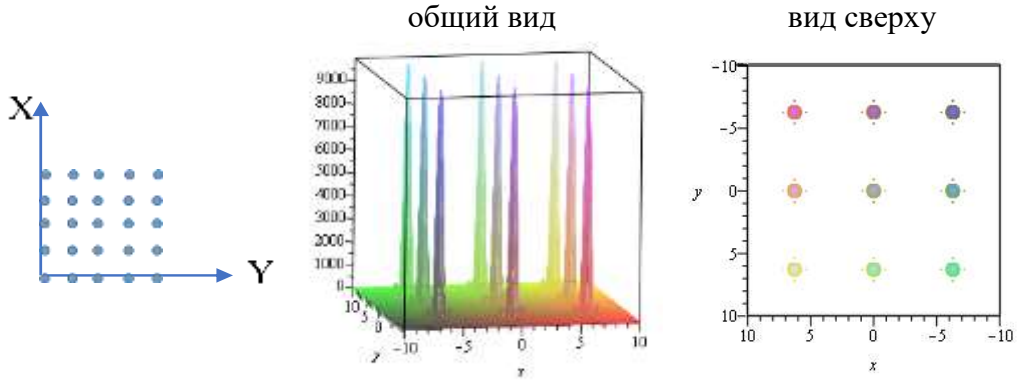
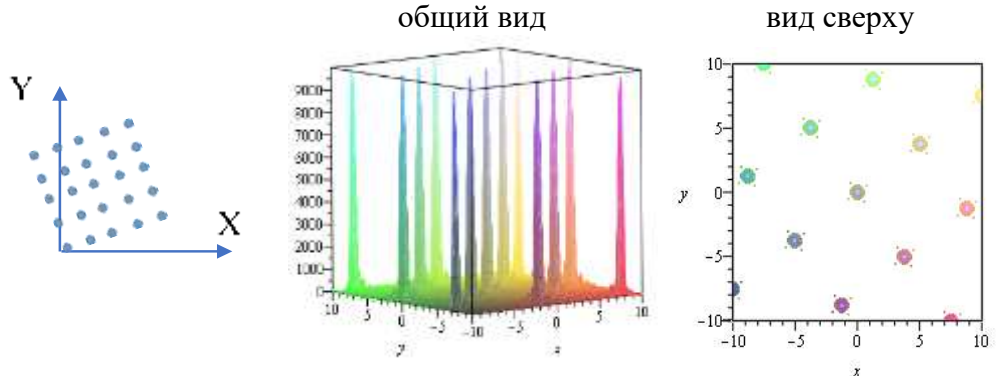


Рис. 2. Общий вид дифракционной картины и ее проекция на плоскость *XOY*

«Развернутый» блок с элементарной ячейкой в виде квадрата (10×10)

Трансляционные вектора имеют компоненты: $\vec{a}_1(a\cdot\cos\alpha, a\cdot\sin\alpha)$ $\vec{a}_1(a\cdot\cos\alpha, -a\cdot\sin\alpha)$, где α – угол трансляционного вектора $\vec{a}_1$ с осью X

$$I = A_0^2\left|\frac{1-\exp(iN(x\cos\alpha+y\sin\alpha)}{1-\exp(i(x\cos\alpha+y\sin\alpha)}\frac{1-\exp(iN(x\sin\alpha-y\cos\alpha)}{1-\exp(i(x\sin\alpha-y\cos\alpha)}\right|^2 \qquad (2)$$



Система из двух блоков, развернутых друг относительно друга, лежащих внутри области, ограниченной радиусом когерентности (10×10 +10×10)

$$I = A_0^2\left|\frac{1-\exp(iN(x\cos\alpha+y\sin\alpha)}{1-\exp(i(x\cos\alpha+y\sin\alpha)}\frac{1-\exp(iN(x\sin\alpha-y\cos\alpha)}{1-\exp(i(x\sin\alpha-y\cos\alpha)}+\right.$$
$$\left.+\frac{\exp(i(Nx+\Delta))-\exp(i\Delta)}{1-\exp(ix)}\frac{1-\exp(iNy)}{1-\exp(iy)}\right|^2, \qquad (3)$$

где Δ – величина смещения «прямого» блока вдоль оси *X*.

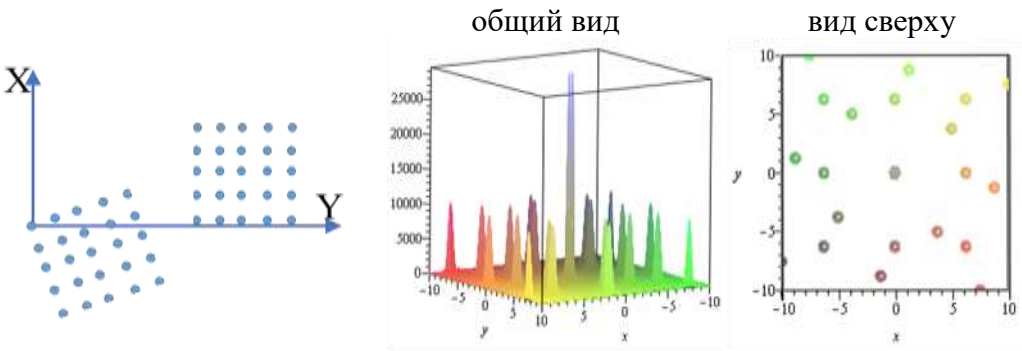


Рис. 4. Дифракционная картина от системы из двух блоков, развернутых друг относительно друга

Геометрия дифракционной картины от двух блоков

Из рис. 5 следует, что картина дифракции от системы из двух блоков представляет собой наложение двух дифракционных картин от каждого из блоков в отдельности.

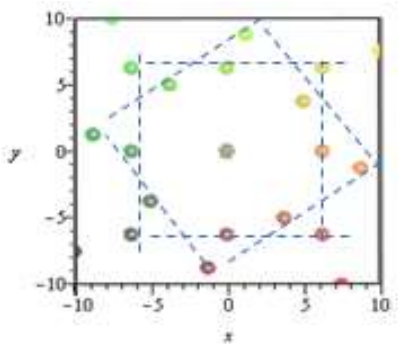


Рис. 5. Наложение дифракционных картин от двух блоков

Этот факт используется для интерпретации сложных картин дифракции медленных электронов (ДМЭ) от частично упорядоченных поверхностных структур, возникающих на начальной стадии рекристаллизации вольфрамовой фольги: сетка гномостереографических (ГНСТ) проекций от различных граней [2] накладывается на изображение картины ДМЭ и, путем поворота сеток этих проекций относительно (00) рефлекса, определяются рефлексы, совпадающие с пересечением меридианных и параллельных линий. Из представленных результатов следует, что на собирательной стадии рекристаллизации начинают формироваться блоки, с гранями (100) и (112), выходящими на поверхность, которые разориентированны друг относительно друга.

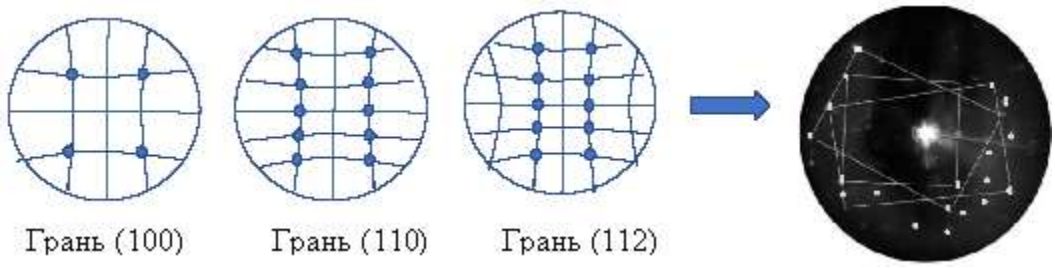


Рис. 6. Гномостереографические проекции различных граней и картина ДМЭ от W полоски на ранней стадии рекристаллизации

Влияние межблочной интерференции на дифракционную картину.

Если первое слагаемое в формуле (3) обозначить как A, а второе как B, то $|A+B|^2 = (A+B)(A^*+B^*) = AA^* + AB^* + BA^* + BB^*$, где первое слагаемое AA^* – это интенсивность дифракционной картины от первого блока, BB^* – от второго и AB^*+BA^* – это вклад в интенсивность, обусловленный интерференционными эффектами.

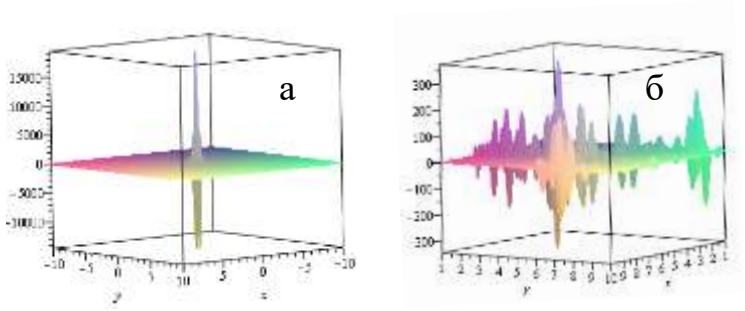


Рис. 7. Дифракционная картина
от $BA^* + AB^*$, a – общий вид, b – вне (00) рефлекса

Из рис. 7 видно, что интерференционное слагаемое оказывает основное влияние только на (00) рефлекс.

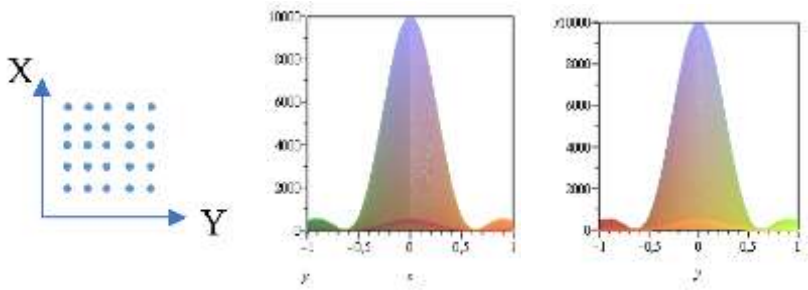


Рис. 8a. Интенсивность и форма (00) рефлекса при дифракции на одном блоке 10×10

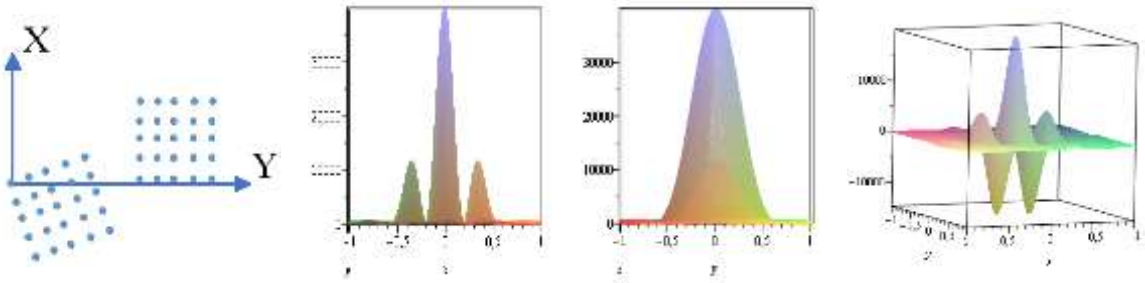


Рис. 8b. Интенсивность и форма (00) рефлекса при дифракции двух блоках
и интерференционное слагаемое

При дифракции на одном блоке угловая ширина (положение первого минимума) (00) рефлекса одинакова для обоих направлений. При дифракции на двух блоках угловая ширина остается неизменной – изменяется форма рефлекса за счет интерференции.

Выявление системы разориентированных блоков
по значительно большей интенсивности одного из рефлексов

Для выявления блоков, поверхность которых параллельна поверхности W образца, было необходимо изменить угол падения первичного пучка с тем, чтобы вывести (00) рефлекс из области тени от кристаллодержателя.

Совмещение центра сеток ГНСТ проекций с положением зеркально отраженного пучка показало, что в некоторых областях на поверхности фольги происходит самоорганизация блочных структур, лежащих в плоскости поверхности образца и разориентированных друг относительно друга.

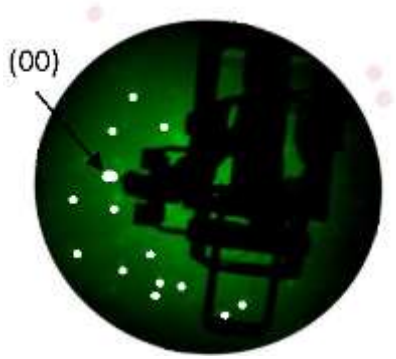


Рис. 9. Картина ДМЭ от Ni полоски

Таким образом, анализ взаиморасположения рефлексов и их сравнительной интенсивности на картинах ДМЭ в рамках кинематического приближения позволяет получать информацию о структурных дефектах в нанометровом поверхностном слое.

Список используемых источников

1. Иверонова В. И., Ревкевич Г. П. Теория рассеяния рентгеновских лучей. М.: изд-во МГУ, 1978.
2. Шаскольская М. П. Кристаллография. М.: Наука, 1984. 376 с.

Статья представлена на X Юбилейной международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», прошедшей 24–25 февраля 2021 года.

УДК 537.533.73
ГРИТИ 29.19.11

ДИФРАКЦИЯ НА СТУПЕНЧАТОЙ СТРУКТУРЕ В КИНЕМАТИЧЕСКОМ ПРИБЛИЖЕНИИ

С. А. Князев[1], Б. А. Обидов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Физико-технический институт РАН им. А. Ф. Иоффе

В рамках кинематической теории рассеяния рассматриваются особенности дифракции на поверхностных структурах, состоящих из упорядоченно и неупорядоченно расположенных ступеньках. Показано, что эти структурные дефекты приводят к существенным изменениям интенсивности и формы дифракционных максимумов по сравнению с картиной дифракции от идеальной поверхности.

дифракция, ступенчатая поверхность, кинематическое приближение.

Реальная поверхность твердого тела всегда состоит из отдельных блоков с различной степенью разориентации. Основными типами структурных

нарушений в направлении перпендикулярном поверхности (шероховатость), которая в макромасштабе считается плоской, являются микроступеньки и гофрировка. Для обработанной по высшему классу полировки поверхности допустимы неровности ~10 нм, тогда как длина волны у электронов с энергией 150 эВ – 0,1 нм т. е. в 100 раз меньше. Вместе с тем, после различного рода обработки поверхности монокристаллов в сверхвысоковакуумных условиях удается получить качественную картину дифракции медленных электронов (ДМЭ). Теоретические аспекты рассеяния электронов на несовершенных структурах были заложены еще в работах M. Hensler [1]. Большинство работ по исследованию ступенчатых структур эмиссионными методами связаны с изучением специфики образования доменных структур, процессам адсорбции, фазовым переходам на поверхностных ступенчатых структурах [2–5]. В данной работе в рамках кинематического приближения рассматривается влияние различных параметров ступенек и длины волны анализирующих электронов на форму и интенсивность дифракционных максимумов.

Из курса общей физики – раздел оптика, многолучевая интерференция, дифракционная решетка [6].

Дифракция на цепочке из рассеивающих центров

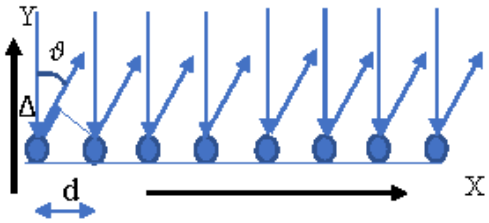


Рис. 1. Рассеивающая цепочка

$$A_{\text{общ}} = A_0 \sum_{m=1}^{N-1} e^{i\cdot m\cdot\delta} = A_0 \frac{\exp(iN\delta)-1}{\exp(i\delta)-1};$$

$$I = A_0^2 \left| \frac{\exp(iN\delta)-1}{\exp(i\delta)-1} \right|^2 = \frac{\sin^2(N\frac{\delta}{2})}{\sin^2(\frac{\delta}{2})}. \quad (1)$$

Условие образования дифракционных максимумов: $\delta = 2k\,\pi$

Переход к трехмерному рассмотрению дифракционного процесса

Если волновой вектор падающей волны $\vec{k}_0$ направлен вдоль оси Z, то его компоненты по осям *XYZ* равны $(0,0,\frac{1}{\lambda})$, а у вектора рассеянной волны $\vec{k}(\frac{1}{\lambda}\sin\vartheta\cdot\cos\varphi,\frac{1}{\lambda}\sin\vartheta\cdot\sin\varphi,-\frac{1}{\lambda}\cos\vartheta$. Результирующая амплитуда рассеяния находится суммированием вторичных волн по всем узлам рассматриваемой структуры $A_{\text{общ}} = A_0\sum_{m,n}^{N,N}\exp(2\pi\cdot i(\vec{k}-\vec{k}_0,\vec{r}_{m,n})$ где $\vec{r}_{\text{mn}}$ – вектор узла рассеивающей структуры, а интенсивность – как квадрат ее модуля.

Дифракция на ступенчатых структурах

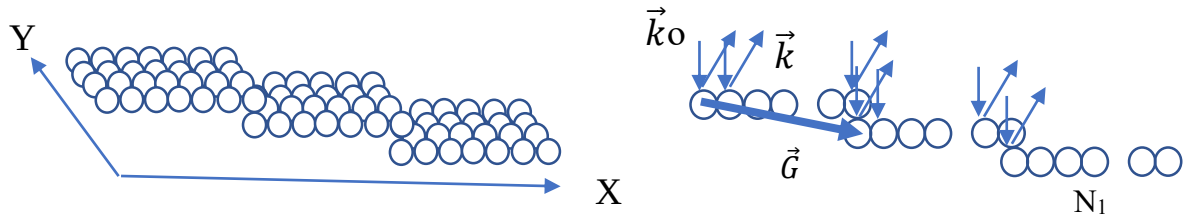
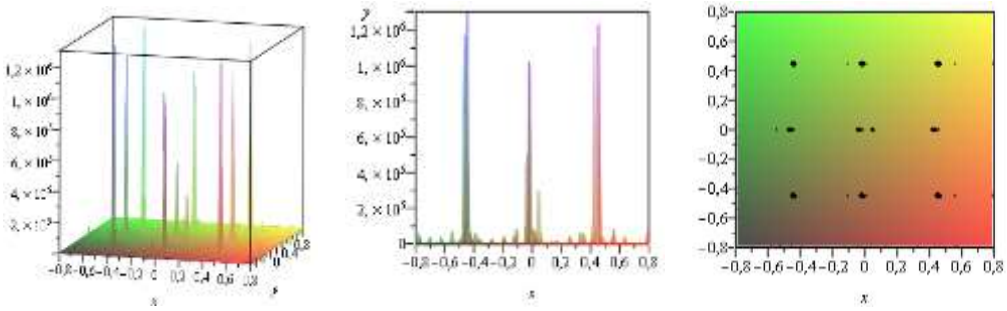


Рис. 2. Параметры ступенчатой структуры

Интенсивность дифракционной картины определяется соотношением:

$$I = A_0^2 \left| \frac{\exp(i\cdot B\cdot N_1\cdot x)-1}{\exp(i\cdot B\cdot x)-1} \frac{\exp(i\cdot B\cdot N_2\cdot y)-1}{\exp(i\cdot B\cdot y)-1} \times \right. \\ \left. \times \frac{\exp(i\cdot B\cdot N_3\cdot (x\cdot (N_1-1)+(1+\sqrt{1-(x^2+y^2)})))-1}{\exp(i\cdot B\cdot (x\cdot (N_1-1)+(1+\sqrt{1-(x^2+y^2)})))-1} \right|^2 \quad (2)$$

где N_1 – число атомов на ступеньке вдоль оси X, N_2 – число атомов на ступеньке вдоль оси Y, N_3 – число ступене, $\vec{G}((N-1)\cdot a,0,-a)$ – вектор межступенчатого рассеяния, $x = \sin\vartheta\cdot\cos\varphi$, $y = \sin\vartheta\cdot\sin\varphi$, $B = 2\pi\cdot a/\lambda$.



панорама вид со стороны оси X вид сверху

Рис. 3. Дифракционная картина от ступенчатой структуры
($N_1 = 5$, $N_2 = 40$, $N_3 = 10$, $a = 3Å$)

Основная особенность на картинах дифракции от ступенчатых структур – это появление раздвоенных рефлексов. Для строгого периодичных дефектных структур угловые положения этих раздвоений обладают определенной симметрией, которая изменяется в зависимости от *Ep* – длины волны λ. Другой особенностью, вытекающей из первой, является значительная вариация интенсивности рефлексов в зависимости от λ.

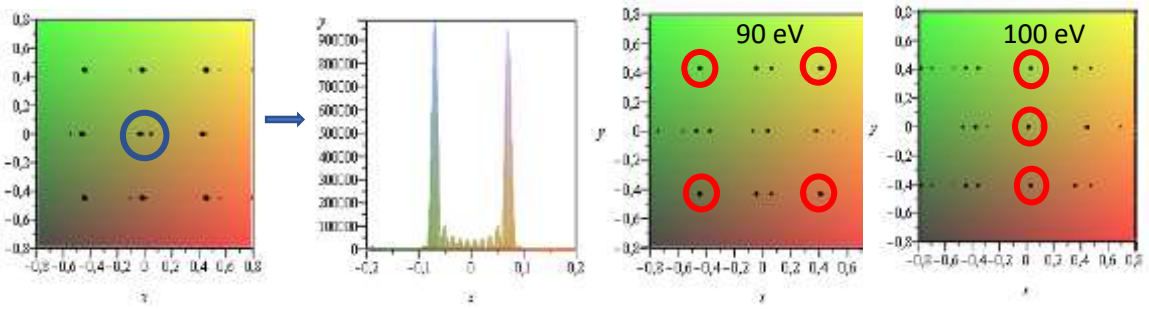


Рис. 4. Раздвоение рефлексов на дифракционных картинах
(N_1 = 5, N_2 =40, N_3 = 10, a = 3$Å$)
слева синий кружок – раздвоенный (00) рефлекс,
справа красные кружки – «одиночные» рефлексы

Перекачка интенсивности в раздвоенном (00) рефлексе

При рассеянии электронной волны на идеальной двумерной структуре (00) рефлекс имеет постоянную интенсивность и не меняет своего углового положения при изменении λ.

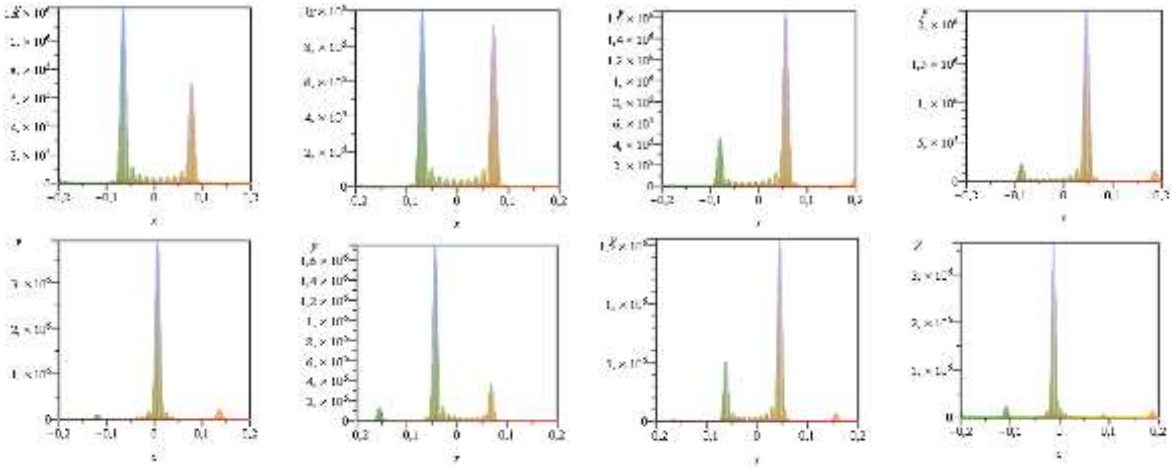


Рис. 5. Динамика раздвоения рефлексов на дифракционных картинах в зависимости от *Ep* (длины электронной волны) (N_1 = 5, N_2 = 40, N_3 = 10, a = 3Å)

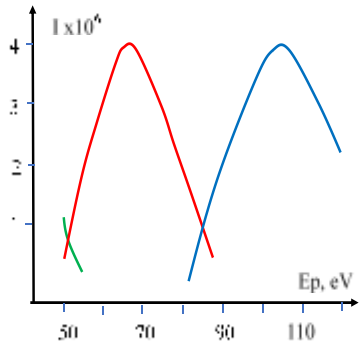


Рис. 6. Зависимость *I*(*Ep*)

Верхний ряд. *Ep* 50→ 56 эВ. Происходит перекачка интенсивности от левого максимума к правому. Вся дифракционная картина смещается влево. Нижний ряд. *Ep* 50→ 56 эВ. Правый рефлекс смещается в положение x = 0, достигая максимума интенсивности. Левый рефлекс исчезает полностью. С увеличением *Ep* правый рефлекс продолжает смещаться влево, теряя интенсивность. Появляется новый максимум справа,

который набирает интенсивность с увеличением *Ep*. При дальнейшем увеличении Ep появляется новый рефлекс.

Предыдущие графики имеют разный масштаб по шкале интенсивности. На рис. 6 энергетическая зависимость интенсивности право/левых рефлексов имеет одинаковый масштаб.

Зависимость величины расщепления (00) рефлекса от глубины ступенек b

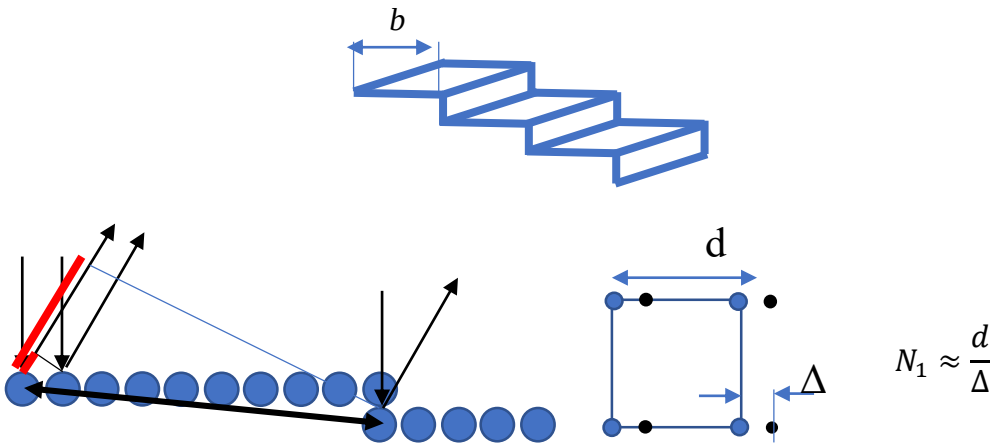


Рис. 7. *d* – расстояние между Брегговскими мах, Δ – между расщепленными мах

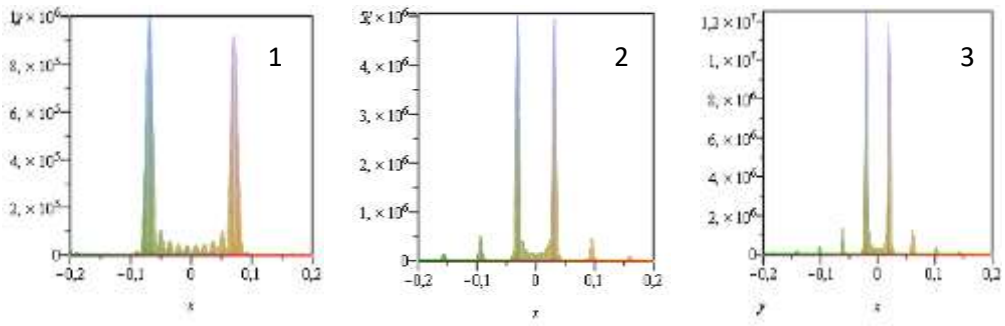


Рис. 8. Зависимость величины расщепления (00) рефлекса от глубины тупенек *b* *1* – N_1 = 5, *2* – N_2 = 10, *3* – N_3 = 15

Отношение расстояния между основными и расщепленными рефлексами определяет глубину ступеньки.

Другая форма ступенчатых структур

$$I = \left| \frac{\exp(i \cdot B \cdot N_1 \cdot x) - 1}{\exp(i \cdot B \cdot x) - 1} \frac{\exp(i \cdot B \cdot N_2 \cdot y) - 1}{\exp(i \cdot B \cdot y) - 1} (1 + \exp(i \cdot B \cdot (x \cdot (N_1 - 1) + (1 + \sqrt{1 - (x^2 + y^2)}))) \right|^2$$

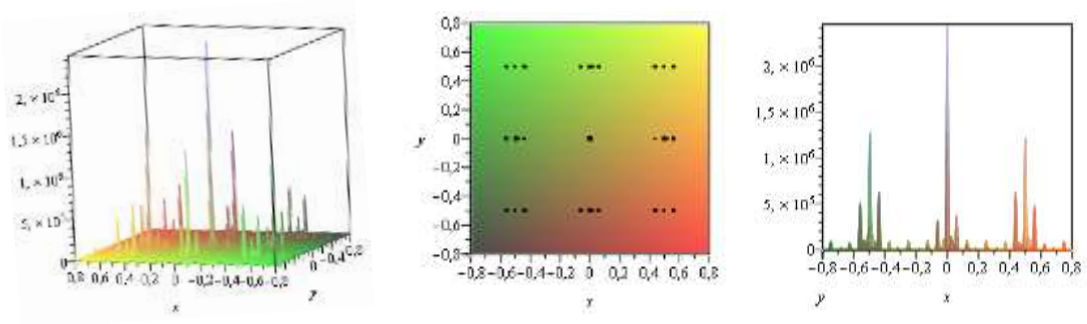


Рис. 9. Дифракционная картина от ступенчатой структуры (5×40, M = 4, 100 эВ)

Степень самоорганизации ступенчатых дефектных структур и форма рефлексов на картинах ДМЭ

Рис. 10. Профили рефлексов

На рис. 10 представлен вид дифракционных картин при различной степени упорядочения поверхностных структур: *a* – самоорганизация на макроуровне – одинаковые по размерам ступеньки, ориентированные в одинаковом направлении, *b* – ориентированные в одинаковом направлении, но разные по глубине ступеньки *c* – разные по глубине ступеньки с небольшой разориентацией по направлению.

Основные особенности дифракции на ступенчатых структурах на начальных стадиях упорядочения поверхностной структуры – это разнообразие формы и интенсивности рефлексов, а на упорядоченных – чередование раздвоенных и одиночных дифракционных максимумов.

Список используемых источников

1. Henzler M. Studies of Surface Imperfections // *Appl. Surf. Sci*. 1982 V. 11/12. pp. 450–469.

2. Saxena A., Ala-Nissilä T., Gunton J. D. Structural phase transitions on stepped surfaces // Surf. Sci. 1986 V. 169 P. L231-L236

3. Bardi U., Santucci A., Rovida G., Ross P. N. LEED study of the Pt3Ti(510) stepped single crystal surface // Proceedings of the 2nd International Conference on the Structure of Surfaces (ICSOS II), Amsterdam, The Netherlands, June 22–25, 1987. pp. 147–151.

4. Hoffmann W., Benndorf C. Water adsorption structures on flat and stepped Ru(0001) surfaces // Journal of Vacuum Science & Technology. 2000. V. 18. pp. 1520.

5. Besocke K., Wagner H. LEED studies on stepped W surfaces // Surf. Sci. 1975. V. 52. pp. 653–663.
6. Савельев И.В. Курс общей физики: в 3-х т. М.: Наука, 1987. Т. 3. 532 с.

УДК 621.372
ГРНТИ 47.45.33

ИСПОЛЬЗОВАНИЕ УСЕЧЁННЫХ ОБЪЁМОВ В КАЧЕСТВЕ МИКРОВОЛНОВЫХ РЕЗОНАТОРОВ

Е. А. Коновалова, В. И. Мотренко, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе показаны этапы исследования усечённых резонаторов: полусферического, полуцилиндрического, полусфероидного. Для этих структур производится сравнительный анализ добротностей, приводится экспериментальное подтверждение их работоспособности. Наиболее подробно описывается резонатор в виде сплюснутого полусфероида, так как его исследование является логическим завершением ряда работ.

СВЧ резонатор, полурезонатор, усечённый резонатор, микроволновый генератор.

Как известно, в технике СВЧ широко применяются полые резонаторы взамен колебательных контуров с сосредоточенными параметрами, т.к. добротность последних уменьшается с повышением частоты. Классические объёмные резонаторы, такие как цилиндрический или сферический, уже давно известны и рассчитаны, усечёнными же вариантами этих объёмов никто не занимался, хотя они обладают некоторыми полезными особенностями. Например, уменьшение объёма в два раза приводит к снижению добротности на величину менее двух раз, а также к более экономному использованию материала. Кроме того, усечённые резонаторы гораздо удобнее интегрировать на платы.

В СПбГУТ на протяжении последних лет были исследованы следующие виды усечённых резонаторов (рис. 1).

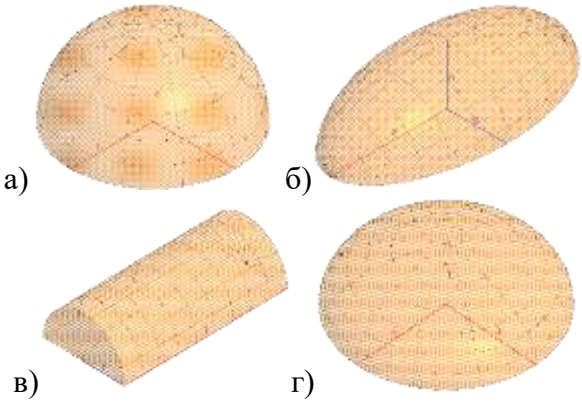


Рис. 1. Усечённые резонаторы:
а – полусфера; б – вытянутый полусфероид;
в – полуцилиндр; г – сплюснутый полусфероид

Исследование усечённых резонаторов начиналось с полусферы (рис. 1а), поэтому и рассмотрим сначала её. На рис. 2 представлено сравнение добротностей сферы и полусферы. Ключевой особенностью данного типа резонаторов является то, что отношение их добротностей всегда составляет полтора раза.

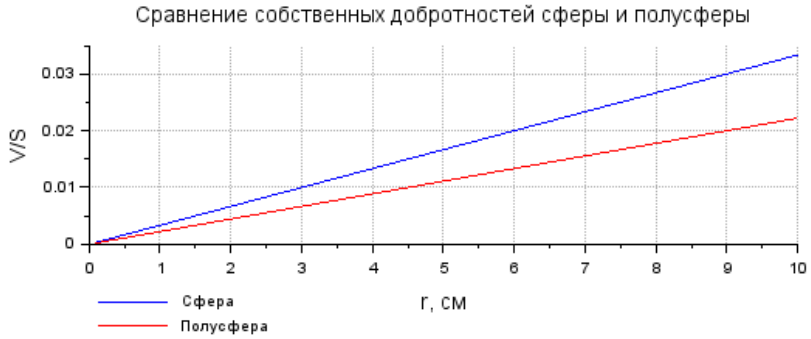


Рис. 2. Сравнение добротностей сферы и полусферы

Сравнение добротностей здесь и далее производится в первом приближении формулы (1) [1], то есть как отношение объёма к площади.

$$Q = \frac{2}{\delta} * \frac{V}{S}, \quad (1)$$

где V – объём, S – площадь внутренней поверхности, δ – толщина скин-слоя.

Изучение данной тематики началось с работ [2] и [3]. В них подтверждается то, что полусфера является резонансной структурой. Также с использованием полусферических резонаторов были изготовлены генератор и режекторный фильтр с ослаблением в полосе запирания более 40 дБ.

Исследование полусферы было продолжено работой [4]. В ней предложена, рассчитана и экспериментально проверена эквивалентная проволочная модель полусферического резонатора (рис. 3 слева). Также был изготовлен генератор с использованием этой модели, его спектрограмма представлена справа на рис. 3.

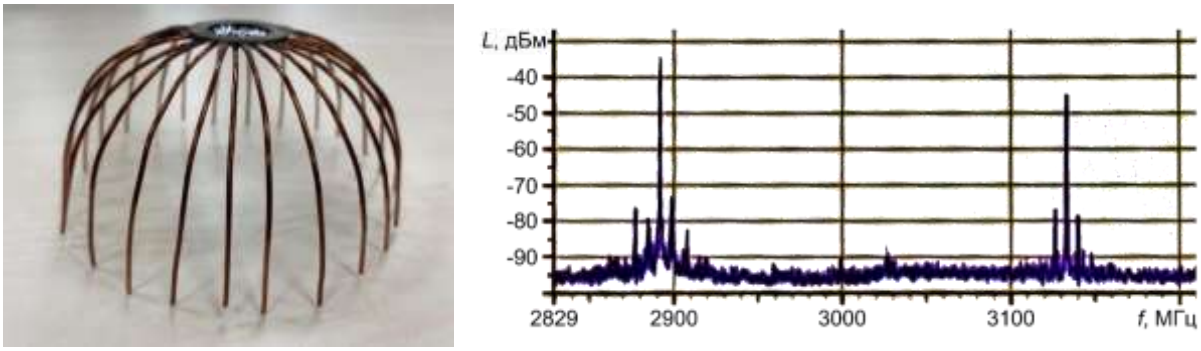


Рис. 3. Проволочный макет полусферического резонатора (слева)
и спектрограмма генератора на его основе (справа)

Исторически следующим стал резонатор в форме вытянутого сфероида (рис. 1б). На рис. 4 представлено аналогичное сравнение добротностей для вытянутых сфероида и полусфероида. Из особенностей можно отметить, что разница между этими фигурами стремится к значению 1,65.

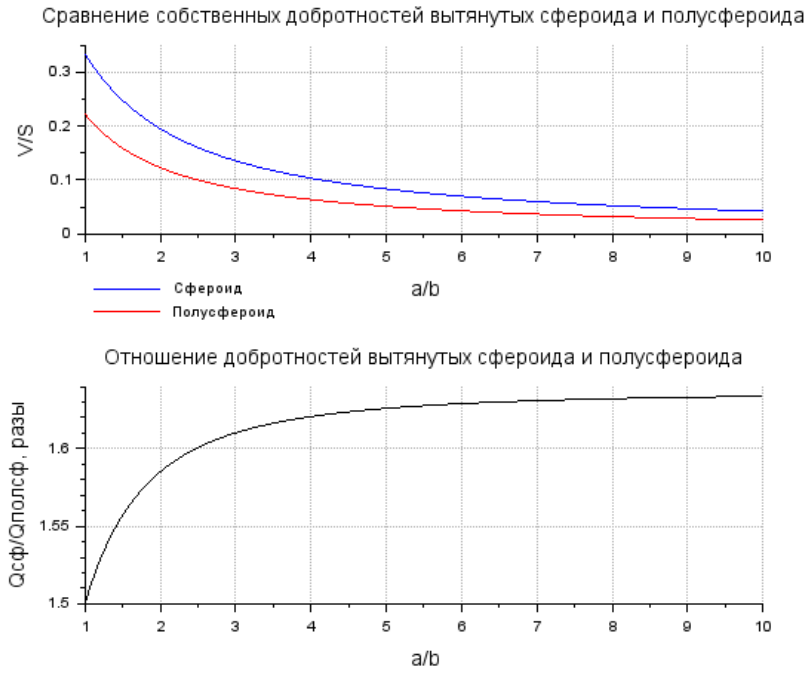


Рис. 4. Сравнение добротностей вытянутых сфероида и полусфероида

Вытянутый полусфероид описывается в работе [5]. С использованием этого резонатора был изготовлен генератор СВЧ колебаний (рис. 5 слева), частотная характеристика которого показана справа на рис. 5.

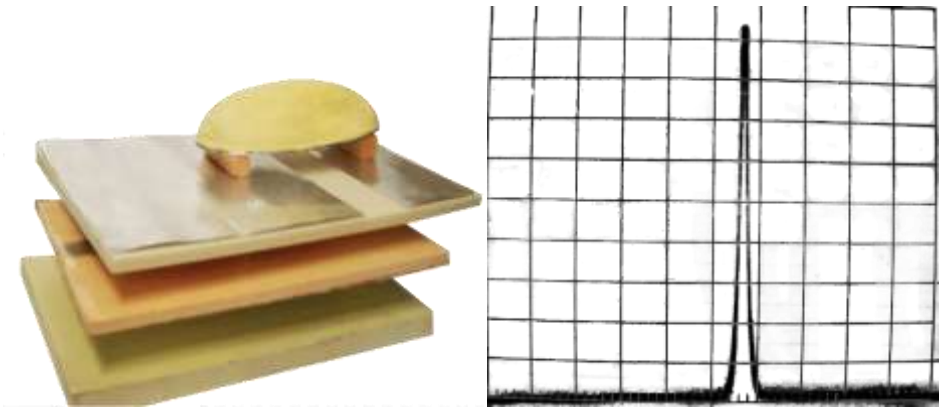


Рис. 5. Макет генератора с резонатором в виде вытянутого полусфероида (слева) и характеристика этого генератора (справа)

Далее идёт полуцилиндрический резонатор (рис. 1в). Как и в предыдущих случаях, сравнение его добротности с цилиндрическим резонатором показано на рис. 6.

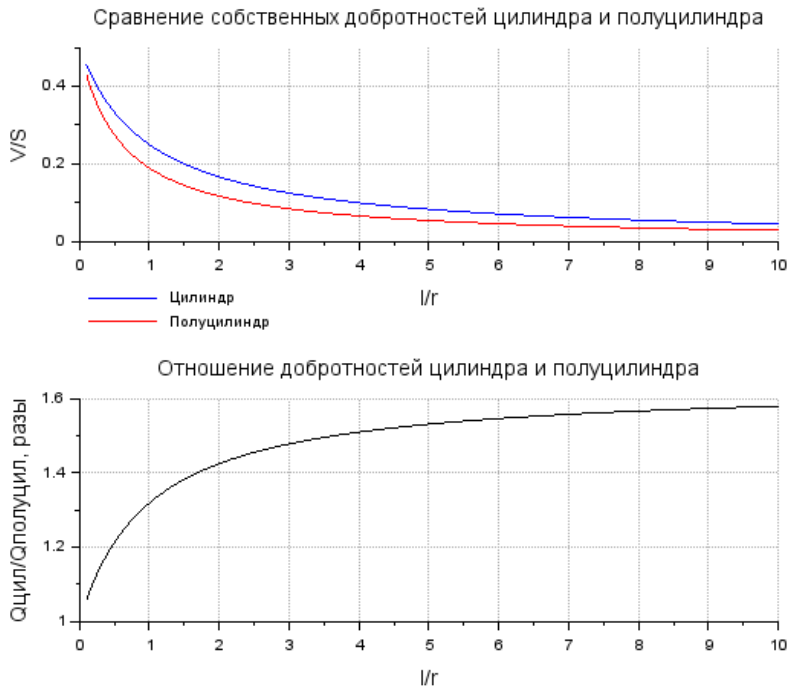


Рис. 6. Сравнение добротностей цилиндра и полуцилиндра

Он интересен следующим: если соотношении длины к радиусу составляет менее 3,5, то разница добротностей с полной фигурой составляет менее полутора раз. Также при дальнейшем увеличении этого отношения разрыв стремится к значению 1,65.

Полуцилиндрический резонатор частично рассмотрен в работе [6]. Для данной структуры было проведено электродинамическое моделирование, экспериментально подтверждены резонансные свойства, а также создан генератор, спектрограмму которого можно увидеть ниже (рис. 7).

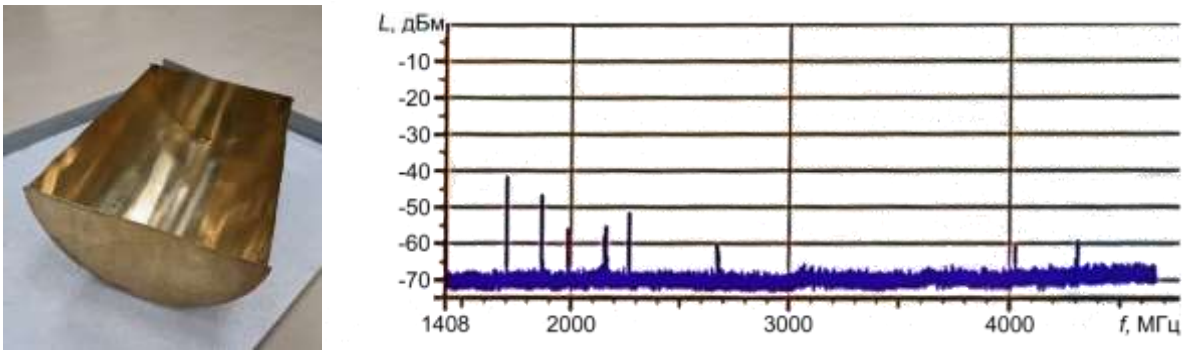


Рис. 7. Макет полуцилиндрического резонатора (слева)
и спектральная характеристика генератора на его основе (справа)

На завершающем этапе авторами работы исследовался резонатор в виде сплюснутого полусфероида (рис. 1г). И чем более он сплюснут, тем меньше эффективность его использования по отношению к полной фигуре с точки зрения добротности, что видно из рис. 8.

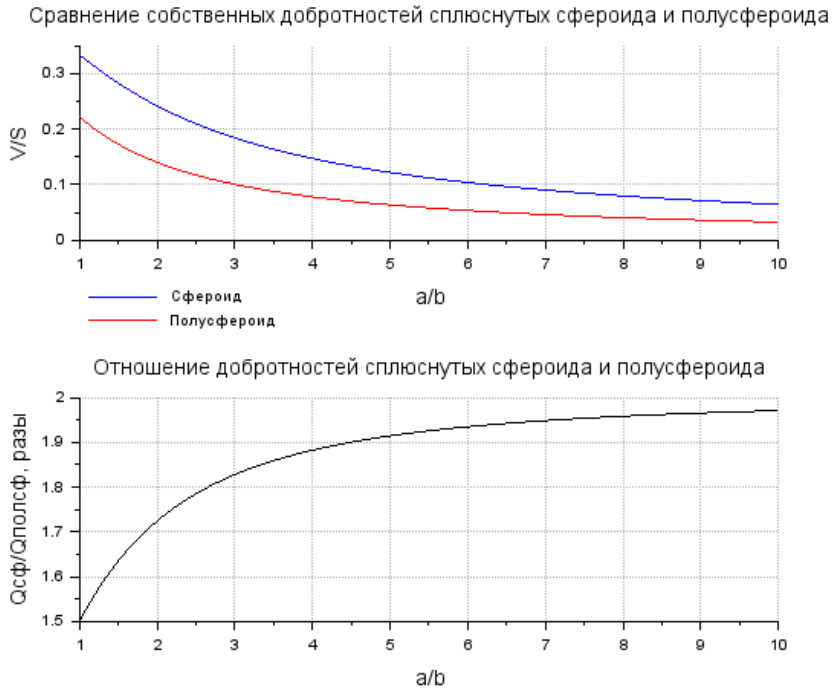


Рис. 8. Сравнение добротностей сплюснутых сфероида и полусфероида

Как и в случае с полуцилиндром, было проведено электродинамическое моделирование данной структуры (рис. 9), которое подтвердило резонансные характеристики. Расчётная частота первого резонанса составляет 3,55 ГГц.

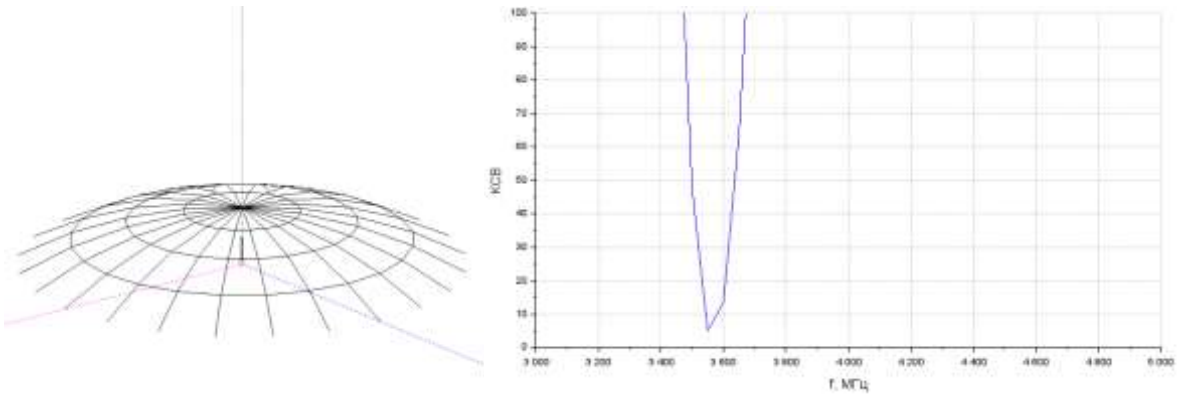


Рис. 9. Эквивалентная проволочная модель в *MMANA-GAL* (слева)
и результаты моделирования (справа)

По результатам моделирования был изготовлен генератор (рис. 10) на основе сплюснутого полусфероидного резонатора и активного двухполюсника. Спектральная характеристика этого генератора показана в правой части рис. 10. Резонансная частота первой моды составляет 4 ГГц. Сдвиг экспериментальной резонансной частоты вправо относительно теоретической объясняется тем, что геометрические параметры макета отличаются от компьютерной модели в меньшую сторону.

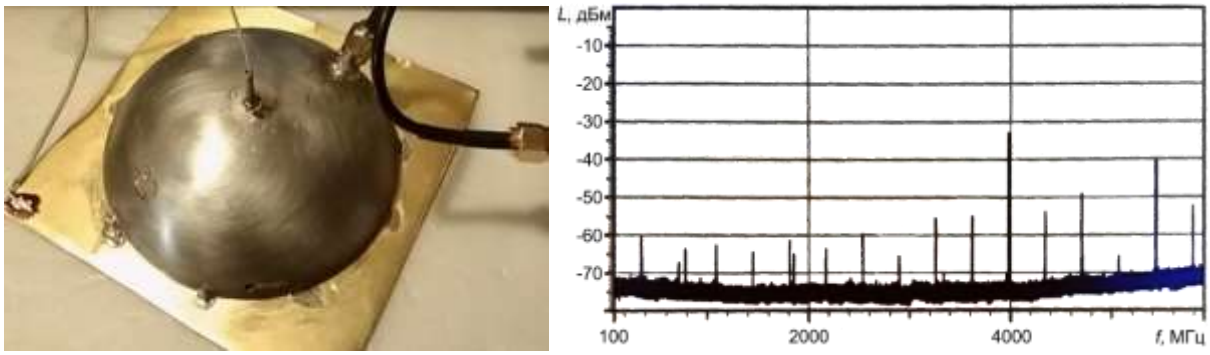


Рис. 10. Генератор с резонатором в виде сплюснутого полусфероида (слева)
и его спектральная характеристика (справа)

У всех видов усечённых резонаторов – полусферы, вытянутого и сплюснутого полусфероидов, полуцилиндра – экспериментально подтверждены резонансные свойства.

В качестве усечённых могут выступать и диэлектрические резонаторы, что значительно расширяет области применения данной серии работ, в том числе и на монолитные интегральные схемы.

Замена классических резонаторов на усечённые в некоторых случаях позволит повысить добротность. Например, использование полусферического диэлектрического резонатора вместо диэлектрических цилиндров (шайб). Отметим, что *современные* технологии позволяют изготавливать усеченные резонаторы без каких-либо затруднений.

Список используемых источников

1. Лебедев И. В. Техника и приборы СВЧ / под ред. академика Н. Д. Девяткова. М.: «Высш. школа», 1970. 440 с.

2. Захаров А. Н. Высокостабильный генератор СВЧ на сфероидальном объёме // XII Всероссийская научная конференция студентов-радиофизиков: Тез. докл., СПб, 2-3 дек. 2008 г. СПб.: Изд-во Политехн. ун-та, 2008. С. 20–22.

3. Сайко Н. Ю. Исследование полого сферического резонатора // XII Всероссийская научная конференция студентов-радиофизиков: Тез. докл., СПб, 2-3 дек. 2008 г. СПб.: Изд-во Политехн. ун-та, 2008. С. 62–64.

4. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. Микроволновый генератор на полусфере // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 457–461.

5. Иванов М. Ю. Генератор СВЧ на объёмном резонаторе в гибридно-интегральном многослойном исполнении // XIV Всероссийская научная конференция студентов-радиофизиков: Тез. докл., СПб, 7-8 дек. 2010 г. СПб.: Изд-во «Соло», 2010. С. 45–47.

6. Мотренко В. И., Седышев Э. Ю. Определение точки включения диода в полуцилиндрическом резонаторе с помощью электродинамического моделирования // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): сборник лучших докладов конф. СПб.: СПбГУТ, 2022. С. 114–118.

УДК 53.082.54
ГРНТИ 29.31.29

ЧУВСТВИТЕЛЬНОСТЬ ИНТЕРФЕРОМЕТРИЧЕСКОЙ СХЕМЫ РЕГИСТРАЦИИ КОЛЕБАНИЙ ПРЕЦИЗИОННЫХ КВАРЦЕВЫХ РЕЗОНАТОРОВ

Е. В. Кравец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с невозможностью строгого аналитического описания процесса колебаний при разработке прецизионных кварцевых резонаторов в последние годы исследуются оптические методы контроля динамического амплитудного распределения на поверхности кристалла. Амплитуды колебаний прецизионных резонаторов составляют от единиц до десятков ангстрем. Рассматривается схема измерительного устройства на основе интерферометра Майкельсона, проводится анализ его параметров. Для оценки чувствительности проводится учет влияния параметров оптической схемы на интерференционную картину и шумов на работу устройства. Оценивается возможный амплитудный диапазон измерений.

кварцевый резонатор, интерферометр, чувствительность.

В работах [1, 2] для измерения распределения амплитуд по поверхности кварцевого резонатора предложена оптическая схема на основе интерферометра Майкельсона (рис. 1).

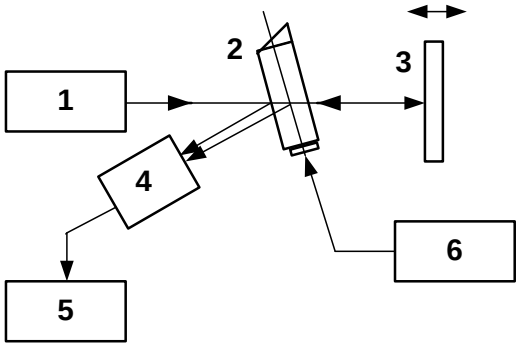


Рис. 1. Схема интерферометра с акустооптическим модулятором:
1 – лазер, *2* – акустооптический модулятор, *3* – кварцевый резонатор,
4 – фотоприемник, *5* – блок обработки, *6* – генератор

Обозначив выходную мощность лазера *W*, мгновенное значение мощности на фотоприемнике определяется разностью фаз φ между опорным и предметным лучами в устройстве [1–3]:

$$W_{\Sigma}(t) = W\left(\alpha_1 + \alpha_2 + 2\sqrt{\alpha_1 \cdot \alpha_2} \cdot \cos(\omega_A t + m \cdot \cos\Omega t + \varphi)\right), \qquad (1)$$

где ω_A – частота ультразвуковой волны в акустооптическом модуляторе, $m = (4\pi A/\lambda)$ – индекс фазовой модуляции света, A – амплитуда и Ω – частота колебаний кварцевого резонатора, φ – фазовый сдвиг, α_1, α_2 – энергетические коэффициенты пропускания оптической системы.

Оптический сигнал состоит из двух компонент, одна из которых формируется путем отражения от грани акустооптического модулятора *2* (рис. 1):

$$\alpha_1 = \left(\frac{n-1}{n+1}\right)^2.$$

Вторая компонента формируется за счет прохождения сквозь акустооптический модулятор *2*, отражения от вибрирующей поверхности кварцевого резонатора *3* (рис. 1) и дифракции в модуляторе:

$$\alpha_2 = \left[1 - \left(\frac{n-1}{n+1}\right)^2\right]^4 \cdot \eta \cdot R_{Au},$$

где n – показатель преломления материала акустооптического модулятора (TeO_2), η – эффективность акустооптического взаимодействия (в зависимости от уровня управляющего сигнала в модуляторе η = 0,4–0,8).

Наглядно результат интерференции (1) проявляется в том случае, когда интенсивность волн, определяемых коэффициентами α_1 и α_2 одинакова. Дисперсия показателя преломления материала акустооптического модулятора TeO_2 в диапазоне от 480 до 1 150 нм меняется незначительно, однако коэффициент отражения R_{Au} от поверхности кварцевого резонатора имеет значение < 0,4 в диапазоне до 500 нм [4, 5]. С учетом дисперсии и спектрального коэффициента отражения для источника с длиной волны 650 нм коэффициенты интенсивности опорного и предметного луча составляют соответственно $\alpha_1 = 0{,}15$, $\alpha_2 = 0{,}16$.

В работе [1] экспериментально показано, что индекс фазовой модуляции для интерферометрической схемы $m<<1$. Это позволяет применить при обработке, принимаемого фотоприемником сигнала, узкополосный перестраиваемый фильтр для выделения амплитуд несущей и первой гармоники спектра сигнала с последующим вычислением их отношения.

Компоненты тока фотодиода можно представить суммой гармоник [6]:

$$i(t) = i_T + i_N(t) + \gamma \cdot W_\Sigma(t), \qquad (2)$$

где i_T – темновой ток, i_N – шумовая составляющая тока, которая представляет стационарный гауссовский случайный процесс с дисперсией $G(f)$, γ – спектральная чувствительность фотодиода.

Постоянная составляющая тока фотодиода информационного значения не имеет, но влияет на величину шумового тока приемника:

$$i_{=} = i_{\text{Т}} + \gamma \cdot W \cdot (\alpha_1 + \alpha_2).$$

Амплитуды нулевой (несущей) и первой гармоники (с частотой $\omega_A \pm \Omega$) интермодуляционной составляющей (2) равны соответственно:

$$i_0 = 2 \cdot \gamma \cdot W \cdot \sqrt{\alpha_1 \cdot \alpha_2} \cdot J_0(m),$$
$$i_1 = 2 \cdot \gamma \cdot W \cdot \sqrt{\alpha_1 \cdot \alpha_2} \cdot J_1(m).$$

Используя разложения в ряд функций Бесселя для малых значений индекса модуляции m, мощность нулевой гармоники сигнала на нагрузке фотодиода может быть выражена как:

$$W_0 = \frac{i_0^{\,2}}{2} \cdot R_0 \cdot p = 2 \cdot \gamma^2 \cdot W^2 \cdot \alpha_1 \cdot \alpha_2 \cdot \left(1 - \frac{m^2}{2}\right) \cdot R_0 \cdot p.$$

Для первой гармоники сигнала мощность на нагрузке фотодиода определяется выражением:

$$W_1 = 0,5 \cdot \gamma^2 \cdot W^2 \cdot \alpha_1 \cdot \alpha_2 \cdot m^2 \cdot \left(1 - \frac{m^2}{4}\right) \cdot R_0 \cdot p. \quad (3)$$

где p – коэффициент передачи мощности от фотодиода в нагрузку, $p \le 1/4$.

Потенциальная чувствительность ограничена принципиально неустранимыми источниками помех: тепловым (джонсовским) шумом, дробовым шумом и фликкер-шумом. Рассмотрим влияние основных шумов, к которым относятся собственные шумы лазера и шумы приемного устройства.

В этом случае шумовая составляющая тока представляет стационарный гауссовский случайный процесс, который характеризуется дисперсией [6, 7]:

$$G(f) = 4kTR_0^{-1} + i_{=} \cdot \left(2q + af^{-1}\right) + i_{=}^{2} \cdot RIN\,, \quad (4)$$

где q – заряд электрона, a – коэффициент фликкер-шума зависящий от типа фотодиода, RIN – относительная интенсивность шума, создаваемого лазером в полосе частот 1 Гц.

Мощность шума, определяемая шумовой составляющей тока в полосе пропускания тракта обработки сигнала Δf с центральной частотой f_A, в соответствии с выражением (4):

$$W_N(f) = \Delta f \cdot p \cdot R_0 \left\{ 4kTR_0^{-1} + i_{=} \cdot \left(2q + \frac{a}{f_A}\left(1 + \frac{1}{4} \cdot \frac{\Delta f}{f_A}\right)\right) + i_{=}^{2} \cdot RIN \right\}.$$

Отношение сигнал–шум на выходе линейной части устройства обработки для нулевой гармоники сигнала с учетом коэффициента шума N:

$$SNR_0 = \frac{2 \cdot \gamma^2 \cdot W^2 \cdot \alpha_1 \cdot \alpha_2 \cdot \left(1 - \frac{m^2}{2}\right) \cdot R_0}{\Delta f \cdot \left\{ 4kTN + i_{=} \cdot R_0 \cdot \left(2q + \frac{a}{f_A}\left(1 + \frac{1}{4}\frac{\Delta f}{f_A}\right)\right) + i_{=}^{2} \cdot R_0 \cdot RIN \right\}}$$

Для первой гармоники сигнала отношение сигнал-шум составляет:

$$SNR_1 = \frac{\gamma^2 \cdot W^2 \cdot \alpha_1 \cdot \alpha_2 \cdot \frac{m^2}{2} \cdot \left(1 - \frac{m^2}{4}\right) \cdot R_0}{\Delta f \cdot \left\{ 4kTN + i_{=} \cdot R_0 \cdot \left(2q + \frac{a}{f_A}\left(1 + \frac{1}{4}\frac{\Delta f}{f_A}\right)\right) + i_{=}^{2} \cdot R_0 \cdot RIN \right\}}.$$

Для расчёта числовых характеристик примем следующие значения: лазер с длиной волны λ= 0,65 мкм, выходной мощностью W = 5 мВт, R_0 = 1 кОм, N = 10 дБ, p = 0,25, γ = 0,6 А/Вт, RIN = 10^{-15} Гц$^{-1}$; акустооптический модулятор с частотой сигнала f_A = 50 МГц, полоса пропускания тракта обработки – Δf = 50 Гц.

Значение $SNR_1 \geq 10$ обеспечивается при индексе фазовой модуляции $m \geq 2{,}5 \cdot 10^{-6}$ и соответствует амплитуде колебаний А = $1{,}3 \cdot 10^{-13}$ м. При этом мощность шумов в полосе составляет W_N=$1{,}6 \cdot 10^{-17}$ Вт, мощность несущей W_0 = $1 \cdot 10^{-4}$ Вт, мощность первой гармоники сигнала W_1 = $1{,}6 \cdot 10^{-16}$ Вт.

Зависимость минимально определяемой амплитуды колебаний кварцевого резонатора в зависимости от мощности лазера при различных значениях отношения сигнал шум представлена на рис. 2.

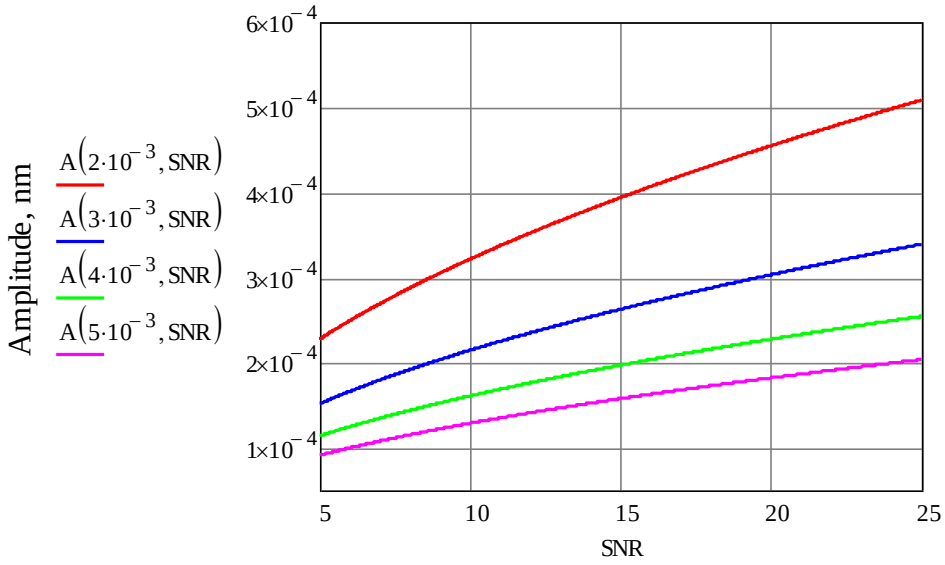


Рис. 2. Зависимость минимально определяемой амплитуды колебания от мощности лазера и отношения сигнал-шум

Представленные результаты позволяют сделать вывод, что чувствительность будет определяться не шумами лазера и фотоприемника, а параметрами анализатора спектра. В этом случае минимальный уровень мощности первой гармоники сигнала $W_1 \geq -120$ дБм. В соответствии с выражением (3) это позволяет определить минимальный индекс модуляции m = $6{,}1 \cdot 10^{-6}$ и амплитуду колебаний кварцевого резонатора A = $3{,}15 \cdot 10^{-13}$ м.

Список используемых источников

1. Вороховский Я. Л., Молоток В. В., Клудзин В. В., Пресленев Л. Н. Измерение амплитуды упругих смещений кварцевого резонатора // Информационно-управляющие системы. 2009. № 6. С. 63–66.

2. Протопопов В. В. Лазерное гетеродинирование / Под ред. Н. Д. Устинова. М.: Наука, 1985. 288 с.

3. Whitman R. L., Laub L. J., Bates W. J. Acoustic surface displacements on a wedge-shaped transducer using an optical probe technique. IEEE Transactions on Sonics and ultrasonics. 1968. Vol. 15. pp. 186–189.

4. Блистанов А. А., Бондаренко В. С., Переломова Н. В. Акустические кристаллы. Справочник. М.: Наука, 1982. 632 с.

5. Оптические постоянные природных и технических сред: справочник / В. М. Золотарев, В. Н. Морозов, Е. В. Смирнова. Л.: Химия. Ленинградское отделение, 1984. 214 с.

6. Розеншер Э., Винтер Б. Оптоэлектроника. М.: Техносфера, 2004. 592 с.

7. Бланк Т. В, Гольтберг Ю. А. Полупроводниковые преобразователи для ультрафиолетовой области спектра // Физика и техника полупроводников. 2003. Том 37. вып. 9. С. 1025–1056.

УДК 621.373.1
ГРНТИ 47.45.00

ГЕНЕРАТОР С УПРАВЛЯЕМЫМ РЕЗОНАТОРОМ НА ФЕРРОШПИНЕЛИ

А. Э. Ланда, Т. В. Никитина, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе была представлена разработка управляемого генератора на кольцевых резонаторах на подложке из феррошпинели. Предложена конструктивно сложная линия, состоящая из двух разных подложек. Проведен эксперимент с предложенной моделью управляемого генератора.

СВЧ, генератор, кольцевой резонатор, феррошпинель, волновое сопротивление, ферритовая подложка, полосковая линия.

В данной статье исследована возможность создания управляемого кольцевого резонатора с использованием феррошпинели, находящегося под действием магнитного поля.

Условие резонанса в таком резонаторе – в кольце должно укладываться целое число длин волн [1]. Длина кольца (по средней линии) 88 мм, первый резонанс (по предварительным расчетам) находится на частоте 1 400 МГц. Исходя из предположения, что на этой частоте в кольце укладывается одна длина волны, можно определить скорость распространения волны в резонаторе. Формула для расчета длины волны:

$$\lambda = \frac{c}{f_0 * \sqrt{\mu\varepsilon}}, \quad (1)$$

где c – скорость света,

f_0 – частота резонанса,

ε – относительная диэлектрическая проницаемость,

μ – относительная магнитная проницаемость.

Как было указано выше, исходя из предварительных результатов экспериментального исследования, первая резонансная частота кольцевого резонатора составляет около 1.4 ГГц. Если эта частота соответствует первому резонансу, то произведение με примерно равно 5.9.

Сам резонатор имеет сложную структуру. Была предложена линия нестандартной конструкции (рис. 1).

Рис. 1. Структура сложной линии
(*1* – подложка из феррошпинели, *2* – линия, *3* – подложка из прессованного стекла, *4* – металлизация)

Линия создана на диэлектрической подложке, сверху которой размещается ферритовая пластина. Такая конструкция обеспечивает сравнительно простое изготовление линии и в тоже время позволяет менять скорость распространения волны в линии, воздействуя магнитным полем на магнитную проницаемость феррошпинели.

Для проверки возможности управления электрической длиной линии был проведен эксперимент с кольцевым резонатором, в составе генератора. В качестве активного элемента в работе использовался туннельный диод АИ201Б.

В ходе эксперимента была создана объёмная интегральная схема, состоящая из 2 слоев и представленная на рис. 2.

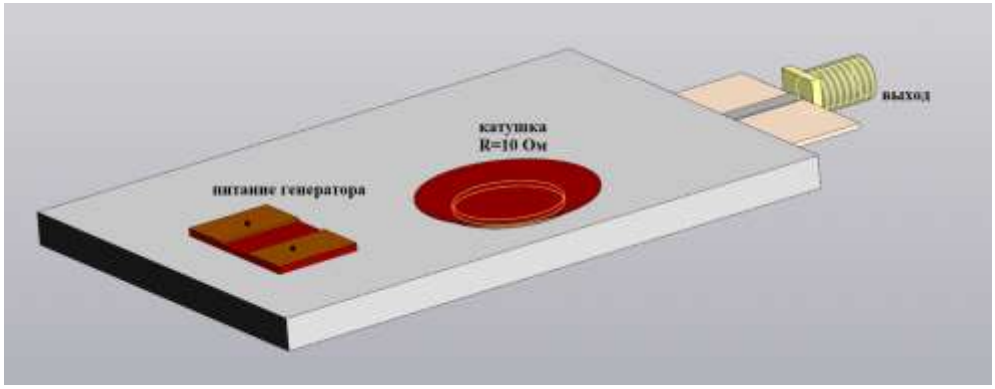


Рис. 2. Генератор с управляемым резонатором на подложке из феррошпинели

Первый слой представляет собой подложку из феррошпинели, плотно прилегающую к кольцевому резонатору.

Второй слой представляет собой кольцевой резонатор на подложке из прессованного стекла, представленный на рис. 3.

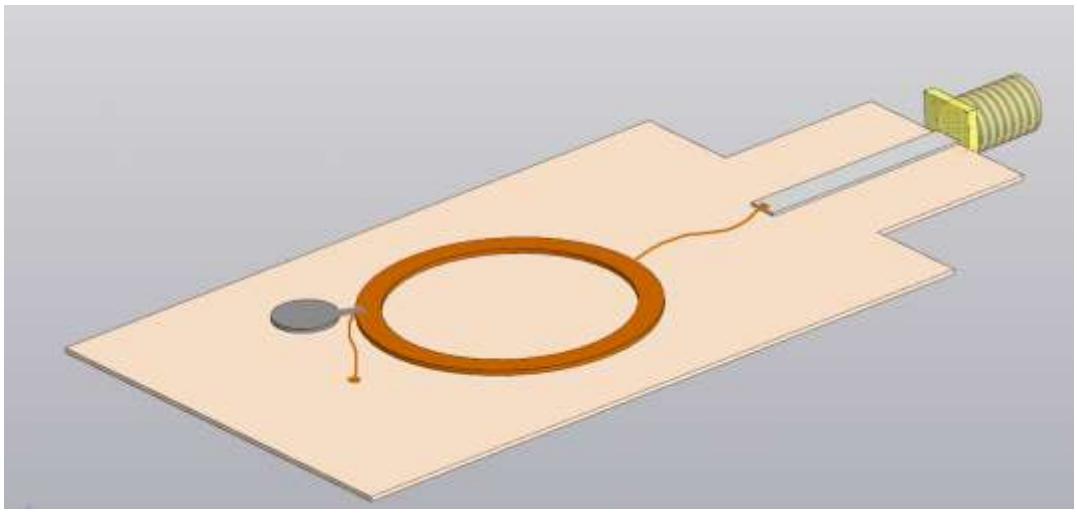


Рис. 3. Нижняя часть ОИС СВЧ

Эксперимент позволил проверить, как влияет магнитное поле на резонансную частоту кольца и соответственно, на частоту генерации сигнала. На спектрограмме видно полученную частоту генерации (рис. 4). Устройство работает на частоте, примерно, равной 1 395 МГц.

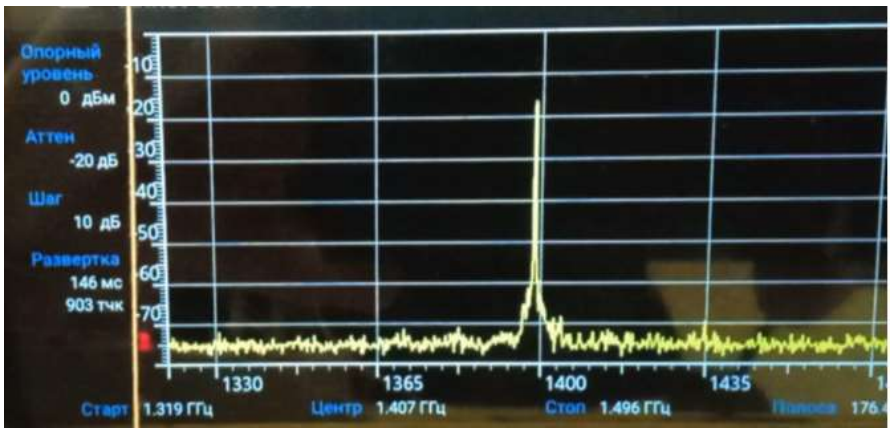


Рис. 4. Спектр сигнала до влияния постоянного магнита

Далее был поднесен никель-кобальтовый магнит к верхней части ОИС. Как видно из спектрограммы, рабочая частота сместилась (рис. 5).

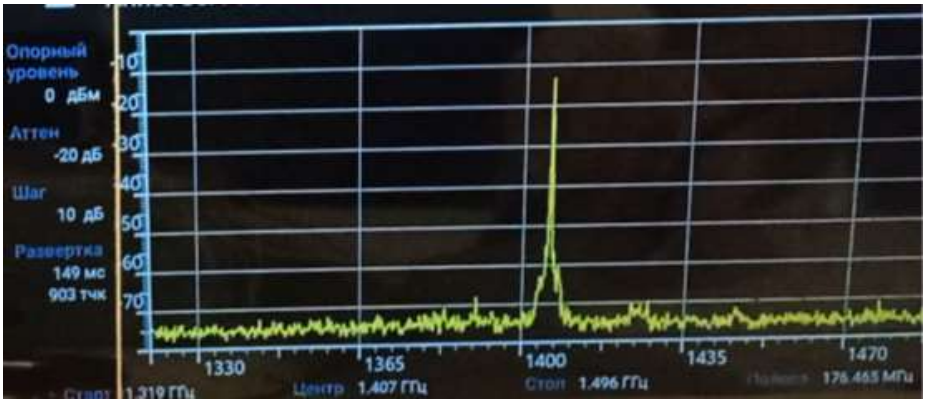


Рис. 5. Спектр сигнала после воздействия постоянного магнита

Эти изменения не значительны, примерно 10–15 МГц, но все равно можно заключить, что постоянное магнитное поле изменило спектр сигнала. Можно сделать вывод, что при изменении постоянного магнитного поля, электрическая длина кольца меняется, вследствие чего и происходит смещение частоты.

Эксперимент доказал, что создание управляемого генератора на управляемом резонаторе на подложке из феррошпинели возможно.

Список используемых источников

1. Семенов Н. А. Техническая электродинамика: учебное пособие для вузов. М.: Связь, 1973. 265 с.

2. Кушнир Ф. В. Электрорадиоизмерения: учебное пособие для вузов. Л.: Энергоатомиздат. Ленингр. отд-е, 1983. 320 с.

УДК 621.373.52
ГРНТИ 47.45.99

ИССЛЕДОВАНИЕ МИКРОВОЛНОВОГО ГЕНЕРАТОРА НА КОЛЬЦЕВОМ РЕЗОНАТОРЕ С УЧЕТОМ ЭКВИВАЛЕНТА АКТИВНОГО ДВУХПОЛЮСНИКА

А. К. Ларионова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе приведены результаты серии экспериментов, целью которых было повышение мощности генератора СВЧ. В качестве активных элементов использовались двухполюсники с отрицательным сопротивлением (туннельные диоды). К сожалению исследуемые макеты генераторов не давали алгебраического сложения уровня мощности при увеличении количества активных элементов, при этом схема с двумя диодами давала заметное увеличение уровня шума. В работе даны объяснения данного эффекта. Сделан вывод о невозможности установки двух диодов параллельно. В качестве альтернативы предложена многослойная конструкция со сложением мощности идентичных генераторов.

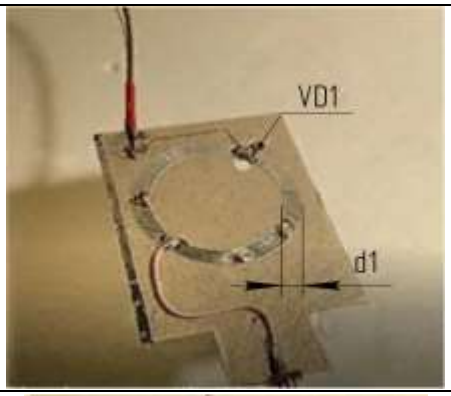
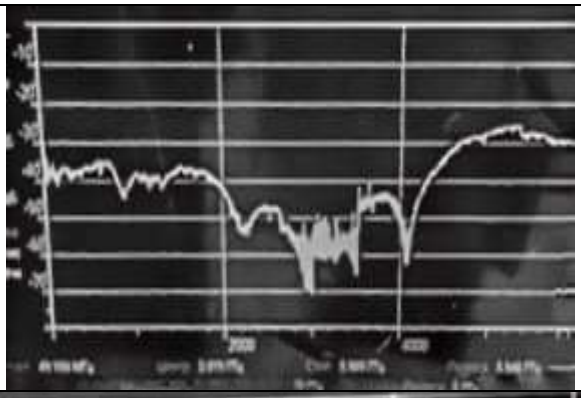
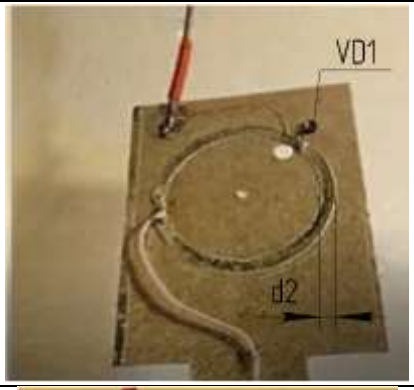
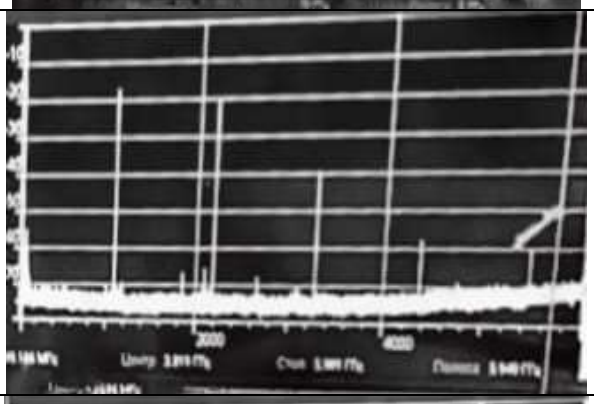
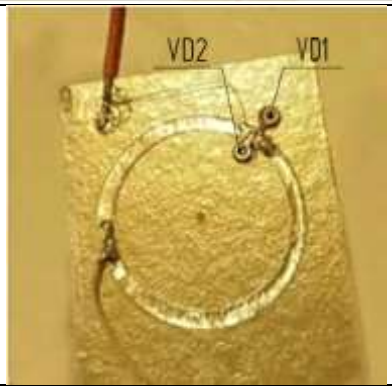
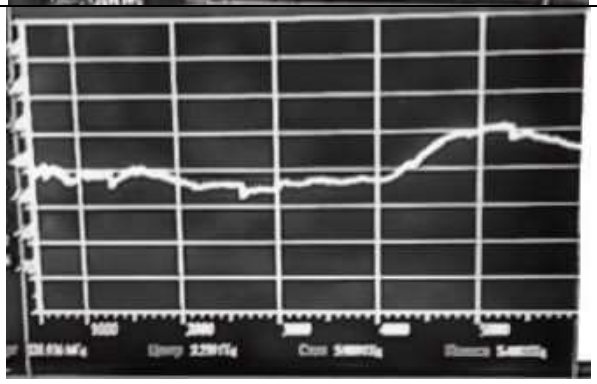
эквивалентная схема, СВЧ, генератор, активный двухполюсник, резонатор, шум.

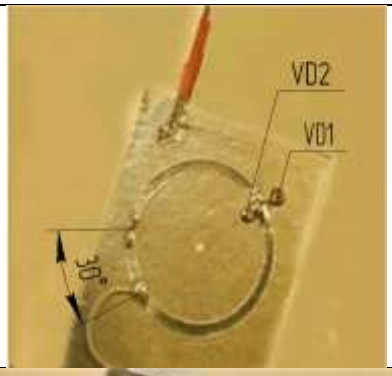
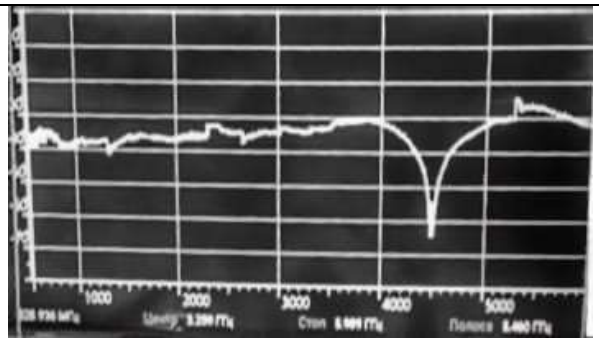
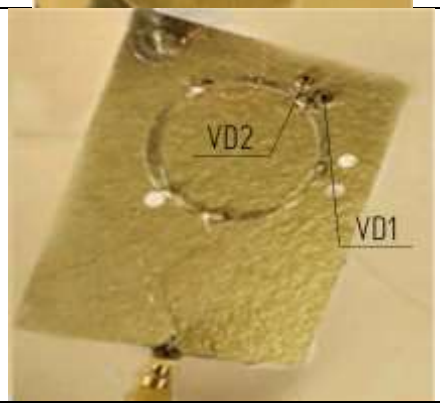
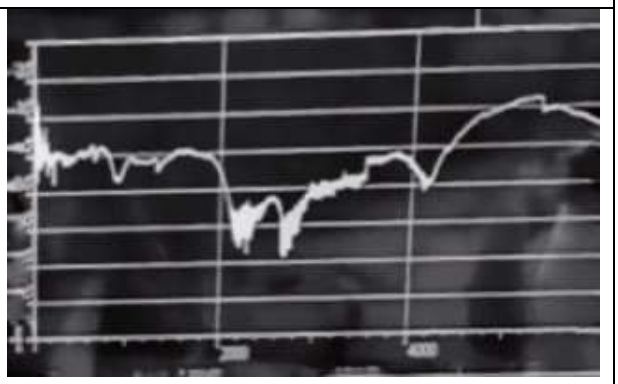
Использование планарных эллиптических кольцевых резонаторов в интегральных схемах (ИС) генерации СВЧ сигнала является актуальным и перспективным направлением развития СВЧ электроники. На сегодняшний день уже известен генератор СВЧ на нескольких активных двухполюсниках, синтезированный в Лаборатории синтеза СВЧ устройств СПбГУТ [1]. Генерационные диоды в данной работе были установлены в шлейфах, которые гальванически были соединены с кольцевым резонатором. Кольцевой резонатор в этой ИС выполнял роль элемента стабилизации и сложения сигнала.

В этой работе мы поставили перед собой следующую задачу: исследовать одновременную работу в генерационной схеме нескольких полупроводниковых диодов с отрицательным сопротивлением, установленных в 1 точку. Один из возможных выигрышей такого включения – повышение мощности генератора. Также мы попытались понять процессы в полупроводнике при синхронной и асинхронной работе p-n – перехода. На настоящий момент поставлено значительное количество экспериментов, которые не дали ожидаемого результата, хотя некоторые варианты включения все же дают незначительное увеличение мощности.

Все исследуемые в этой работе макеты СВЧ генераторов на кольцевых эллиптических резонаторах (КЭР) и их экспериментально полученные характеристики приведены в таблице 1.

ТАБЛИЦА 1. Макеты СВЧ генераторов на КЭР
и их экспериментально полученные характеристики

№ эксперимента	Исследуемый макет СВЧ генератора	Экспериментально полученная характеристика
1		
2		
3		

№ эксперимента	Исследуемый макет СВЧ генератора	Экспериментально полученная характеристика
4		
5		

Для первого эксперимента был создан макет генератора на кольцевом резонаторе с использованием 1-го активного двухполюсника. В данном эксперименте получить ожидаемую генерацию не удалось. В районе 200мВ наша исследуемая модель стала представлять из себя генератор шума, при этом с весьма насыщенной шумовой характеристикой.

Затем (эксперимент № 2), поменяв толщину кольцевого резонатора, тем самым, увеличив волновое сопротивление линии, нам удалось получить довольно устойчивую генерацию. Таким образом, существенную значимость в получении генерации представляет волновое сопротивление кольца, которое напрямую связано с добротностью.

В эксперименте № 3 была предпринята попытка подключения 2-х активных двухполюсников в 1 точку, для того чтобы получить повышенную мощность генератора. Однако, к сожалению, генерацию получить не удалось. Необходимо отметить то, что генератор «чувствует» 2 диода. О данном факте свидетельствует уровень шума −20 дБм, который генерируется в диапазоне 0….6 ГГц. Такая модель может найти применение при синтезе генераторов шума.

Следующим шагом мы поменяли схему включения нагрузки (эксперимент № 4), переместив точку подключения примерно на 30°. Модель, как и в предшествующем эксперименте, представляла собой «умощенный» генератор шума. Следовательно два диода не могут работать синхронно, либо

для этого режима необходимы какие-то специальные характеристики резонатора.

В заключительном эксперименте № 5 была изменена схема подключения самих активных двухполюсников (между диодами сделан небольшой разнос по геометрии). Однако параллельно включенные туннельные диоды через микролинию не изменили общую картину, и устройство все так же представляло собой генератор умощенного шума.

Таким образом, параллельное подключение 2-х диодов в 1 точку не дает прогнозируемого увеличения мощности СВЧ генератора. По какой причине диоды ведут себя подобным образом точно не ясно. Было сделано предположение о том, что проблема заключена в самих двухполюсниках. Для того, чтобы объяснить природу асинхронной работы диодов, необходимо провести компьютерное моделирование реального макета в RFSim99 с учетом эквивалентной схемы двухполюсника. В генерационных структурах могут работать диоды Ганна, ЛПД и туннельные диоды. Рассмотрим последние, так как они самые простые и при этом имеют самую сложную эквивалентную схему [2], представленную на рис. 1, где

- Rg – дифференциальное отрицательно сопротивление туннельного диода, пропорциональное наклону падающего участка вольтамперной характеристики (ВАХ) в точке, определяемой смещением,
- C – емкость диода, определяемая емкостью перехода (она изменяется в пределах падающего участка ВАХ примерно на 20 %,
- L – суммарная индуктивность диода, в которую входит индуктивность патрона и выводов (зависит в основном от геометрической формы выводов),
- r – суммарное сопротивление потерь в материале полупроводника, в контактах и выводах (примерно одно и то же в пределах всего рабочего участка ВАХ),
- C0 – емкость патрона диода (обычно рассматривают как часть внешней цепи, поэтому при дальнейшем моделировании не учитывалось).

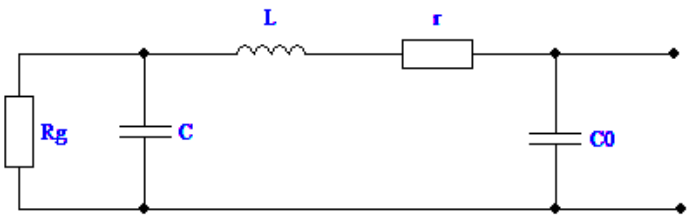
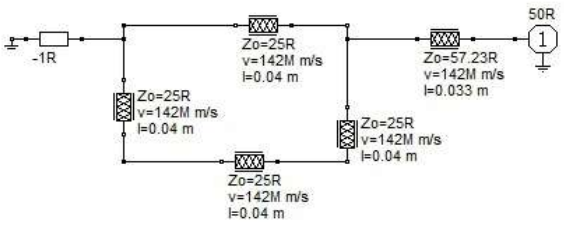


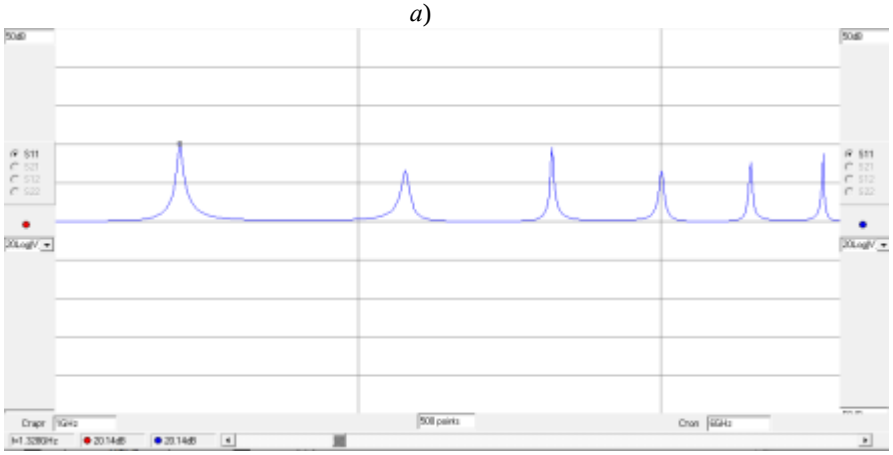
Рис. 1. Эквивалентная схема туннельного диода

На рис. 2 и 3 представлены результаты компьютерного моделирования двух принципиальных схем СВЧ-генератора. Первая схема (рис. 2а) учитывает лишь отрицательное дифференциальное сопротивление диода, а вторая (рис. 3а) – более точная компьютерная модель структуры, которая учитывает полную эквивалентную схему активного двухполюсника.

Характеристики существенно отличаются друг от друга. Полученный результат свидетельствует о том, что предлагаемая эквивалентная схема приближает компьютерную эмуляцию к реальной работе схемы. Также нельзя забывать, что проблемы сложения мощности находятся и в самом p-n переходе, возможно одновременная синхронная работа невозможна при низких добротностях резонаторов.



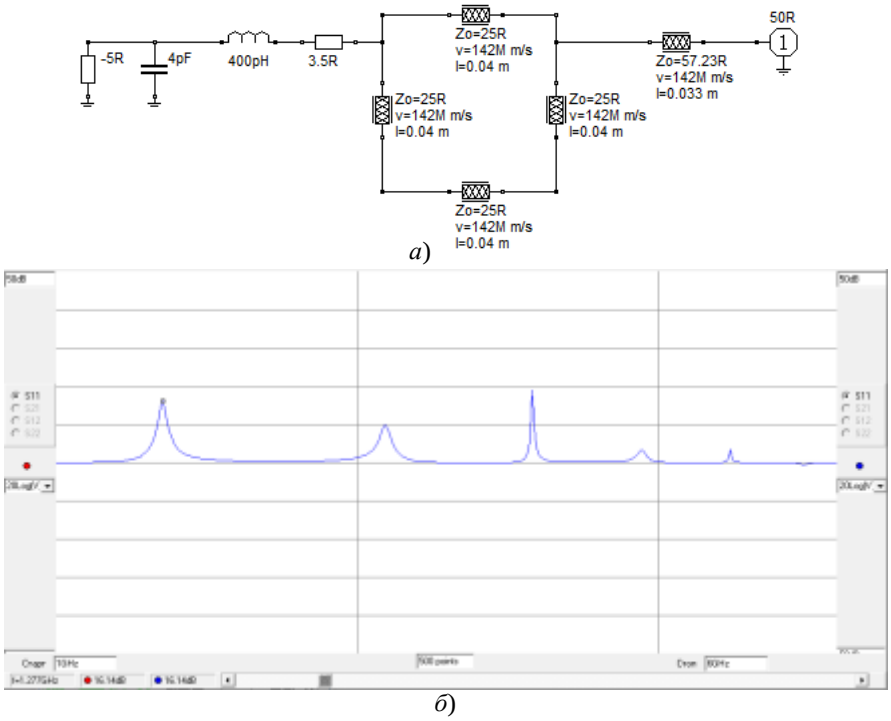
а)



б)

Рис. 2. Принципиальная схема СВЧ генератора без учета эквивалентной схемы туннельного диода (а) и полученная в САПР RFSim99 АЧХ (б)

Требуемый синхронизм работы полупроводников проще получить путем создания двух независимых устройств генерации, мощности которых складываются после резонаторов. Увеличение мощности путем сложения мощности от двух идентичных кольцевых генераторов (в случае объемных интегральных схем это не представляет никаких трудностей) не приведет к шумовым эффектам. Наши генераторы могут быть расположены в разных слоях объемной интегральной схемы. 3D модель предложенного генератора представлена на рисунке ниже. При макетировании такая конструкция дает алгебраическую сумму мощностей генераторов.



а)

б)

Рис. 3. Принципиальная схема СВЧ генератора с учётом эквивалентной схемы туннельного диода (а) и полученная в САПР RFSim99 АЧХ (б)

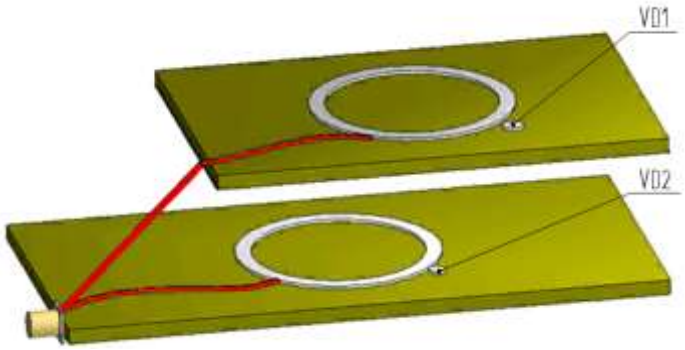


Рис. 4. 3D модель генератора повышенной мощности

Главным результатом проделанной работы является то, что квазистатический учет всех параметров кристалла p-n-перехода, включая паразитные емкости и индуктивности его корпуса, не дает ответа на вопрос о шумовой природе получаемой генерации. Из этого следует, что повышение уровня выходной мощности возможно только при соблюдении условия синхронизма работы p-n переходов. Если это условие не выполняется, то каждый последующий активный элемент просто увеличивает уровень выходного шума.

Список используемых источников

1. Ларионова А. К., Седышев Э. Ю. Кольцевой эллиптический генератор на активных двухполюсниках // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020) : Региональная научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 38–40.
2. Захаров В. И. Расчет и конструирование СВЧ усилителей на туннельных диодах. Министерство связи СССР, Московский электротехнический институт связи. Москва, 1969. С. 43–44.
3. Сазоненко Н. Ю., Седышев Э. Ю. Генератор на кольцевом резонаторе в микрополосковом исполнении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 509–513.
4. Кондрашова М. А., Сазоненко Н. Ю., Селиверстов Л. А., Улитина А. С., Седышев Э. Ю. Частотно-селективные устройства на кольцевых эллиптических резонаторах // Проектирование и технология электронных средств.2019. № 2. С. 13–20.

УДК 621.375
ГРНТИ 47.41.33

ИССЛЕДОВАНИЕ НЕЛИНЕЙНЫХ РЕЗОНАНСОВ В УСИЛИТЕЛЯХ КЛАССА *D* С ОТРИЦАТЕЛЬНОЙ ОБРАТНОЙ СВЯЗЬЮ

М. А. Межевова, В. А. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описана методика компьютерного моделирования частотных характеристик ключевых (нелинейных) усилителей мощности, работающих в режиме класса D. Методика учитывает спектры реальных установившихся процессов, возникающих при воздействии гармонического возмущения в замкнутом контуре отрицательной обратной связи. Приводятся и анализируются результаты расчетов.

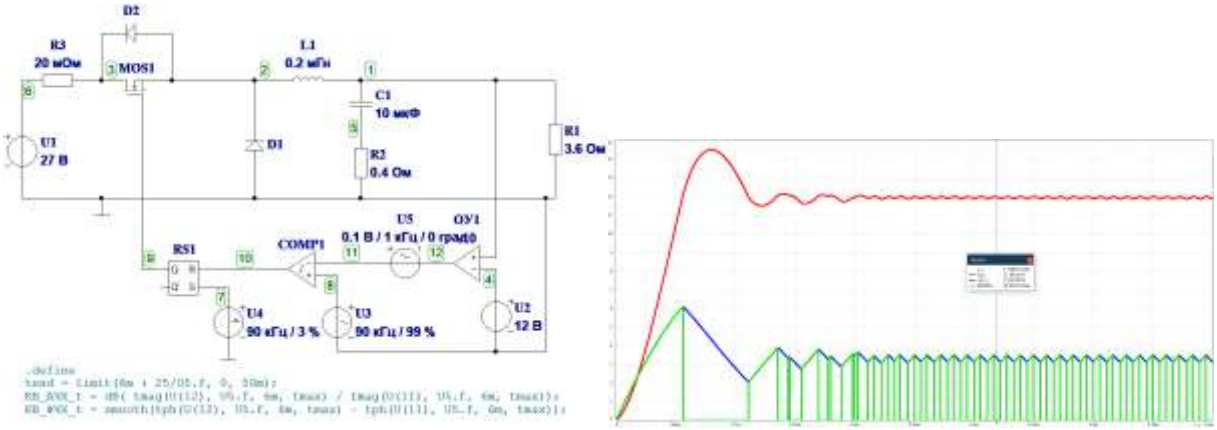
ключевые усилители мощности, метод замкнутого контура, нелинейные замкнутые системы.

Ключевые усилители мощности, как известно, обладают КПД, близким к 100 %, однако формирование выходного сигнала сопровождается сложными импульсными процессами. Применение отрицательной обратной связи (ООС) делает динамику таких устройств еще более сложной, способной в неустойчивом режиме генерировать непериодические и хаотические

колебания. Анализ таких усилителей традиционными частотными методами линейных схем фактически не учитывает специфику процессов, и не может служить основой рационального проектирования [1].

Методом замкнутого контура были рассчитаны эквивалентные частотные характеристики ключевых усилителей класса D с ООС, являющихся замкнутыми системами с широтно-импульсной модуляцией (ШИМ). Особенностью данного метода является то, что контур обратной связи не разрывается при вводе гармонического возмущения.

Применим данный метод к DC-DC преобразователю понижающего типа с ШИМ и ООС, являющегося моделью низкочастотного усилителя класса D (рис. 1а). Автоматизированный анализ проведем в программе FASTMEAN 6.0. Выходная мощность преобразователя составляет 40 Вт, тактовая частота блока ШИМ f_T = 90 кГц. На рис. 1б представлена переходная характеристика DC-DC преобразователя, по которой видно, что он работает в ключевом режиме, КПД составляет более 93 %.



а б

Рис. 1. Эквивалентная схема DC-DC преобразователя и его переходная характеристика.

В сечение контура обратной связи вводится источник гармонического возмущения U5. Амплитуда и частота которого подобрана так, чтобы не нарушать режим работы ШИМ. Методом замкнутого контура получены амплитудно- и фазо-частотные характеристики в диапазоне частот от 30 кГц до 110 кГц. Анализ этих характеристик показывает, что заметны неравномерности на субгармониках тактовой частоты ШИМ, а в окрестностях тактовой частоты- хаотичные всплески (рис. 2).

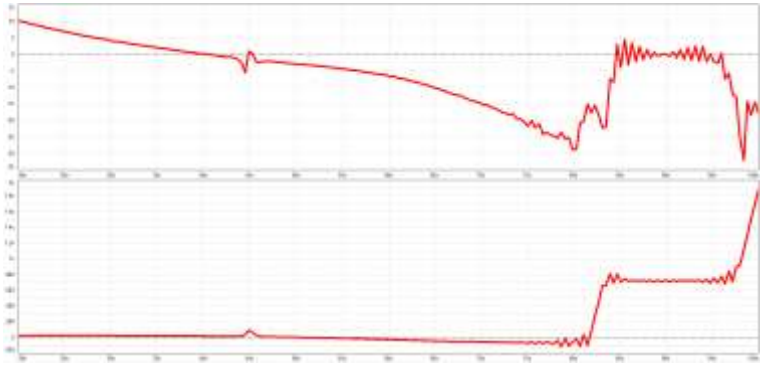
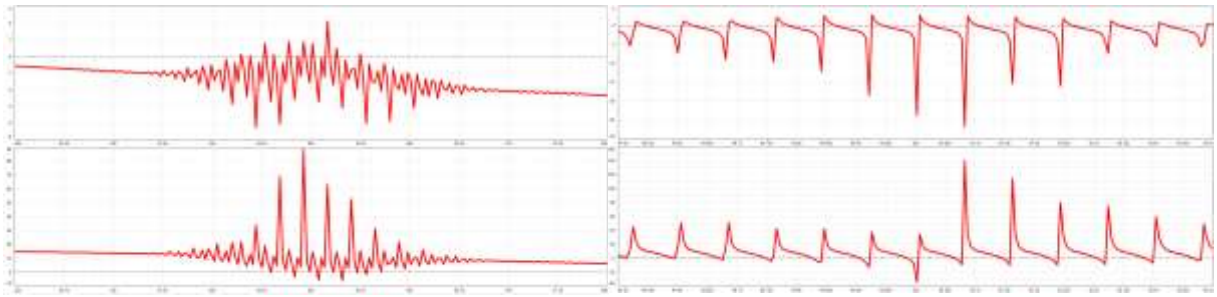


Рис. 2. Частотные характеристики DC-DC преобразователя

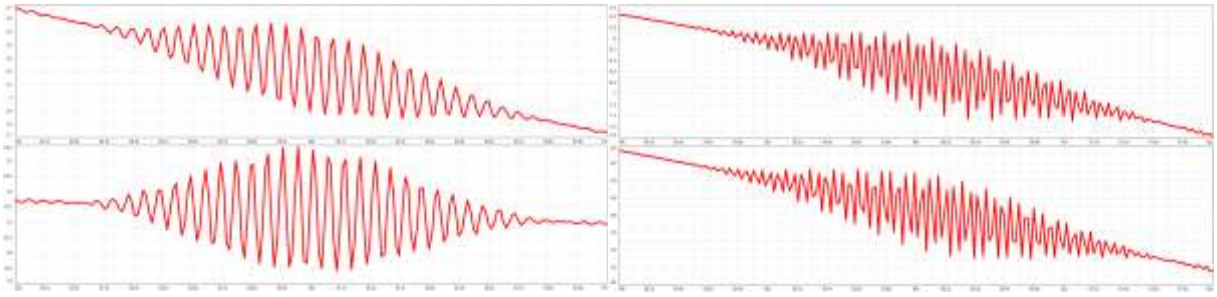
Рассмотрим подробнее частотную характеристику вблизи половины тактовой частоты (вторая субгармоника $f_T/2$) (рис. 3). Амплитуда всплесков АЧХ достигает 4,4 дБ, а ФЧХ – 130 градусов. Размах всплесков по АЧХ равен 29,4 дБ, по ФЧХ – 174,5 градусов. Для точного измерения максимального значения отклонения по амплитуде и фазе необходимо значительно уменьшать интервал расчета частотных характеристик, приближая его к субгармонике (рис. 3б). Это связано с ограничениями компьютерного моделирования, а именно с дискретным представлением данных характеристик.



а) 42–48 кГц б) 44,5–45,5 кГц

Рис. 3. Частотные характеристики DC-DC преобразователя в близи половины тактовой частоты

На частотах кратных 1/3 тактовой частоты также возникают резонансные колебания (рис. 4). По амплитуде и размаху они меньше колебаний на 1/2 $f_т$ (таблица 1). Однако они уменьшают запас по фазе и вызывают опасность генерации.



а) 29–31 кГц б) 58–62 кГц

Рис. 4. Частотные характеристики DC-DC преобразователя в близи 1/3 (а) и 2/3 (б) тактовой частоты

ТАБЛИЦА 1. Аналитические данные автоматизированного расчета

	Амплитуда		Размах	
	АЧХ, дБ	ФЧХ, градусы	АЧХ, дБ	ФЧХ, градусы
1/2 *f*т	4,4	130	29,4	174,5
1/3 *f*т	0,4	2,1	0,7	3,9
2/3 *f*т	0,7	4,7	1,6	10,3

Моделирование частотных характеристики устройства класса D с ШИМ и ООС показало, что вблизи 1/2, 1/3 и 2/3 тактовой частоты возникают колебания резонансного характера, что приводит к уменьшению запаса устойчивости по амплитуде и частоте, что может привести к генерации и хаотическим колебаниям. Генерация в значительной степени ухудшает энергетические и качественные показатели усилителя класса D, и устранение условий ее возникновения требует при проектировании ООС учета эквивалентных частотных характеристик, определяемых в нормально функционирующей системе [2].

Список используемых источников

1. Межевова М. А., Филин В. А. Моделирование и анализ частотных характеристик ВЧ усилителей мощности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 2. С. 518–522.

2. Смирнов В. С. Эквивалентные частотные характеристики транзисторных ключевых устройств с отрицательной обратной связью (математическое моделирование, методика измерения и оптимизации): дисс. … канд. техн. наук: 05.12.04 / Смирнов Василий Сергеевич. СПбГУТ. – СПб., 2006.

УДК.621.396.6
ГРНТИ 47.47

УМЕНЬШЕНИЕ УРОВНЯ ДИСКРЕТНЫХ ПОМЕХ В СИНТЕЗАТОРНЫХ КОЛЬЦАХ ИФАП

Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены основные методы активного цифроаналогового синтеза частот, которые позволяют обеспечить требуемое качество формируемых колебаний и минимизировать уровень дискретных побочных спектральных составляющих (ДПСС). Произведена их классификация. Показаны основные преимущества и недостатки.

кольцо импульсно-фазовой автоподстройки частоты, счетчик импульсов, накапливающий сумматор, нониус. Побочные спектральные составляющие.

В основе методов активного цифрового (цифроаналогового) синтеза лежит идея управления частотой перестраиваемого генератора (ПГ) с помощью цепи отрицательной обратной связи по частоте или по фазе. Другими словами, структура активного синтеза частот является системой автоматического регулирования, которая содержит внутренние генераторные (генерирующие колебания) элементы [1].

Основным признаком устройств активного синтеза является наличие выходного колебания $f_{\text{выхВЧ}}$ при отключении источника опорного колебания $f_{\text{опНЧ}}$ (но частота выходного колебания в этом случае не соответствует коду управления).

Методы активного синтеза реализуют как с помощью колец импульсно-фазовой автоподстройки частоты (ИФАП), так и с помощью колец компенсации (КК) или возвратного гетеродинирования.

Помехи в «ближней» зоне отстроек от выходного (несущего) колебания $f_{\text{выхВЧ}}$ – шумовых побочных спектральных составляющих (ПСС) и дискретных ПСС (ДПСС) обязаны своим появлением идеологии построения (структуре) ССЧ, используемым методам активного синтеза, схемотехнике и качеству выполнения его узлов.

В системах связи уровни ПСС и ДПСС – важнейшие параметры. Внутри полосы частот, занимаемой информационным сигналом, они определяют достоверность его передачи; вне информационной полосы уровни ПСС и ДПСС определяют интенсивность внеполосного излучения, т. е. электромагнитную совместимость (ЭМС) радиоэлектронных средств.

Введение в цепь отрицательной обратной связи счетчика импульсов (СИ) превращает непрерывное аналоговое кольцо ФАП в импульсную систему автоматического регулирования – ИФАП (рис.1).

Это влечет за собой существенные последствия:

1. Кольцо ИФАП становится импульсной системой автоматического регулирования, сохраняя астатизм по частоте, но прекращает фильтрацию помех при отстройках от несущей, больших $f_{\text{опНч}}/2$;

2. Уменьшается зона компенсации помех, воздействующих на ПГ;

3. Возрастает подчеркивание в N раз низкочастотных помех, приходящих с опорным колебанием и попадающих в полосу прозрачности условно разомкнутого кольца;

4. Появляется возможность умножения частоты дискретизации $f_{\text{опНч}}$ в N раз.

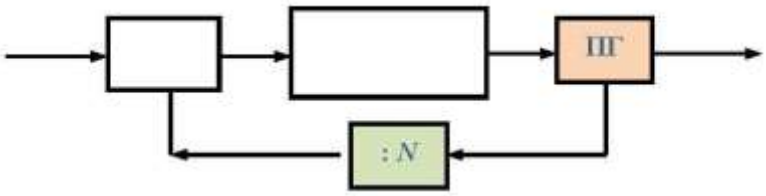


Рис. 1. Кольцо ИФАП в качестве умножителя частоты

В кольцах ИФАП принято называть СИ с управляемым коэффициентом пересчета делителем с переменным или дробно-переменным коэффициентом деления (ДПКД или ДДПКД).

Основной дискретной помехой, подлежащей фильтрации в кольце ИФАП, является помеха с частотой шага сетки F_s. Существует несколько путей уменьшения этой помехи [2].

Во-первых, можно «утяжелить» петлевой фильтр нижних частот кольца ИФАП. Однако, такое решение влияет на устойчивость кольца и существенно увеличивает время переходных процессов при перестройке частоты.

Во-вторых, можно ввести дробность в СИ, управлять коэффициентом деления с помощью дельта-сигма модулятора на основе накапливающего сумматора (НС или цифровой интегратор) – рис. 2. Период помехи не изменится, но ее величина уменьшится, что облегчит фильтрацию. Помеха с частотой F_s будет умножаться кольцом не в N раз, а в $\lfloor N \rfloor$ раз, где $\lfloor N \rfloor$ – целая часть N, меньшая или равная ему. Заметим, что СИ и НС являются разновидностями конечного автомата (КА) и широко используются в технике синтеза частот [3].

В-третьих, можно увеличить число цифровых интеграторов в цепи обратной связи СИ и повысить крутизну убывания амплитуд гармоник F_s (субгармоник частоты сравнения $f_{\text{опНЧ}}$). Такое решение позволяет уменьшить влияние помех дробности на спектральные характеристики кольца.

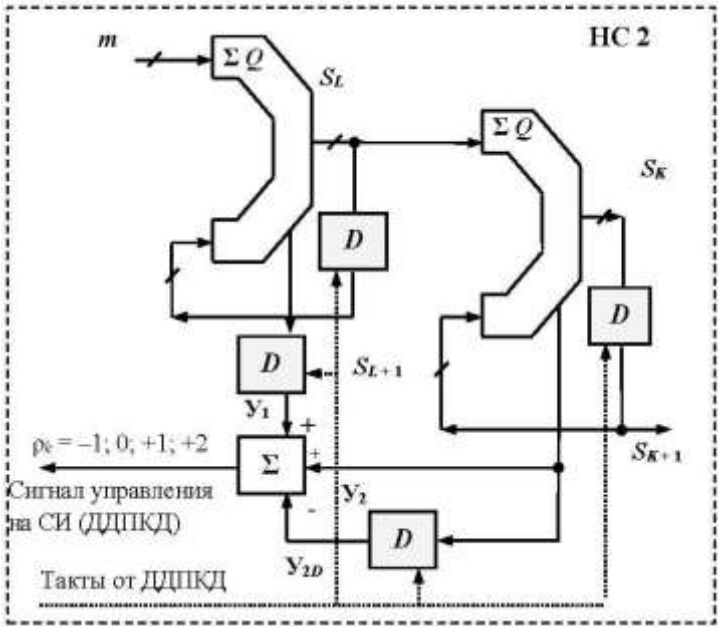


Рис. 2. ΔΣ модулятор второго порядка

Платой, кроме некоторого роста шумов и неполной компенсации помех дробности, является удвоение периода неравномерности на выходе ДДПКД и, соответственно, уменьшение значения минимальной фильтруемой частоты до $f_{\text{опНЧ}}/2$. При некоторых реализациях дельта-сигма модуляторов период неравномерности может дополнительно увеличиваться в 3 и 6 раз [4].

Функция переполнения ρ_k в НС2 есть конечная разность второго порядка $\rho_k^{(2)}$ и описывается формулой:

$$\rho_k^{(2)} = \left\lfloor (k+2)\frac{m}{Q} \right\rfloor - 2\left\lfloor (k+1)\frac{m}{Q} \right\rfloor + \left\lfloor k\frac{m}{Q} \right\rfloor.$$

Здесь k – номер импульса переполнения ρ_k; m – значение дробности N; Q – модуль дробности N:

$$N = \lfloor N \rfloor + \frac{m}{Q}.$$

В-четвертых, можно понизить частоту на входе СИ с помощью внешнего колебания подставки F_{LO} – рис. 3.

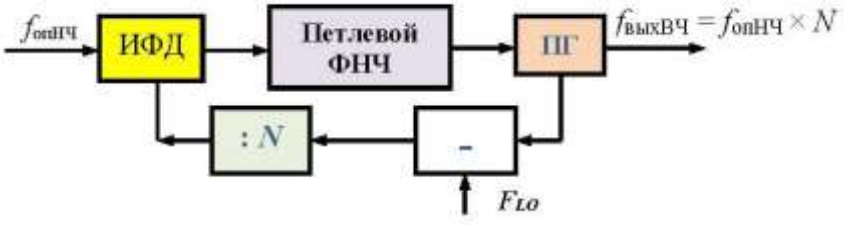


Рис. 3. Понижение частоты на входе СИ с помощью частоты подставки F_{LO}

В-пятых, можно распараллелить каналы управления и вместо одного использовать Q каналов, где Q – модуль дробности [5] – рис. 4.

В-шестых, можно использовать многоуровневые тракты приведения частоты ПГ $f_{\text{выхВЧ}}$ к частоте опорного колебания $f_{\text{опНЧ}}$ – рис. 5 [5].

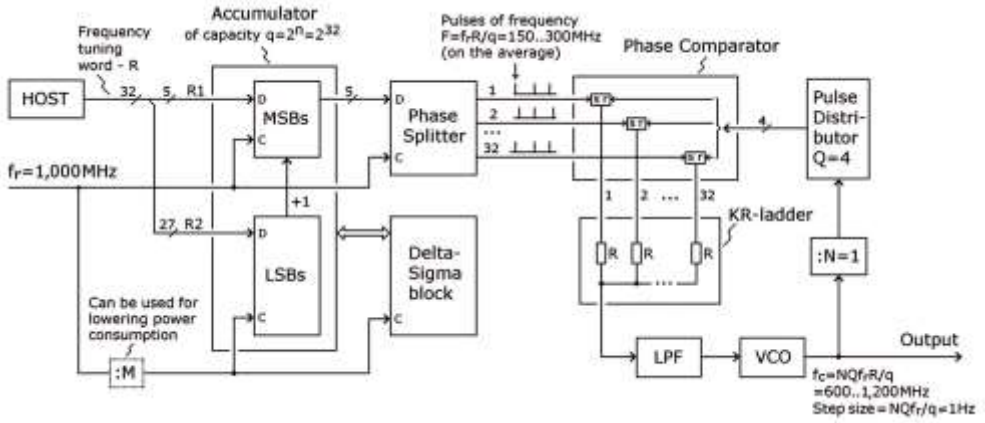


Рис. 4. Вариант «параллельного» тракта приведения умножающего кольца ИФАП

На рис. 5 приведена структура тракта приведения с двумя НС – и в тракте R опорного колебания, и в тракте N выходного колебания.

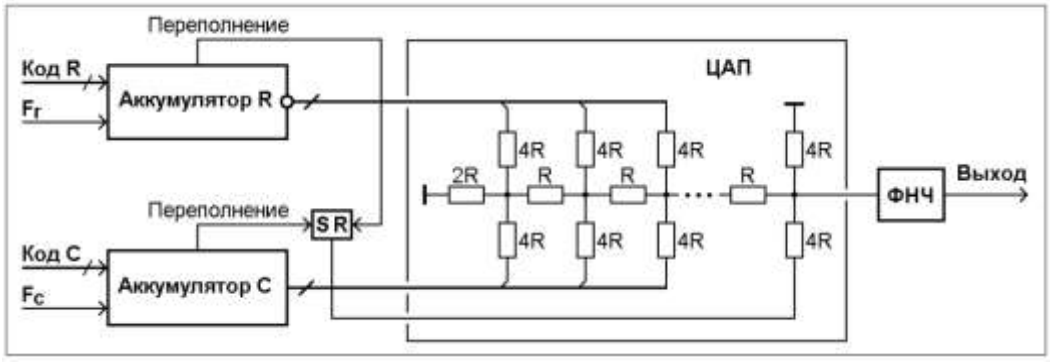


Рис. 5. Многоуровневый тракт приведения с НС в обеих ветвях

Помехи дробности с частотой шага сетки в таком тракте не исчезают, но уменьшаются пропорционально увеличению разрядности накапливающих сумматоров. Импульсно-фазовый детектор (ИФД) на основе RS-триггера тактирует многоуровневое колебание опорной частоты, сформированное с помощью накапливающего сумматора НС (другие названия – накопительный сумматор, цифровой интегратор, аккумулятор фазы, дельта-сигма модулятор).

Амплитуда такого колебания пропорциональна его мгновенной фазе, а распределение амплитуд определяется арифметической структурой числа R – коэффициента деления опорной частоты.

В итоге уровень дискретных ПСС, кратных частоте шага сетки уменьшается, но не полностью, поскольку арифметические структуры чисел R и N

различны в принципе. Фильтрация помех, кратных частоте F_s облегчается, но остается необходимой. Выходная частота определяется по формуле:

$$f_{\text{выхВЧ}} = f_{\text{опНЧ}} \frac{N}{R}.$$

В-седьмых, можно ввести рандомизацию коэффициента деления ДДПКД (изменение его модуля с нулевым средним), что, однако, приводит к уширению спектральной линии [6].

В-восьмых, можно использовать алгоритмическую компенсацию помех дробности [1, 7].

В-девятых, можно использовать фазовращатель на входе тракте СИ [8].

В-десятых, можно применить амплитудную или фазовую компенсацию помех дробности с помощью ЦАП или управляемого устройства задержки [1].

Наконец, можно использовать нониусный тракт приведения [9] – рис. 6.

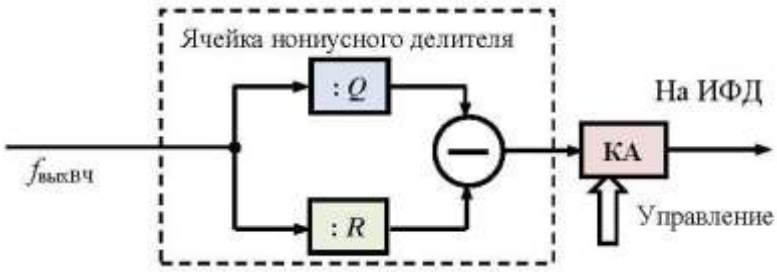


Рис. 6. Цифровая нониусная ячейка

Выбор предпочтительной структуры умножающего кольца ИФАП и способов улучшения качества спектральной линии на его выходе зависит от квалификации инженера, его кругозора и уровня полученных знаний.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника: монография. СПб.: Изд-во СПб ГУТ, 2018. 367 с.

2. Никитин Ю. А. Построение тракта приведения активного синтезатора частот // Известия вузов. Приборостроение. 2012. № 3. С. 19–26.

3. Никитин Ю. А. Конечный автомат как элемент цифровой системы синтеза частот // X Международная научно-техническая конференция «Радиолокация, навигация, связь». Воронеж: НПФ «САКВОЕЕ» ООО, 2004. Т. 1. С. 526–533.

4. https://www.analog.com/media/en/technical-documentation/data-sheets/ADF41513.pdf

5. Козлов В. И. Способ цифрового фазового детектирования // Радиотехника. 1980. Т. 35, № 4. С. 25–29.

6. Шишов С. Я., Ямпурин Н. П. Спектральные характеристики синтезатора частот на основе цифрового накопителя со случайной вариацией емкости // Техника средств связи. Серия ТРС. 1984. Вып. 9. С. 80–84.

7. Гуревич И. Н., Никитин Ю. А. Методика синтеза оптимального алгоритма управления делителем с дробным коэффициентом деления // Техника средств связи. Сер. ТРС. 1978. № 5. С. 59–67.

8. Модель В. М. Быстродействующий синтезатор частот // ТСС, сер. ТРС. вып. 5. 1984. С. 88–93.

9. Никитин Ю. А. Анализ дробного нониусного тракта приведения умножающего кольца импульсно-фазовой автоподстройки частоты // Известия вузов России. Серия Радиоэлектроника. 2012. № 1. С. 31–37.

УДК 621.396.6
ГРНТИ 47.47

ПАССИВНЫЙ ЦИФРОВОЙ СИНТЕЗ НА ОСНОВЕ НС И ДДПКД

Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены методы пассивного цифрового синтеза частот на основе накапливающего сумматора и делителя с дробно-переменным коэффициентом деления, дополненные управляемым устройством задержки. Такие синтезаторы применяются в современных системах синтеза частот и позволяют обеспечить требуемое качество формируемых колебаний. Показаны основные преимущества и недостатки.

пассивный цифровой синтез частот (ПЦС), конечный автомат (КА), модифицированный двухуровневый конечный автомат (МКА), счетчик импульсов (СИ), накапливающий сумматор (НС), управляемое устройство задержки (УУЗ).

Возможно построение прямочастотного МКА на основе НС (рис. 1) [1].

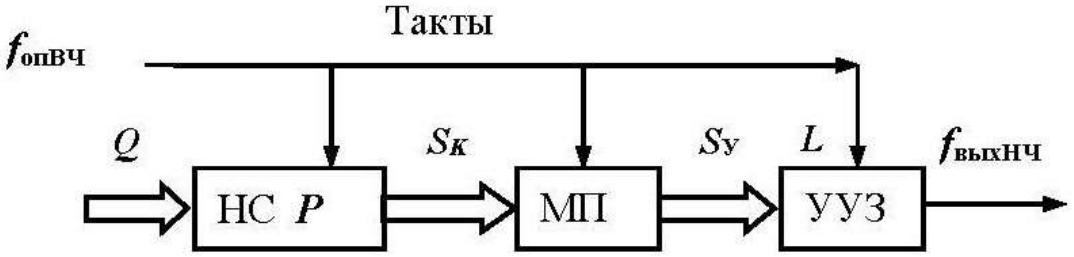


Рис. 1. Структурная схема двухуровневого КА на основе НС и УУЗ

На рис. 2 показан пример введения в КА УУЗ с числом интерполируемых участков $L = 5$ при установке кода выходной частоты $Q = 4$.

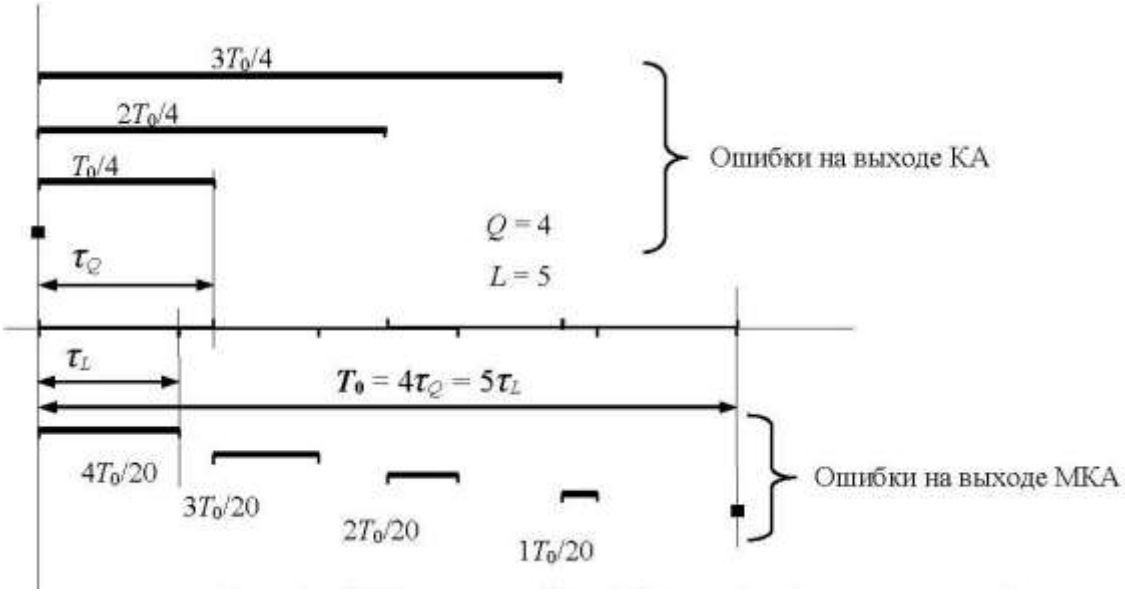


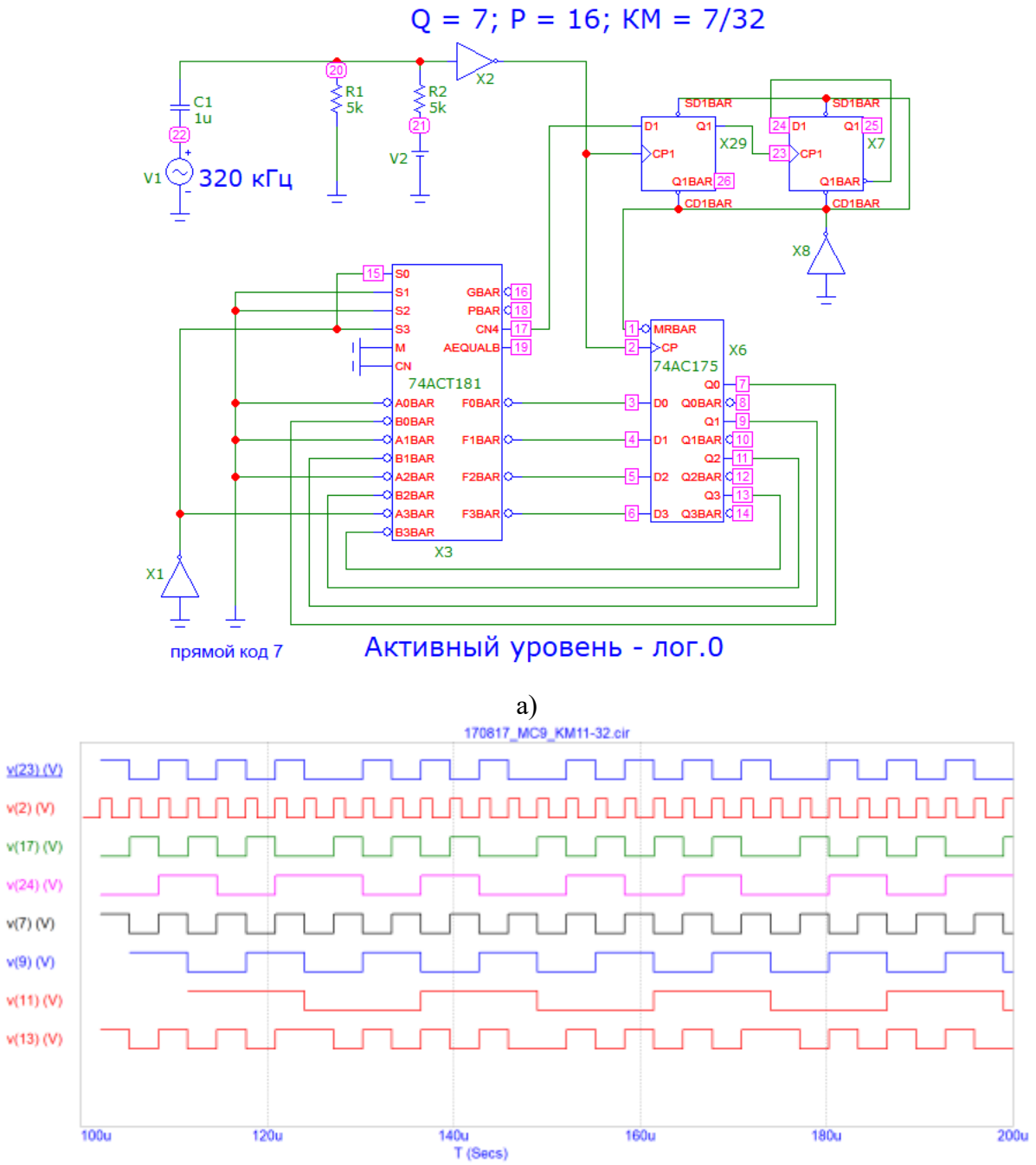
Рис. 2. Сравнение временной ошибки КРП на выходе КА и МКА при $Q = 4$ и числе градаций задержки в УУЗ $L = 5$

Значения текущей фазы S_K на периоде неравномерности $T_S = 1/F_S = QT_Г = PT_0$ пробегают все значения от 1 до P-1 в очередности, которая определяется структурой числа $N = P/Q$ – его разложением в цепную дробь по алгоритму Евклида.

Отметим, что при выполнении цифровой части МКА в виде НС (рис. 1) задача МП заключается в пересчете текущего кода фазы S_k с выхода НС в код текущей задержки $S_У$. Тактируют НС, МП и УУЗ импульсами с входной частотой $f_{опВЧ}$. Поэтому требования к быстродействию указанных устройств достаточно жесткие.

Полезным сигналом, кроме кода текущей фазы, при двухуровневом синтезе служат импульсы переполнения НС, следующие с усредненной на периоде неравномерности $T_S = 1/F_S$ частотой $f_{ВыхНЧ}$:

$$f_{ВыхНЧ} = f_{ОпВЧ}\frac{Q}{P} = QF_S.$$



а)

б)

Рис. 3. Модель пассивного синтезатора на основе 4-х битового НС (а), временные диаграммы его работы (б)

Возможно также построение прямопериодного МКА на основе ДДПКД (рис. 4) [2]. Тактируют НС, МП и УУЗ импульсами выходной частоты $f_{\text{выхНч}}$. Поэтому требования к быстродействию указанных устройств ослаблены в K раз.

КА на основе ДДПКД оптимальный, как и КА на основе НС. Поэтому уровень ДПСС на его выходе при коэффициенте деления K будет не хуже:

$$D[\text{дБн}] \le 20\lg(f_{\text{выхНЧ}}/(f_{\text{опВЧ}})) = 20\lg(K).$$

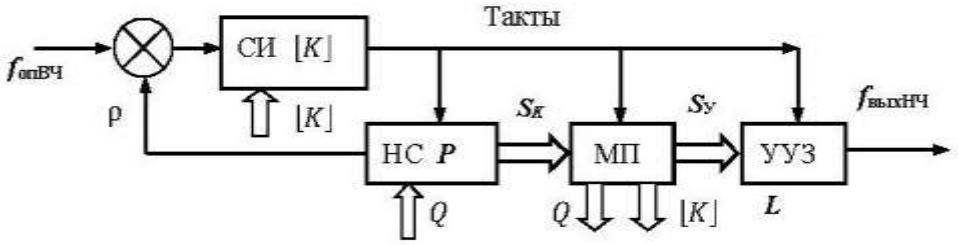


Рис. 4. Структурная схема КА на основе ДДПКД и УУЗ

На выходе КА имеется информация о временном рассогласовании между импульсами (одноименными перепадами) идеально равномерной во времени (гипотетической) двухуровневой последовательности частоты $f_{\text{выхНЧ}}$ и импульсами (одноименными перепадами) синтезируемой квазиравномерной последовательности. Например, для случая НС (рис. 2) с параметрами $P = 16$, $Q = 7$ запишем:

$$\Delta_i = \frac{S_i}{Q} = \left\{ i\frac{Q}{P} \right\}. \quad (1)$$

Результат расчетов сведем в табл. 1.

Отметим, что, согласно (1) и табл. 1 код задержки в МКА на основе НС накапливается в долях P. Следовательно, для правильного управления УУЗ необходимо выполнять операцию:

$$x_{\text{ууз}} = \left(1 - \left\{ i\frac{Q}{P} \right\}\right)\frac{P}{Q_{\text{Н}}}.$$

Следовательно, МП на рис. 2 должен выполнять арифметическую операцию $S_У = P - S_i$ в момент переполнения НС (в моменты тактов с номерами 0, 3, 5, 7, 10, 12, 14, 16 и т. д.). Кроме того, МП должен осуществлять текущий пересчет кода управления, поскольку настройку УУЗ производят на одной частоте выходного диапазона, а работать необходимо в широком диапазоне выходных частот.

Аналогично, для ДДПКД (рис. 4) запишем $N = P/Q = 16/7 = 2 + 2/7$. Соответственно, в СИ запишем число $K = 2$, емкость НС выберем $P = 7$ и запишем в него число $Q = 2$. Тогда таблица состояний примет вид представленный в табл. 2.

ТАБЛИЦА 1. Временные диаграммы работы КА на основе НС

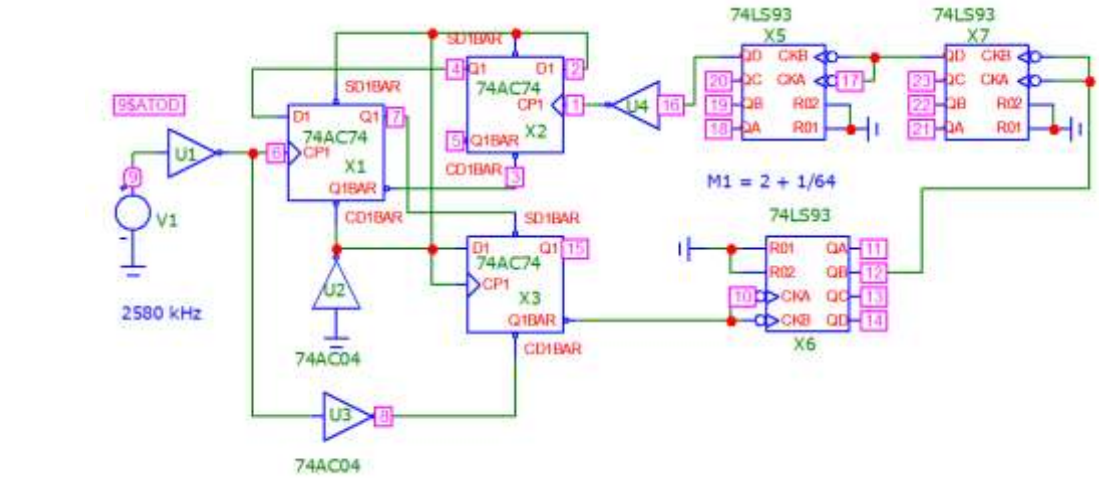
Такты i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Текущая сумма S_i	0	7	14	5	12	3	10	1	8	15	6	13	4	11	2	9	0	7
Переполнение ρ_i	**1**	0	0	**1**	0	**1**	0	**1**	0	0	**1**	0	**1**	0	**1**	0	**1**	0
Относительная ошибка Δ_i	**0**			**5/16**		**3/16**		**1/16**			**6/16**		**4/16**		**2/16**		**0**	
Требуемая задержка τ_i	**1**			**11/16**		**13/16**		**15/16**			**10/16**		**13/16**		**11/16**		**15/16**	

ТАБЛИЦА 2. Временные диаграммы работы КА на основе ДДПКД

Такты i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Выход СИ $\lfloor N_i \rfloor$	**1**	0	0	**1**	0	**1**	0	**1**	0	**1**	0	0	**1**	0	**1**	0	**1**	0
Текущая сумма S_i	0			2		4		6		1			3		5		0	
Переполнение ρ_i	**1**	0	0	**0**	**0**	0	0	0	0	**1**	0	0	0	0	**1**	0	**1**	0
Относительная ошибка Δ_i	**0**			**2/7**		**4/7**		**6/7**			**1/7**		**3/7**		**5/7**		**0**	
Требуемая задержка τ_i	**0**			**2/7**		**4/7**		**6/7**			**1/7**		**3/7**		**5/7**		**0**	

Тактируют НС и МП импульсами выходной частоты $f_{\text{выхНЧ}}$, поэтому требования к их быстродействия ослаблены в $\lfloor K \rfloor$ раз. А с учетом того факта, что быстродействие СИ значительно выше, чем быстродействие НС и может быть сделано равным быстродействию первого триггера счетчика, двухуровневые КА такого вида применяют (в виде ДДПКД) в микроволновых синтезированных генераторах на основе колец ИФАП для синтеза частот.

Код требуемой задержки соответствует коду текущей суммы и не требует пересчета. Но микропроцессор в обоих случаях должен домножать код текущей задержки на текущий множитель $Q/Q_{\text{Н}}$, где Q – установленное значение выходной частоты, $Q_{\text{Н}}$ – частота, на которой производилась настройка УУЗ [3].



а)

б)

Рис. 5. Модель пассивного синтезатора на основе ДДПКД (а), временные диаграммы его работы (б)

Задачей УУЗ является изменение временного положения импульса переполнения $\boldsymbol{\rho_k}$ на Δt_k в соответствии с (1) таким образом, чтобы устранить или уменьшить ФФИМ на выходе двухуровневого МКА.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника: монография. СПб.: Изд-во СПб ГУТ, 2018. 367 с.

2. Никитин Ю. А. Широкополосный синтез частот с помощью делителя с дробно-переменным коэффициентом деления // Известия вузов. Серия Приборостроение. 1989. № 10. С. 33–39.

3. Никитин Ю. А. Двухуровневый синтез частот с помощью модифицированного конечного автомата // Электросвязь. 1990. № 5. С. 33–35.

УДК.621.396.6
ГРНТИ 47.47

ИСПОЛЬЗОВАНИЕ УПРАВЛЯЕМОГО УСТРОЙСТВА ЗАДЕРЖКИ «КОД-НАПРЯЖЕНИЕ-ВРЕМЯ» В ПАССИВНОМ ЦИФРОВОМ СИНТЕЗАТОРЕ

Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены методы пассивного цифрового синтеза частот на основе накапливающего сумматора и делителя с дробно-переменным коэффициентом деления, дополненные управляемым устройством задержки. Управление задержкой необходимо для уменьшение функциональной фазоимпульсной модуляцией, присущей данному методу синтеза частот. Управляемое устройство задержки построено на основе промежуточных преобразований кода задержки во временной интервал. Рассмотрена структура устройства и требования к ее элементам.

пассивный цифровой синтез частот (ПЦС), конечный автомат (КА), модифицированный двухуровневый конечный автомат (МКА), счетчик импульсов (СИ), накапливающий сумматор (НС), управляемое устройство задержки (УУЗ), генератор стабильного тока, ключ тока (напряжения), цифроаналоговый преобразователь, компаратор.

Задачей управляемого устройства задержки (УУЗ) является изменение временного положения импульса переполнения $\boldsymbol{\rho_k}$ в (1)

$$\boldsymbol{\rho_k} = \lfloor\, kQ/P \,\rfloor - \lfloor\, (k-1)Q/P \,\rfloor, \quad \boldsymbol{\rho_k} \in (0, 1). \qquad (1)$$

в соответствии с рис. 1 или (2)

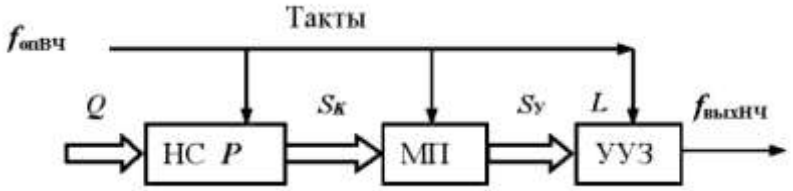


Рис. 1. Структурная схема двухуровневого КА на основе НС и УУЗ

$$\rho_k = \lfloor kP/Q \rfloor - \lfloor (k-1)P/Q \rfloor, \tag{2}$$

в соответствии с рис. 2 на Δt_k в соответствии с (3)

$$\Delta_i = \frac{S_i}{Q} = \left\{ i \frac{Q}{P} \right\}. \tag{3}$$

таким образом, чтобы устранить или уменьшить функциональную фазоимпульсную модуляцию (ФФИМ) на выходе двухуровневого МКА [1].

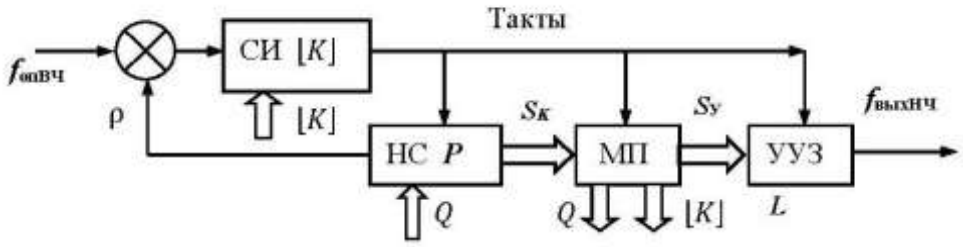


Рис. 2. Структурная схема КА на основе ДДПКД и УУЗ

Поскольку временной сдвиг в сторону опережения физически невозможен, простейшим решением является задержка $\boldsymbol{\rho_k}$ до следующего ближайшего импульса (перепада) гипотетической (идеально равномерной) последовательности требуемой частоты в интервале времен

$$\Delta t_k = t_k^{макс} (X_k = Q) \ \ldots \ t_k^{мин} (X_k = 1)$$

в соответствии с формулой

$$\frac{t_{зk}}{T_0} = \frac{(Q-1)}{Q} - \frac{S_k}{Q} = \frac{X_k}{Q}, \tag{4}$$

при этом S_k может пробегать значения соответственно от 0 до $Q - 1$.

Для правильного функционирования УУЗ в составе широкополосного двухуровневого МКА следует выполнить два условия обеспечения диапазонности (требуемой широкополосности)

$$\frac{\Delta t_k}{T_0} = \frac{K_k}{Q}, \qquad (5)$$

где K_k линейный коэффициент, и условие чистоты спектра (наибольшего подавления ФФИМ)

$$K_k = X_k.$$

Управление задержкой переключения можно реализовать с помощью промежуточных преобразований кода текущей задержки в напряжение (ток), а затем во временной интервал.

Для единообразного рассмотрения таких УУЗ, во-первых, унифицируем их структуры таким образом, чтобы они содержали одинаковые элементы: ЦАП, управляемые генераторы тока на основе ЦАП, компараторы напряжения ***K***, безынерционные ключи тока и напряжения и хронирующие емкости ***C*** [2].

Во-вторых, будем считать, что КА вырабатывает код управления X_k в соответствии с (5), т. е. X_k содержит полную информацию о величине текущей (мгновенной) фазовой ошибки, но конечное число ***n*** двоичных разрядов ЦАП вынуждает использовать для управления УУЗ приближенный код $Y_k < X_k$ ($Y_{макс} = 2^n - 1 < Q$), который получен усечением младших разрядов управляющего слова X_k.

В-третьих, ограничим диапазон синтезируемых частот $f_{выхНЧ} \in F_s$ ($Q_{макс} \ldots Q_{мин}$) одной октавой ($Q_{макс} = 2Q_{мин}$) при двоичном управлении Q.

Последнее обстоятельство не сужает общности рассуждений, поскольку расширение диапазона синтезируемых частот «вниз» без изменения режима работы УУЗ легко достигается подключением к выходу УУЗ цепочки триггеров (двоичных счетчиков импульсов СИ).

В первом варианте УУЗ1 выходной импульс (активный перепад) КА запускает процесс промежуточных преобразований с целью калиброванного сдвига этого импульса (активного перепада) на заданную величину, пропорциональную коду управления задержкой, например, используя преобразование «код – напряжение – время» (рис. 3).

Импульс переполнения ρ_k запускает генератор пилообразного напряжения (ГПН) наносекундного диапазона. Пилообразное напряжение с выхода ГПН подается на первый вход компаратора ***K*** (рис. 3). На второй вход компаратора ***K*** поступает напряжение с выхода ЦАП, пропорциональное коду требуемой задержки.

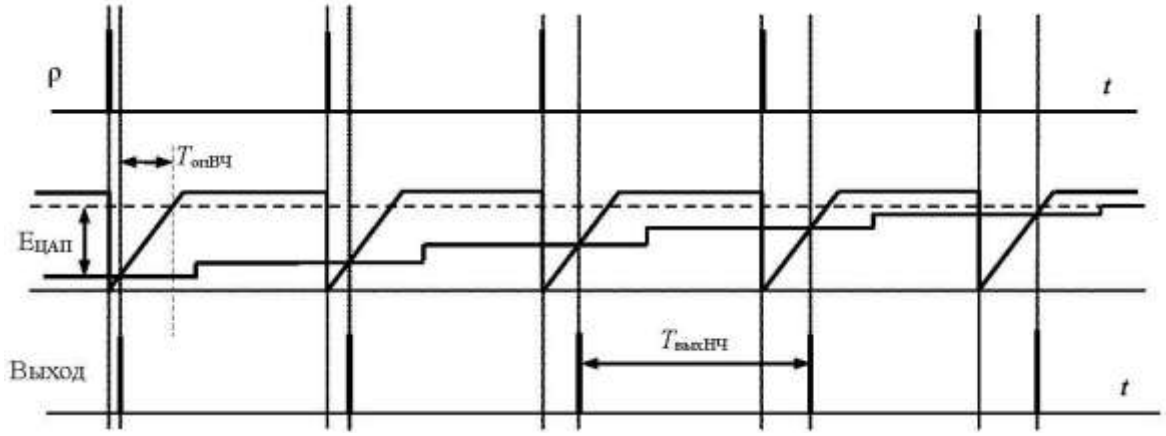


Рис. 3. Управляемое устройство задержки
на основе преобразования «код-напряжение-время»

Выход компаратора формирует двухуровневую последовательность импульсов или активных перепадов, которая является КРП, как и на входе, но с новыми параметрами – рис.4. Если принять, что период интерполяции в УУЗ равен $\tau_0 = T_{ОпВЧ}/L$, где L – разрядность (число градаций задержки) УУЗ, то эквивалентный коэффициент деления КА увеличится и станет равным

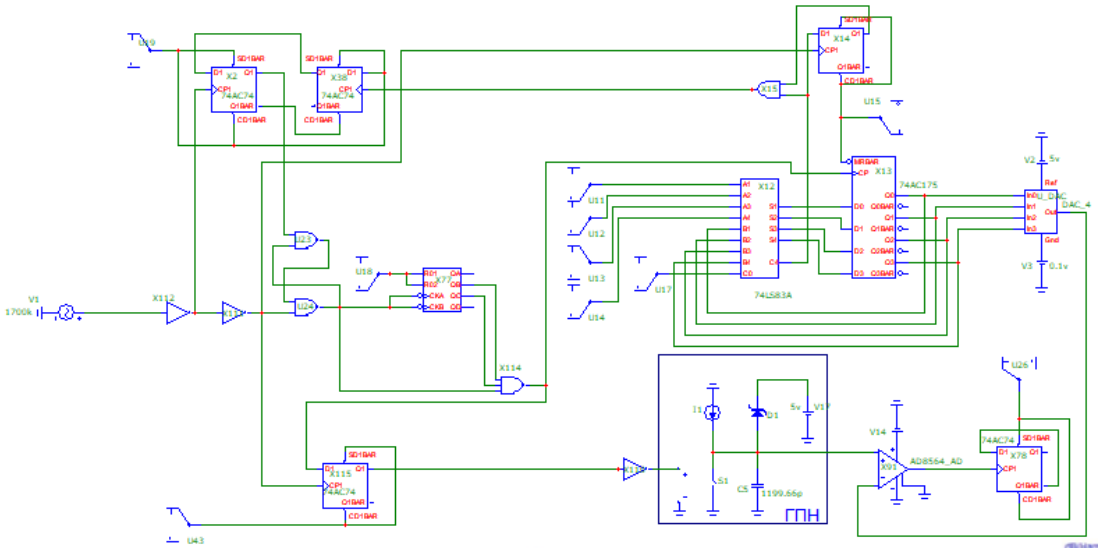
$$N_{ЭКВ} = LP/Q.$$

Иными словами, введение в структуру КА управляемого устройства задержки в линейном приближении эквивалентно увеличению входной частоты $f_{опВЧ}$ в L раз [3].

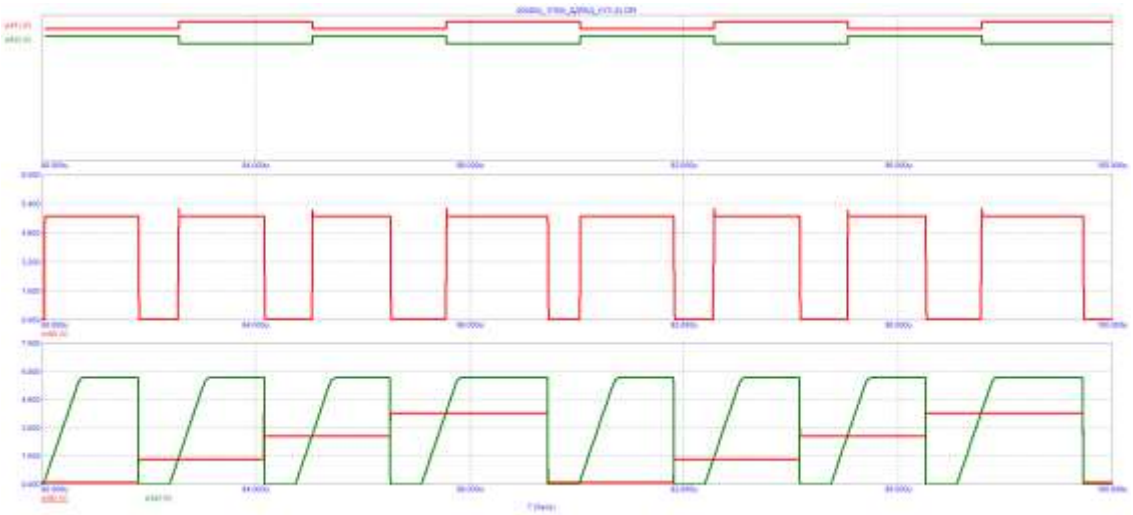
Реально достижимый выигрыш при использовании УУЗ1 составляет 43…48 дБ и ограничен рядом факторов. Прежде всего, это нелинейность генератора пилообразного напряжения (ГПН) наносекундного диапазона (рис. 2), нелинейное изменение емкости *p-n* переходов ключей напряжения, а также конечное быстродействие компаратора и ЦАП. Напряжение на выходе ЦАП вследствие конечного выходного сопротивления и емкости устанавливается с заданной точностью за определенное время [2].

Задержанный импульс (перепад напряжения) на выходе компаратора ***K*** (рис. 4) появляется в момент равенства напряжения $U_{ЦАП}$ и $U_{ГПН}$, т. е. при $U_{ЦАП}(X) = U_{ГПН}(t)$, где $U_{ЦАП}(X) = X \times E$; $0 \le X < 1$ – код требуемой задержки; E – размах напряжения на выходе ЦАП, соответствующий $\tau_з = T_{опВЧ}$.

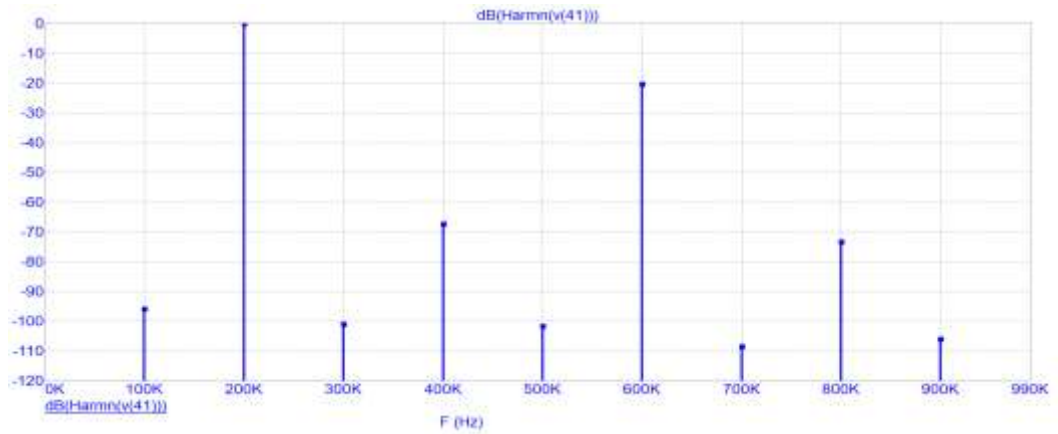
После деления частоты в два раза, на выходе счетного триггера образуется колебание вида квазимеандр, в котором уровень полезной компоненты спектра имеет максимальное значение.



а)



б)



в)

Рис. 4. Модель синтезатора частоты на основе делителя с дробно-переменным коэффициентом деления и управляемого устройства задержки первого типа (а), временные диаграммы его работы (б), спектр на выходе (в)

Гармоники выходного колебания легко отфильтровываются с помощью простейшего фильтра нижних частот, а амплитуды субгармоник существенно уменьшены (в L раз) вследствие введения в структуру синтезатора управляемого устройства задержки.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника: монография. СПб.: Изд-во СПбГУТ, 2018. 367 с.

2. Никитин Ю. А. Влияние нелинейности модифицированного конечного автомата на временную нестабильность формируемого колебания // Известия вузов. Приборостроение. 1991. № 5. С. 28–33.

3. Гуревич И. Н., Никитин Ю. А. Управляемые устройства задержки в системах двухуровневого синтеза частот // Радиотехника. 1993. № 10–12. С. 13–20.

УДК 621.396.6
ГРНТИ 47.41.37

УПРАВЛЕНИЕ ВРЕМЕННОЙ ЗАДЕРЖКОЙ ИМПУЛЬСНЫХ СИГНАЛОВ В НАНОСЕКУНДНОМ ДИАПАЗОНЕ

Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены методы управления временной задержкой активных перепадов цифровых устройств – конечных автоматов. Управляемые устройства задержки используются в современных системах синтеза частот и позволяют обеспечить требуемое качество формируемых колебаний.

управляемое устройство задержки (УУЗ), модифицированный двухуровневый конечный автомат (МКА), генератор стабильного тока, ключ тока и(ли) напряжения, счетчик импульсов (СИ), накапливающий сумматор (НС).

Управление временной задержкой импульсных сигналов играет большую роль в схемотехнике при синхронизации параллельных цифровых потоков в микросхемах программируемой логики, в уменьшении функциональной фазоимпульсной модуляции при цифровом синтезе частот, при измерении временных интервалов, в выравнивании задержек между центральным процессором и схемами оперативной памяти и т. д.

Причем точность установления временных задержек должна составлять единицы – десятки пикосекунд и менее [1]. Поэтому в простейших случаях используют микросхемы с вентилями постоянной калиброванной задержки [2] и микросхемы программируемой калиброванной задержки [3] – рис. 1.

Наиболее простая и очевидная реализация управления задержкой – коммутация соединенных последовательно элементов задержки τ, 2τ, 4τ, 8τ, …[2]. В этом случае к ключам тока (напряжения) предъявляют жесткие требования по величине задержки включения и выключения, а также по величине сопротивления в открытом и закрытом состоянии и стабильности параметров в диапазоне температур. Такой подход реализован в микросхеме *MC*10*EP*195 (*MC*100*EP*195) компании *Motorola*. На рис. 1 приведена схема цифровой реализации коммутируемой УУЗ на этой микросхеме [3].

Задержку можно изменять в широком диапазоне времен – от постоянной задержки переключения (около 2,5 нс) +10 пс до постоянной задержки переключения плюс 10 240 пс с шагом 10 пс при 10-битовом управляющем слове.

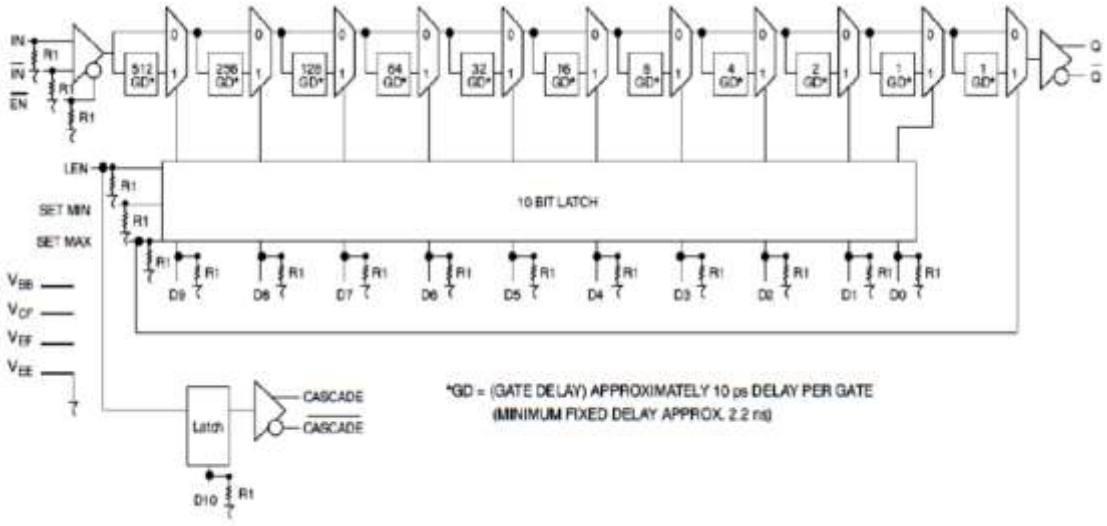


Рис. 1. Структурная схема управляемой задержки на микросхеме *MC*10*EP*195

Анализ приведенной в *Datasheet* информации показывает, что при работе в диапазоне температур необходима термостабилизация микросхемы.

Похожую микросхему *DS*1124 выпускает компания *MAXIM*. При тактовой частоте 125 МГц ее задержка может меняться, как показано на рис. 2 при достаточно малой нелинейности [4].

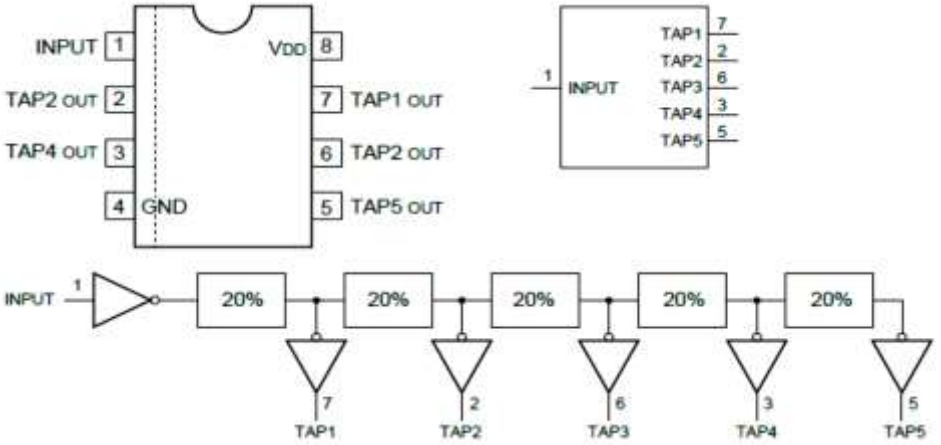


Рис. 2. Микросхема *DS1000*

Выпускают и более простые микросхемы. Например, микросхема *DS*1000 компании *Maxim* (ныне подразделение компании *Analog Devices*) позволяет получить 5 дополнительных каналов с временными сдвигами относительно основного канала, в то время, как микросхема *DS*1110 позволяет получить 10 дополнительных каналов с различными временными сдвигами относительно основного канала [4].

Однако, неточность установки кванта задержки может достигать 20 % длительности единичного интервала, что для пассивного цифрового синтеза недостаточно. Поэтому при динамическом переключении задержек в наносекундном диапазоне времен с высокой точностью задержки внутри интервала интерполяции приходится использовать метод промежуточных преобразований. В этом случае код управления задержкой преобразуется в аналоговый параметр, напряжение или ток, с помощью быстродействующего цифроаналогового преобразователя (ЦАП).

На выходе ЦАП формируется напряжение, пропорциональное коду управления задержкой. Параллельно с этим преобразованием запускается генератор линейно изменяющегося напряжения (генератора пилообразного напряжения) наносекундного диапазона (соответственно, ГЛИН или ГПН).

Запускается ГЛИН активным перепадом того импульса, который надо задержать на требуемое время. Напряжение с выхода ГЛИН и выхода ЦАП подают на входы компаратора напряжений, на выходе которого с точностью постоянной задержки формируется перепад, задержанный относительно входного одноименного перепада на требуемое время. На рис. 3 приведена структура микросхемы управляемого устройства задержки (УУЗ) *AD*9500 [5].

FEATURES
Single +5 V Supply
TTL and CMOS Compatible
10 ps Delay Resolution
2.5 ns to 10 μs Full-Scale Range
Maximum Trigger Rate 50 MHz
MIL-STD-883-Compliant Versions Available

APPLICATIONS
Disk Drive Deskewing
Data Communications
Test Equipment
Radar I & Q Matching

FUNCTIONAL BLOCK DIAGRAM

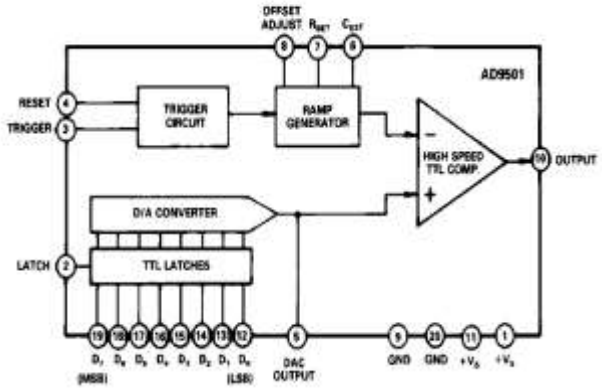


Рис. 3. Структура и основные параметры микросхемы *AD*9500

Основной вклад в неточность (нелинейность) преобразования кода управления во временной интервал вносит ГЛИН наносекундного диапазона, а именно конечное сопротивление генератора стабильного тока и нелинейность вольт-фарадной характеристики барьерной емкости зарядного ключа [6] – рис. 4.

Для правильного функционирования УУЗ в составе широкополосного двухуровневого автомата следует выполнить два условия:

– условие обеспечения диапазонности (требуемой широкополосности)

$$\frac{t_{зk}}{T_0} = \frac{(Q-1)}{Q} - \frac{S_k}{Q} = \frac{X_k}{Q}, \qquad (1)$$

где K_k линейный коэффициент; Q –код выходной частоты.

– условие чистоты спектра (наибольшего подавления функциональной фазоимпульсной модуляции (ФФИМ)

$$K_k = X_k.$$

Управление задержкой переключения можно реализовать с помощью промежуточных преобразований кода текущей задержки X_k в напряжение (ток), а затем во временной интервал.

Для единообразного рассмотрения таких УУЗ, во-первых, унифицируем их структуры таким образом, чтобы они содержали одинаковые элементы: ЦАП, управляемые генераторы тока на основе ЦАП, компараторы напряжения ***K***, безынерционные ключи тока и(или) напряжения и хронирующие емкости $\boldsymbol{C = C_0 + C_{кл} + C_{гст}}$.

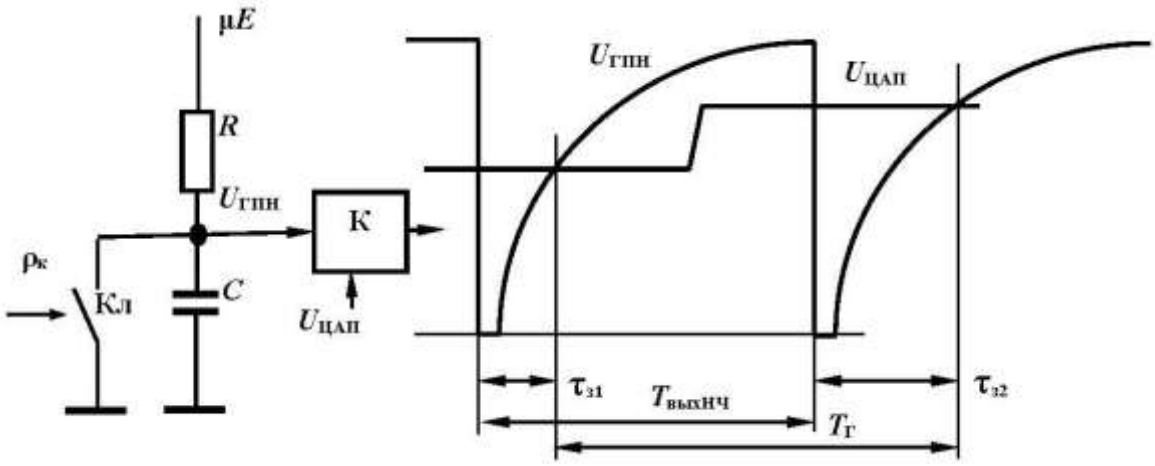


Рис. 4. Упрощенная схема и временные диаграммы работы простейшей УУЗ на основе *RC* генератора пилообразного напряжения и ЦАП

Во-вторых, будем считать, что конечный автомат (КА) вырабатывает код управления X_k в соответствии с (1), т е. X_k содержит полную информацию о величине текущей (мгновенной) фазовой ошибки.

В-третьих, ограничим диапазон синтезируемых частот $f_{выхНЧ} \in F_s\,(Q_{макс} \ldots Q_{мин})$ одной октавой ($Q_{макс} = 2Q_{мин}$) при двоичном управлении Q.

Последнее обстоятельство не сужает общности рассуждений, поскольку расширение диапазона синтезируемых частот «вниз» без изменения режима работы УУЗ легко достигается подключением к выходу УУЗ цепочки триггеров (двоичных счетчиков импульсов – делителей частоты).

Импульс переполнения ρ_k запускает генератор пилообразного напряжения (ГПН) наносекундного диапазона. Пилообразное напряжение с выхода ГПН подается на первый вход компаратора ***К*** (рис. 3). На второй вход компаратора ***К*** поступает напряжение с выхода ЦАП, пропорциональное коду требуемой задержки.

Выход компаратора формирует двухуровневую последовательность импульсов или активных перепадов, которая является квазиравномерной последовательностью, как и на входе, но с новыми параметрами. Если принять, что период интерполяции в УУЗ равен $\tau_0 = T_0/L$, где L – разрядность (число градаций задержки) УУЗ, то эквивалентный коэффициент деления КА увеличится и станет равным

$$N_{ЭКВ} = LP/Q.$$

Задержанный импульс (перепад напряжения) на выходе компаратора ***К*** (рис. 4) появляется при $U_{ЦАП}(X) = U_{ГПН}(t)$, где $U_{ЦАП}(X) = X{\times}E$; $0 \le X < 1$ – код

требуемой задержки; μ >> 1; E – размах напряжения на выходе ЦАП, соответствующий $\tau_з = T_0$; μ E/R – эквивалентное выходное сопротивление генератора стабильного тока.

Таким образом, введение в структуру КА управляемого устройства задержки в линейном приближении эквивалентно увеличению входной частоты f_0 в L раз [6]. Реально достижимый выигрыш составляет 43…48дБ и ограничен рядом факторов – нелинейностью ГПН наносекундного диапазона (рис. 4), конечным быстродействие компаратора и ЦАП.

Список используемых источников

1. Poki Chen, Po-Yu Chen, Juan Lal, Yu-Jin Chen FPGA Vernier Digital-to-Analog Converter With 1,58ps Resolution and 59,3 Minutes Operating Range // IEEE Transactions on Circuits and Systems. 2010. Vol. 59, № 6, pp. 1134–1142.

2. Мовшевич Б. З. Программируемая задержка наносекундного диапазона // Приборы и техника эксперимента. 1980. № 2.

3. 3.3 V ECL Programmable Delay Chip. URL: https://www.onsemi.com/pdf/datasheet/mc100ep195-d.pdf

4. DS1100. 5-Tap Economy Timing Element (Delay Line). URL: https://docs.rs-online.com/edec/0900766b8124d591.pdf

5. https://www.analog.com/media/en/technical-documentation/data-sheets/AD9500.pdf

6. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника: монография. СПб.: Изд-во СПбГУТ, 2018. 367 с.

УДК 621.396.6
ГРНТИ 47.47

МИКРОСХЕМА СИНТЕЗАТОРА ЧАСТОТ *ADF*4158 С ДРОБНЫМ КОЭФФИЦИЕНТОМ ДЕЛЕНИЯ И ФУНКЦИЯМИ ФОРМИРОВАНИЯ СИГНАЛОВ

Ю. А. Никитин[1,2], В. Ю. Смотров[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский филиал ФГУП НИИР-ЛОНИИР

Представлены структура и описание работы микросхемы широкополосного микроволнового синтезатора частот ADF4158, который работает в диапазоне частот от 0.5 ГГц до 6.1 ГГц с управлением по трехпроводному последовательному интерфейсу и позволяет производить программное сканирование по частоте с заданными параметрами по диапазону и времени сканирования.

синтез частот, радиосвязь, спектр, фазовая автоподстройка, фазовые шумы, управление, интерфейс, сигнал, регистр, сканирование.

Умножающие кольца импульсно-фазовой автоподстройки частоты широко используются в радиопередающих и радиоприемных устройствах для формирования сетки частот с заданным шагом, а также сигналов с калиброванной угловой манипуляцией и возможностью сканирования по частоте с заданным шагом на заданном временном интервале [1].

Одной из первых микросхем подобного типа является полностью интегрированный *PLL* синтезатор частот *ADF*4158, который позволяет работать в октавном диапазоне частот с последующим трактом деления [2].

В основе работы цифровой части микросхемы активного синтезатора частот на основе кольца импульсно-фазовой автоподстройки частоты модели *ADF*4158 лежит 25-битный модуль, который позволяет получить разрешение по частоте менее 1 Гц в диапазоне от 0.5 до 6.1 ГГц. Регистры *INT* и *FRAC* определяют общий коэффициент *N*-делителя частоты как $N = INT + (\frac{FRAC}{2^{25}})$. Управление всеми встроенными регистрами осуществляется через трехпроводной интерфейс – рис. 1.

Управляющие сигналы *CLK* (такты), *DATA* (данные), *LE* (разрешение, выбор кристалла) подаются на входы последовательного порта, позволяя настраивать микросхему в соответствии с заданными параметрами работы. Импульсы, подаваемые на входы портов, должны соответствовать требованиям, предъявляемым к стандартной ТТЛ логике. Несоответствие входных параметров будет приводить к задержкам и сбоям в работе микросхемы.

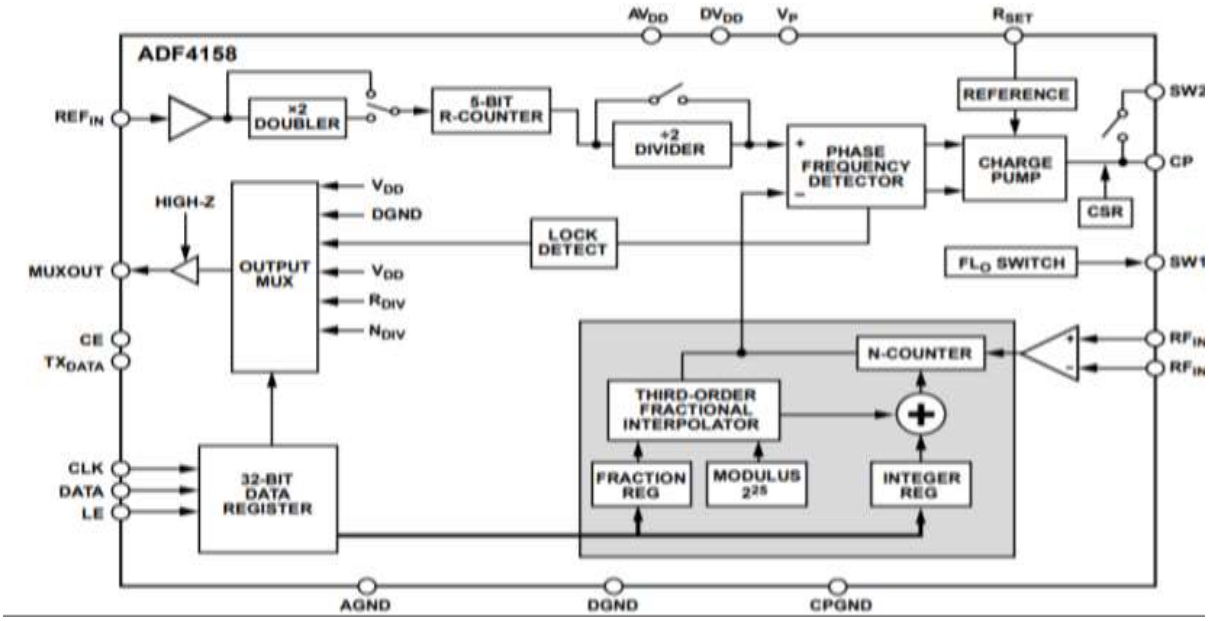


Рис. 1. Структурная схема синтезатора ADF4158

В табл. 1 приведены значения рекомендуемых задержек, которые не должны быть превышены.

ТАБЛИЦА 1. Допустимые задержки по цепям управления

Parameter	Symbol	Test Conditions/Comments	Min	Typ	Max	Unit
Serial Port Interface (SPI) Timing		See Figure 2, Figure 3, and Figure 4				
SCLK Frequency	f_{SCLK}				50	MHz
SCLK Period	t_{SCLK}		20			ns
SCLK Pulse Width High	t_{HIGH}		10			ns
SCLK Pulse Width Low	t_{LOW}		10			ns
SDIO Setup Time	t_{DS}		2			ns
SDIO Hold Time	t_{DH}		2			ns
SCLK Falling Edge to SDIO Valid Propagation Delay	t_{ACCESS}		10			ns
$\overline{CS}$ Rising Edge to SDIO High-Z	t_Z		10			ns
$\overline{CS}$ Fall to SCLK Rise Setup Time	t_S		2			ns
SCLK Fall to $\overline{CS}$ Rise Hold Time	t_H		2			ns

Трехпроводной интерфейс состоит из регистров чтения и записи битов. Для того. чтобы записать информацию в регистр, необходимо подать на вход *LE* логическую единицу, которая разрешает запись. Временная диаграмма для записи информации приведена на рис. 2.

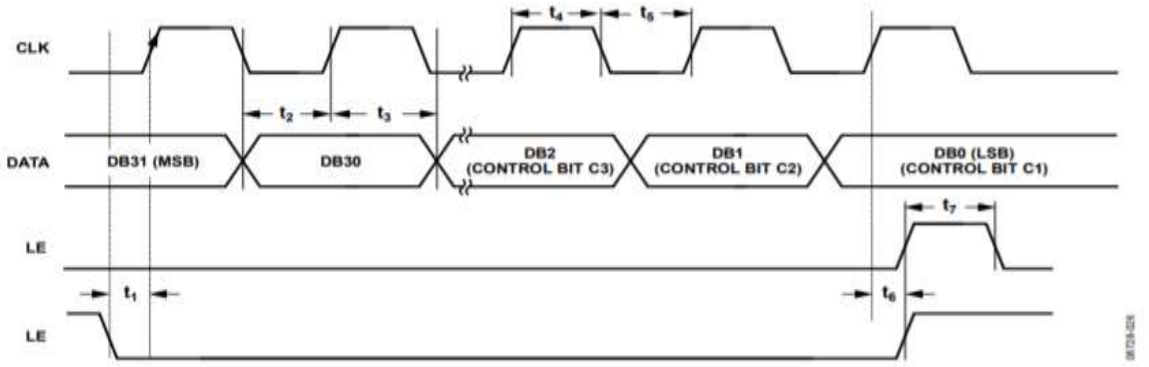


Рис. 2. Временная диаграмма для записи информации в регистры микросхемы

Модуляция сигналов

Микросхема *ADF*4158 может генерировать сигналы, в частотной области, четырех типов.

Тип 1. Одиночный сигнал простой формы. Все остальные сигналы являются его вариациями. Синтезатор синхронизируется с частотой, заданной в регистре *FRAC*, происходит увеличение коэффициента деления *N*, вызывая сдвиг частоты на каждом временном интервале, что приводит к генерации сигнала на рис. 3.

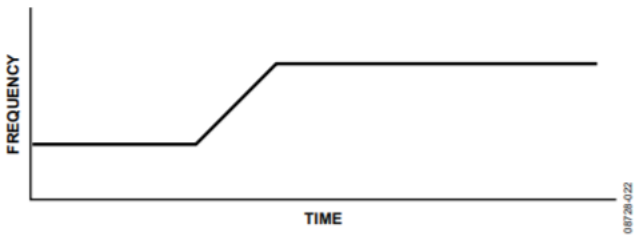


Рис. 3. Одиночный скачок без спада

Тип 2. Одиночный пилообразный сигнал. Генерация происходит так же, как у типа 1, с последующим сбросом коэффициента деления N до первоначального уровня. Форма сигнала представлена на рис. 4.

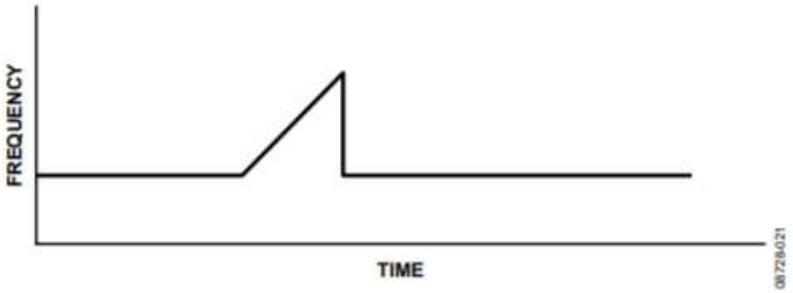


Рис. 4. Одиночный пилообразный скачок

Тип 3. Пилообразный сигнал рис 5. Представляет собой повторяющийся сигнал типа 2. Генерация происходит до тех пор, пока подача данных не будет остановлена.

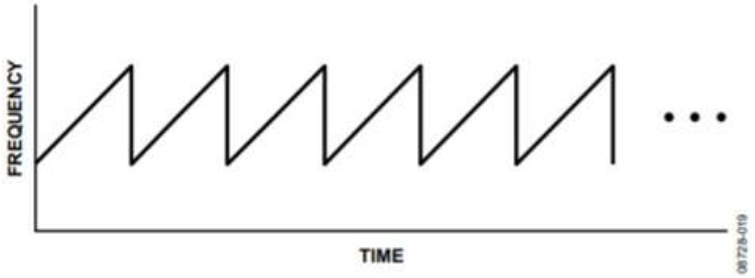


Рис. 5. Пилообразный сигнал

Тип 4. Треугольный сигнал. Генерация происходит за счет того, что синтезатор в начале цикла линейно увеличивает коэффициент деления N до определенного значения, как в типе 1, а затем линейно уменьшает (без резких скачков) до начального значения.

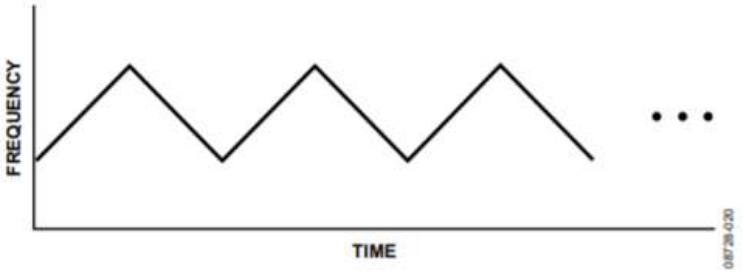
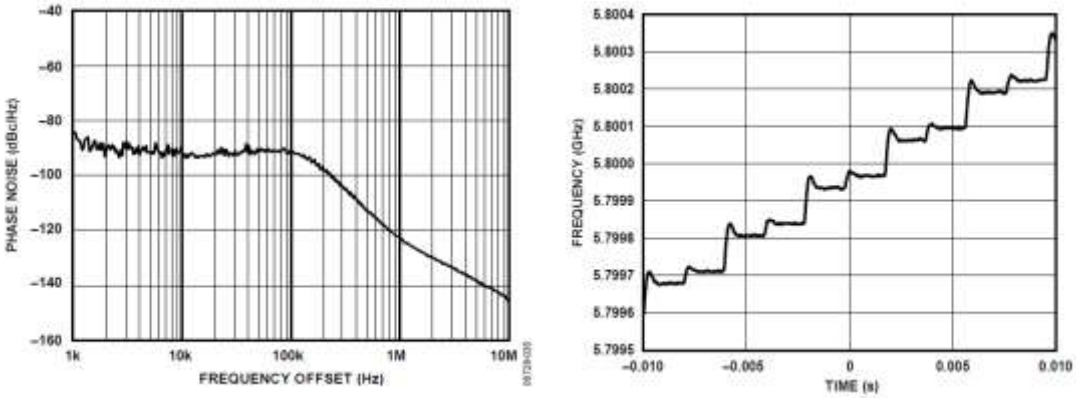


Рис. 6. Сигнал треугольной формы

На рис. 7, а приведено распределение фазовых шумов синтезатора на выходной частоте 5 805 МГц при частоте сравнения 32 МГц и полосе

единичного усиления условно разомкнутого кольца 100 кГц. На рис. 7,б показан результат сканирования по частоте при следующих параметрах кольца ИФАП:

Ramp Settings: PFD = 32 MHz, INT = 181, FRAC = 0, DEV Offset = 4, DEV Word = 20972, Step Word = 200, CLK DIV = 10, CLK_1 Divider = 125; FSK Settings: DEV Offset = 3, DEV Word = 4194



а) б)

Рис. 7. а) относительный уровень фазовых шумов в одной боковой полосе, б) результат программного частотного сканирования

Рассмотренная микросхема позволяет строить синтезаторы частоты в широком диапазоне частот, программно управлять временем и диапазоном сканирования, а также формировать сигналы с угловой модуляцией. Расчет и применение аналогичных синтезаторов рассмотрено в [1, 3].

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника: монография. СПб.: Изд-во СПб ГУТ, 2018. 367 с.

2. https://www.analog.com/media/en/technical-documentation/data-sheets/ADF4158.pdf

3. Ченакин А. В., Горевой А. В. Практическое построение синтезаторов частот СВЧ диапазона. М.: Горячая линия – Телеком, 2021. 280 с.

УДК 53.087.5, 612.15, 621.383.72, 004.048, 004.891.3
ГРНТИ 29.31.26, 29.31.27, 47.33.33, 59.45.37, 76.13.33

ПУТИ ПРОЕКТИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

К. В. Обертий, В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрены современные пути проектирования электронных систем контроля и управления доступом. Проведен анализ технических особенностей реализации системы считывания и идентификации пользователя, предложена концепция для разработки электронной системы контроля и управления доступом на основе считывания биометрических данных пользователя. Рассмотрен способ считывания в виде биометрической идентификации по рисунку вен ладони.

медицинская электроника, оптоэлектроника, диагностическое оборудование, профилактическая медицина, лазерная техника, биомедицина, системы электронного доступа

В современном мире безопасность данных один из самых важных критериев спокойной жизни. Создаётся все больше и больше вариантов систем защиты и контроля доступа к данным: ключи сквозного шифрования, криптографические способы, программные продукты, видеонаблюдение, биометрия и множество других способов как для частных лиц, так и компаний, корпораций и государств, направленные на сохранение информации от рук злоумышленников.

Одним из перспективных и динамично развивающихся направлений проектирования систем безопасности является создание устройств идентификации санкционированных пользователей и электронного контроля доступа (ЭКД), принцип работы которых основан на биометрии, – системе распознавания людей по одной или более физическим или поведенческим чертам.

Существуют различные биометрические данные, отвечающие разным критериям, и тем самым создающие градацию по безопасности от легкой до сложной: трёхмерная фотография лица и/или тела, образец голоса, отпечатки пальцев, рисунок вен руки, группа крови, специальное фото роговицы глаза и т. д. Лидирующей биометрической системой является аутентификация по отпечатку пальца благодаря её доступности, малым форм-фактором. В таких устройствах аналого-цифровая система сканера обрабатывает аналоговый электрический сигнал, который в дальнейшем переводит в цифровое представление данного изображения.

Однако в ряде случаев, обусловленных спецификой работы учреждений, например, стройплощадки, промышленные и пищевые производства, сканирование отпечатка пальца затруднительно, поэтому используются бесконтактные решения, к которым относится распознавание лица. Этот метод стал популярен в смартфонах последнего поколения. В основе технологии лежат две нейросети. Первая – сеть-«выравниватель», в которой с поступающего изображения с камеры наблюдения детектируется лицо или все лица, которые сможет определить система распознавания. Программа выделяет обнаруженные лица (те, что плотно расположены друг к другу, повернуты в профиль или просто очень маленькие и нечеткие). Затем происходит их выравнивание, детектирование на лице точек глаз, носа и рта (рис. 1) [1].

Вторая подсистема нейросети – «распознаватель», которая принимает на входе выровненное изображение, переданное из первой нейросети, а на выходе выдает вектор лица – то есть, набор чисел фиксированной длины. У разных сетей эти векторы могут отличаться, но чаще всего это некая степень двойки. Например, 512.

Рис. 1. Программа приводит фото к стандартному виду

На похожие лица сеть выдает похожие векторы и наоборот (рис. 2) [1].

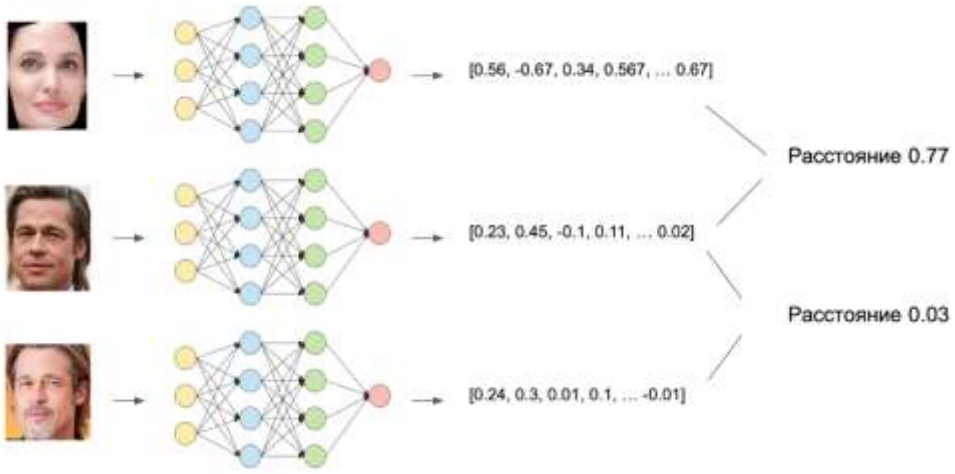


Рис. 2. Принцип работы подсистемы нейросети распознавания человеческого лица

Одним из новейших способов защиты данных и являющийся на данный момент самым надежным является использование в качестве биометрического маркера рисунок вен ладони. Этот метод является самым безопасным из-за уникальности рисунка вен ладони человека, который тяжело украсть и практически нельзя подделать.

Метод считывания рисунка вен основан на явлении поглощения ИК излучения гемоглобином, который находится в крови человека (рис. 3) [2–3]. Специальная программа на основе полученных данных создает цифровую свертку. Сравнивает ее в базе данных с фрагментом предварительно снятого рисунка, который дополнительно зашифрован программой в код для повышения уровня безопасности. На данный момент существует два варианта создания подобного прибора.

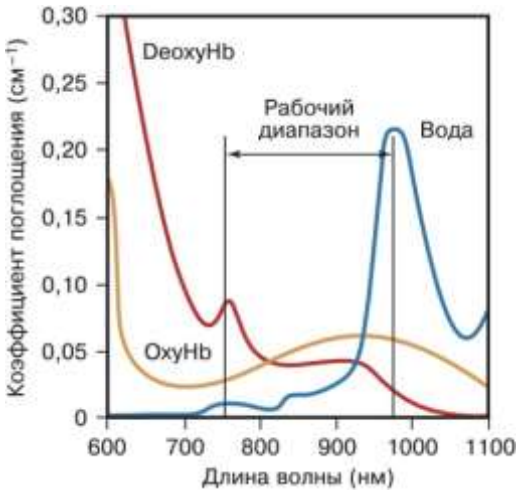


Рис. 3. Графическая зависимость коэффициента поглощения излучения ИК диапазона насыщенной кислородом крови (OxyHb) и крови без кислорода (DeoxyHb), воды [1]

Метод отражения (*reflection*) позволяет разместить все компоненты устройства в одном корпусе, за счет чего уменьшается размер, рука прикладывается к оптической части прибора [4].

Метод пропускания излучения (*transmission*) заключается в установке ИК-подсветки с тыльной стороны ладони, а сама камера с фильтром устанавливается со стороны ладони и принимает ИК-излучение, проходящее через всю ладонь. С помощью метода пропускания получаемые изображения более детализированные. Само устройство представляет собой прибор в корпусе, которого находится камера с ИК-фильтром и ИК-термометром. Между ладонью идентифицируемого и матрицей самого устройства должно измеряться расстояние и температура. Отраженный свет от гемоглобина попадает на светочувствительную матрицу и воспроизводится в виде черно-белого рисунка. Однако этот метод аутентификации не нашел широкого применения во встроенных системах с ограниченными ресурсами. В [5] авторы представили систему, реализованную на ПЛИС *AlteraNios* II, работающей в операционной системе реального времени (*RTOS)Nios2-Linux*. Алгоритмы обработки изображений выполняются во встроенной системе с процессором с фиксированной частотой 50 МГц.

Такое устройство считывания биометрических можно условно разделить на три основных функциональных модуля.

Модуль сбора изображений

Массив инфракрасных светодиодов (*LED*) и тепловизионная камера, модифицированная из веб-камеры, использовалась для захвата рисунка вен в проектируемой системе. Подсветив лучом инфракрасного света тыльную сторону руки, можно зафиксировать рисунок вен на тыльной стороне руки, с помощью модифицированной веб-камеры с прикрепленным ИК-фильтром. Поскольку гемоглобин в крови хорошо поглощает ИК-излучение, на полученных изображениях узоры вен отображаются как тени и кажутся темнее. На рис. 4, *а* - *е* показан пример инфракрасного изображения вен на тыльной стороне ладони, полученного системой [5]. Изображение захватывается в цветном формате *jpeg*, шириной 320 пикселей и высотой 240 пикселей, с 24 битами на пиксель.

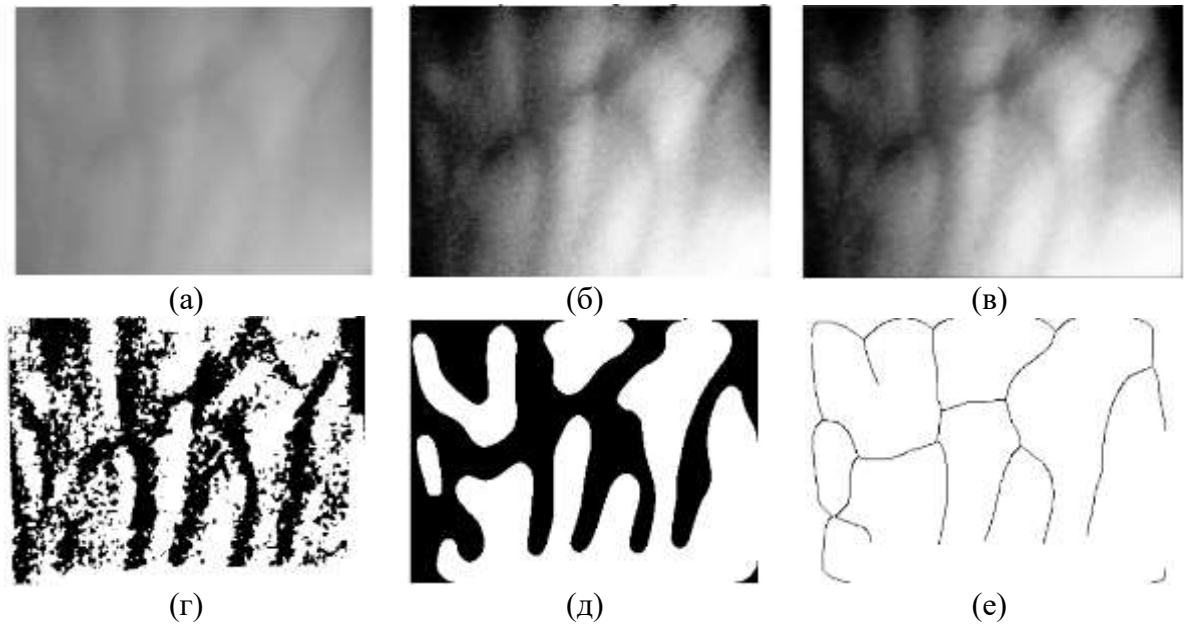


Рис. 4. Рисунок вен в процессе считывания и обработки изображения:
а) изображение в градациях серого; б) выравнивание гистограммы; в) ФНЧ;
г) бинаризация; д) медианный фильтр; е) выделение текстуры

Модуль обработки изображений

Здесь полученное модулем сбора изображение преобразуется в градации серого, путём уменьшения разрядности с 24 бит на пиксель (цветное изображение) до 8 бит на пиксель (рис. 4, *а*).

Захваченное изображение вены имеет низкий контраст, из-за чего рисунок вены не четко отличим от окружающих тканей. Поэтому применяется выравнивание гистограммы к изображению вен для улучшения контраста (рис. 4, б), в результате чего темные пиксели становятся более темными, а светлые – более светлыми.

Далее к изображению применяется фильтр нижних частот, чтобы сгладить резкие переходы уровней серого и удалить высокочастотный шум после выравнивания гистограммы (рис. 4, *в*).

Затем изображение преобразуется с использованием метода бинаризации, т. е. преобразования изображения в градациях серого в двухуровневое представление: черный с пикселем «0» и белый с пикселем «255». В результате из изображения извлекается рисунок вены (рис. 4, *г*).

Изображение вен после бинаризации содержит шумы. Устранение шума можно осуществить путем применения к изображению медианного фильтра (рис. 4, *д*). Итогом преобразований является получение «скелетного» изображения текстуры жилок, состоящее только из текстуры шириной в один пиксель (рис. 4, *е*).

Модуль извлечения признаков

Технология выделения признаков использует мелкие детали, извлеченные из рисунков жилок для распознавания. Признаки включают точки бифуркации и конечные точки. Подобно отпечаткам пальцев, эти характерные точки используются в качестве геометрического представления формы узоров вен. Полученное изображение обрабатывается и сопоставляется с базой данной для идентификации пользователя.

В ходе работы были проанализированы основные функциональные блоки и требования к ним с целью создания биометрической системы ЭКД на основе работы ИК-сканера и сверхчувствительной матрицы, которые выдают четкий рисунок вен. Оптическую приемную часть проектируемого устройства также возможно будет использовать в качестве медицинского сканера для проверки восстановления кровообращения в кистях рук при проведении операций в травматологии и трансплантации.

Список используемых источников

1. Поисковая система изображений. URL: https://yandex.ru/images/ (дата обращения: 13.03.2022).

2. Джемисон Д. Э. Физика и техника инфракрасного излучения. Рипол Классик, 2013. 646 с.

3. Лысенко С. А., Кугейко М. М. Метод неинвазивного определения содержания гемоглобина в биологических тканях // Журнал прикладной спектроскопии. 2012. Т. 79. №. 4. С. 651–657.

4. Стратонников А. А. и др. Использование спектроскопии обратного диффузного отражения света для мониторинга состояния тканей при фотодинамической терапии // Квантовая электроника. 2006. Т. 36. № 12. С. 1103 – 1110.

5. Eng P. C. and Khalil-Hani M., ”FPGA-based embedded hand vein biometric authentication system” // TENCON 2009 IEEE Region 10 Conference. 2009. No. 79900. pp. 1–5.

УДК 621.385.69
ГРНТИ 47.45.99

КВАЗИСОСРЕДОТОЧЕННЫЙ LC-КОНТУР В ГИБРИДНОМ ИСПОЛНЕНИИ ДЛЯ СВЧ УСТРОЙСТВ

А. М. Румянцева, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе описан сложный интегральный элемент – «гибрид» спиральной индуктивности и круглой планарной емкости. Представлен расчет основных геометрических и электрических параметров LC-конструкции. Предложены некоторые варианты использования «гибрида» в интегральных схемах с дальнейшим макетированием. Экспериментально исследована работа гибрида в различных функциональных устройствах.

интегральные схемы, сверхвысокие частоты, плоская спиральная индуктивность, круглая планарная емкость.

В предыдущих работах [1, 2] представлены исследования, где подробно рассматривались плоские спиральные индуктивности и пленочные конденсаторы интегральных схем (ИС) СВЧ различной формы. Данные конструктивные элементы широко используются при реализации принципиальных схем устройств, а также для увеличения степени интеграции ИС СВЧ. Довольно часто в ИС СВЧ можно встретить последовательное соединение емкости и индуктивности, при таком включении возникает ряд технологических неоднородностей (перемычки, изломы), которые затрудняют синтез требуемых рабочих параметров. Для уменьшения зависимости передаточной характеристики от паразитных параметров последовательного контура был предложен «гибрид» индуктивности и емкости. Данное устройство представляет собой объединение круглой емкости на землю и огибающей ее индуктивности. Очевидно, что номиналы таких элементов ограничены формой конструкции и зависят друг от друга.

В расчете круглой спиральной индуктивности использовалась квазистатическая формула (1), проверенная нами с помощью квазидинамического приближения в нижней части СВЧ диапазона [3, 4].

$$L = 2.475 \cdot D_{cp} \cdot \sqrt[3]{N^5} \cdot \lg f_0\left(\frac{4 \cdot D_{cp}}{b}\right), \qquad (1)$$

где N – число витков, $R2$ – внешний радиус, $R1$ – внутренний радиус, $b = R2 - R1$ – ширина катушки, $D_{ср} = R2 + R1$ – средний диаметр.

По результатам исследования трех видов планарных емкостей выбираем планарный конденсатор в форме круга, показавший наилучшее значение КСВН, при параллельном включении в линию передачи. Его номинал рассчитывается по формуле пленочного конденсатора (2).

$$C = \frac{\varepsilon\,\varepsilon_0}{d} \cdot \pi(R1 - t) \qquad (2)$$

где d – толщина диэлектрика, t – расстояние между емкостью и спиралью, ε_0 – электрическая постоянная вакуума ($\varepsilon_0 = 8{,}854 \cdot 10^{-12}$ Ф/м), ε – относительная диэлектрическая проницаемость материала диэлектрика.

Для анализа работы квазисосредоточенного LC-контура в гибридном исполнении был изготовлен макет, содержащий плоскую спиральную индуктивность и круглую планарную емкость (рис. 1, 2). Полученные значения элементов составили 4,8 нГн и 3,7 пФ.

При измерении номиналов элементов на нулевой частоте мы получили существенные расхождения значений номиналов (до 50 %).

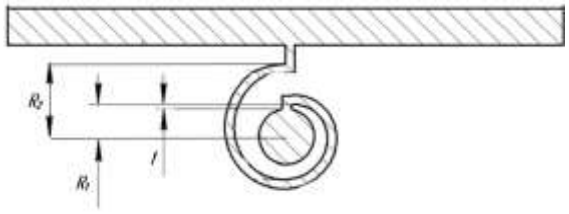


Рис. 1. Эпюр LC-контура в гибридном исполнении

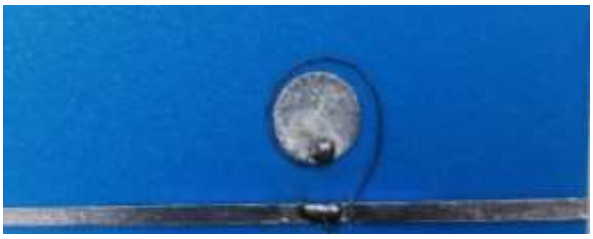


Рис. 2. Макет исследуемого устройства

Исследование работы LC-схемы производилось эмуляцией ее работы в программе RFSimm, а также снятием частотных характеристик макета на векторном анализаторе цепи. На рис. 3 представлена принципиальная схема макета.

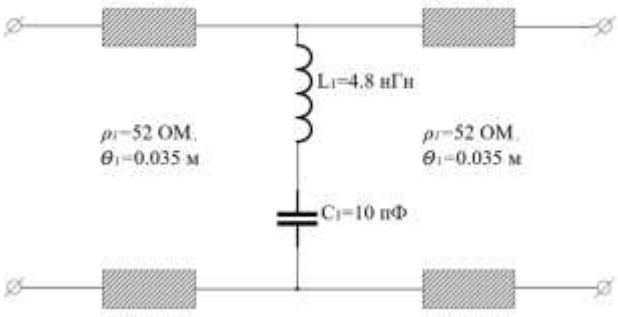


Рис. 3. Принципиальная схема исследуемого LC-контура

В результате проведённых эксперимента и эмуляции получаем частотные характеристики макета, представленные на рис. 4 и 5.

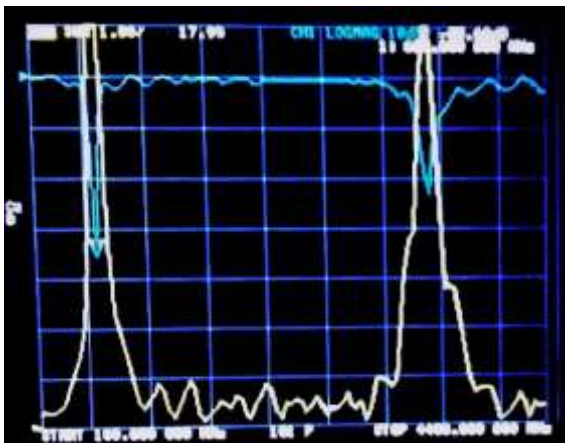


Рис. 4. Частотная характеристика макета, полученная в эксперименте

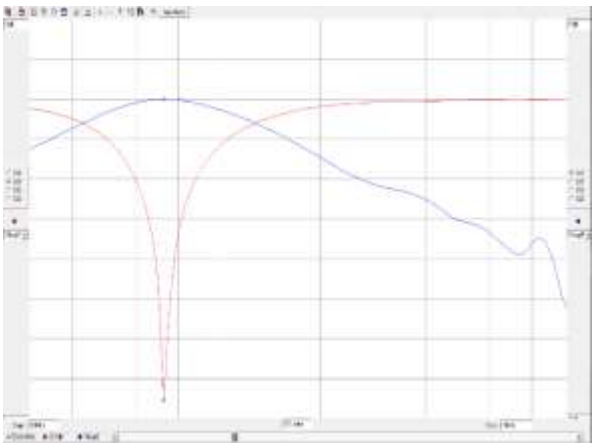


Рис. 5. Частотная характеристика макета в программе RFSimm

Резонансная частота LC-контура (f) рассчитывается по формуле (3).

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{3}$$

Сравнение расчетных результатов и результатов, полученных в эксперименте и эмуляции, представлены в таблице 1.

ТАБЛИЦА 1. Полученные результаты

Расчетный результат	Результат, полученный при эмуляции в САПР	Результат эксперимента
$f = 728\ МГц$	$f = 720\ МГц$	$f_1 = 616\ МГц$, $f_2 = 3{,}4\ ГГц$

Эксперимент показал две резонансные частоты, подобный характер работы цепи говорит о наличии распределенного характера элементов.

В силу низкой разрешающей способности аппликационного метода и наличия паразитных параметров, полученные теоретические результаты совпали с экспериментом с разницей порядка 100 МГц. Резонансный характер цепи и удобство компоновки подтверждены полностью.

С помощью данной цепи получается более высокая степень интеграции и отсутствие перемычки с центральной площадкой индуктивности, эффективно заполнятся пространство при проектировании топологии конструктивных элементов. Данное устройство можно использовать для синтеза согласующих цепей (рис. 6), фильтров, частотно задающих цепей генераторов.

Приведем в качестве примера оригинальную конструкцию LC-генератора на гибридном элементе. Принципиальная схема, чертеж и макет данной структуры представлены на рис. 7.

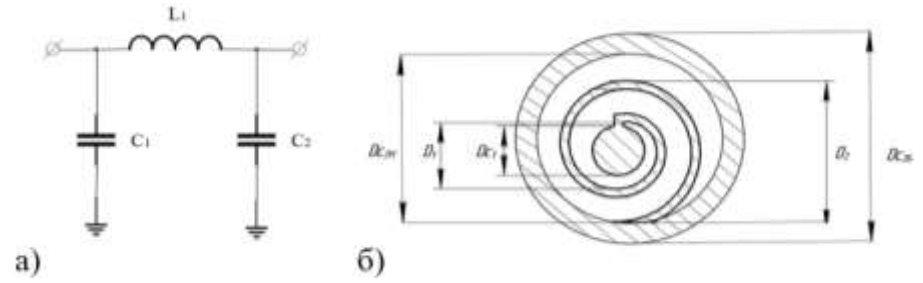


Рис. 6. Согласующая цепь: а) принципиальная схема, б) чертеж

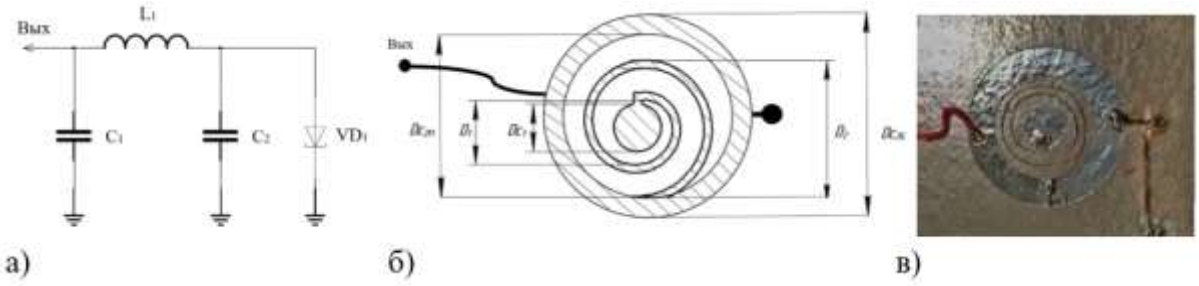


Рис. 7. LC-генератор: а) принципиальная схема, б) чертеж, в) макет

Вывод: предложенная конструктивная компоновка емкости и индуктивности позволяет разработчикам ИС СВЧ повысить степень интеграции схемы, а также избежать установки дополнительных навесных элементов при реализации последовательного контура.

Список используемых источников

1. Румянцева А. М., Седышев Э. Ю. Точный синтез планарных индуктивностей интегральных схем СВЧ // сб. док. X всероссийской научно-технической конференции "Электроника и микроэлектроника СВЧ"., Санкт-Петербург, 31 мая – 4 июня 2021 г. СПб.: СПбГЭТУ «ЛЭТИ», 2021. С. 449–452.

2. Румянцева А. М., Седышев Э. Ю. Исследование конструкций планарных емкостей в интегральных схемах СВЧ // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всероссийская научно-методическая конференция магистрантов и их руководителей. Сб. лучших докладов конференции. СПб. : СПбГУТ, 2022. С. 140–143.

3. Бочаров Е. И., Румянцева А. М., Седышев Э. Ю. Сравнение методов расчета конструктивных индуктивностей интегральных схем СВЧ // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей. Сб. лучших докладов конф. СПб.: СПбГУТ, 2021. С. 330–334.

4. Румянцева А. М., Седышев Э. Ю. Точный синтез конструктивных индуктивностей интегральных схем СВЧ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная международная научно-техническая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 552–557.

УДК 621.375.026
ГРНТИ 47.41.33

РЕАЛИЗАЦИЯ МОДЕЛИ СВЧ УСИЛИТЕЛЯ ДОГЕРТИ С УЧЁТОМ РЕАЛЬНЫХ ПАРАМЕТРОВ ТРАНЗИСТОРА

Э. Сурков, В. А. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описан механизм работы усилителя мощности по схеме У. Догерти. Создана модель для настройки режимов транзисторов в программе Fastmean с использованием кусочно-линейной схемы замещения мощных GaN-транзисторов. Произведена настройка и проверка режимов работы усилителей.

усилитель мощности, Догерти, Fastmean. транзисторный СВЧ усилитель, усилитель класса AB, усилитель класса C.

В середине XX-ого века Уильямом Догерти была предложена схема лампового усилителя мощности амплитудно-модулированного (АМ) сигнала, позволяющая повысить КПД избегая существенных искажений сигнала на выходе. В течении последних десяти лет с ростом исследований и разработок в области интегральных усилителей мощности СВЧ диапазона, вновь проявляется повышенный интерес к энергетически эффективным схемотехническим решениям. В данной работе выполняется настройка одного из фрагментов усилителя и представлен возможный вариант принципиальной схемы всего устройства.

Идея усилителя заключается в построении двух каналов усиления: основного усилителя класса *AB* и вспомогательного усилителя класса *C*. Этим достигается «дополнение» формы выходного сигнала усилителем *C* (далее пиковым) при увеличении амплитуды сигнала и приближении усилителя *AB* (далее основного) к режиму насыщения, тем самым сохраняя форму сигнала на выходе неискажённой. Также данный усилитель отличен тем, что ветви усилителя работают не перегружая друг друга. Это значит, что при работе основного канала, ветвь вспомогательного усилителя разомкнута. На рис. 1 представлена структурная схема данного устройства, содержащая помимо самих усилителей несколько важных для её корректной работы элементов [1].

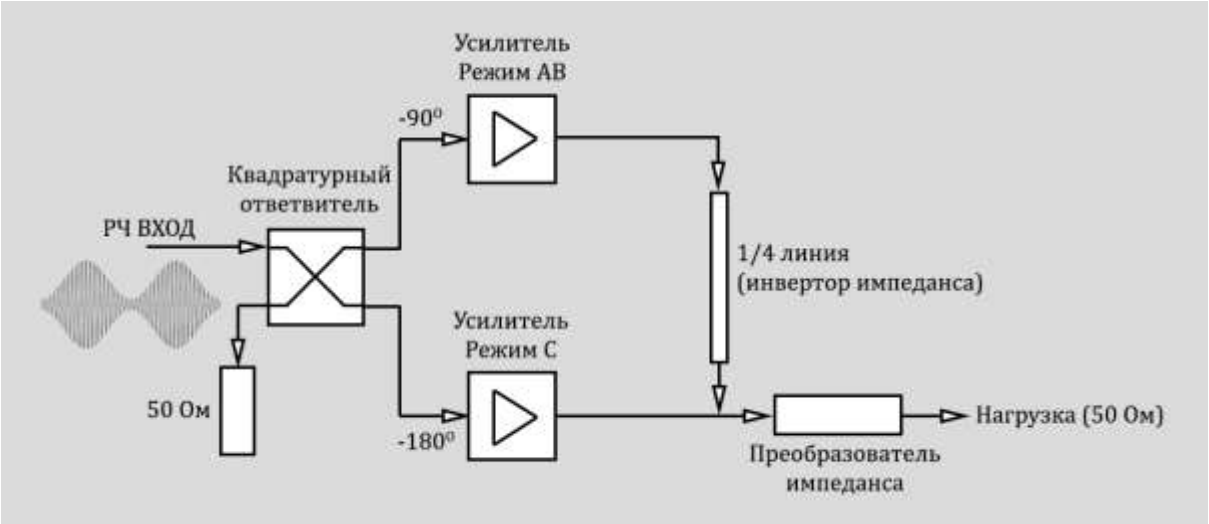


Рис. 1. Структурная схема усилителя Догерти

Для настройки и проверки работы каждого из усилителей была создана модель (рис. 2) в программе Fastmean [2].

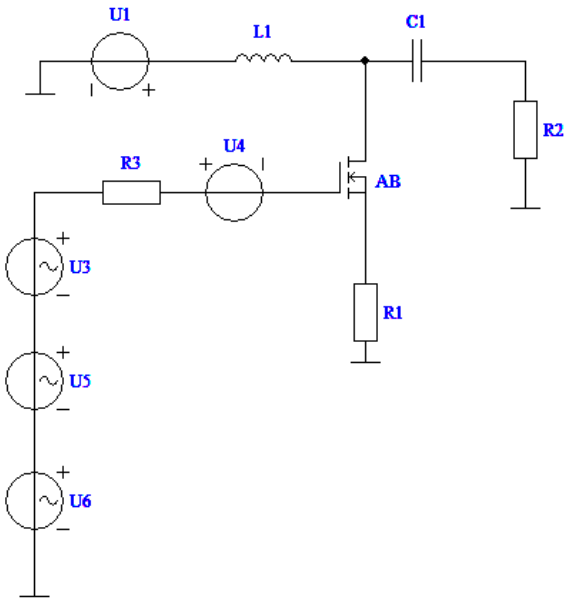


Рис. 2. Схема для настройки и проверки корректности работы усилительного каскада в режимах АВ и С

На вход данной модели подаётся АМ сигнал с центральной частотой 500 МГц, и боковыми частотами 480 и 520 МГц соответственно.

В качестве транзистора используется кусочно-линейная модель нитрид-галлиевого (GaN) полевого транзистора (рис. 3), способная воспроизводить режимы отсечки, насыщения и активный режим [3].

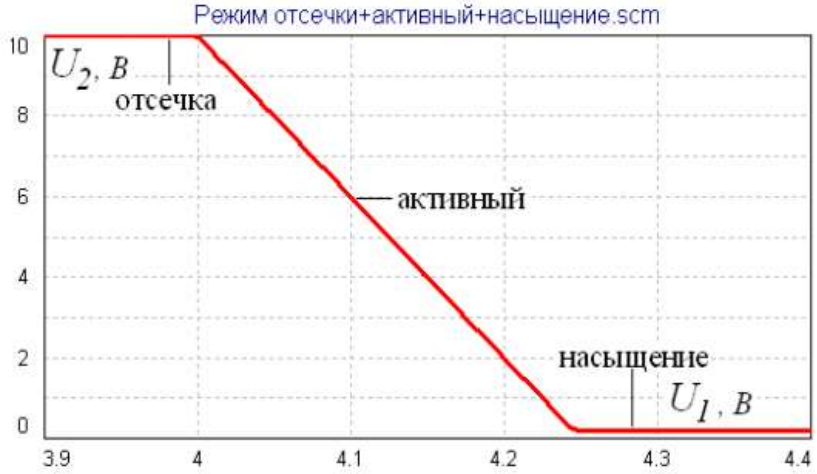


Рис. 3. Статическая передаточная характеристика типового GaN-транзистора

В качестве параметров транзистора были использованы данные из технической документации полевого GaN HEMT транзистора фирмы Wolfspeed [4]. По заявлению разработчиков модель CGH40025 (рис. 4) является достаточно универсальным решением для синтеза разнообразных усилителей, это доказывает распространённость данной модели в сфере разработки СВЧ усилителей мощности.

Рис. 4. Описание и внешний вид GaN HEMT CGH40025

В ходе настройки были выбраны напряжения смещения для обеспечения нужного угла отсечки для каждого из режимов работы транзистора. При этом для проверки корректности работы режима, было произведено изменение глубины модуляции на входе схемы и зафиксирована глубина модуляции на выходе (рис. 5).

Установки источников **500 ± 20 МГц**	Центральная	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4
	Боковые	0,15	0,125	0,1	0,075	0,05	0,04	0,03	0,02	0,01
Амплитуды огибающей сигнала **ВХОДНОГО**	Amax	0,694	0,628	0,585	0,533	0,484	0,476	0,454	0,433	0,409
	Amin	0,0995	0,147	0,195	0,244	0,293	0,313	0,33	0,355	0,375
Спектральный состав сигнала **на нагрузке**	520 МГц	5,609	4,749	3,823	2,864	1,892	1,501	1,106	0,716	0,35
	500 МГц	17,388	17,824	18,187	18,514	19,819	18,934	19,04	19,12	19,165
	480 МГц	5,627	4,765	3,836	2,873	1,899	1,506	1,11	0,718	0,352
Амплитуды огибающей сигнала **НА НАГРУЗКЕ**	Amax	28,609	26,913	25,44	23,873	23,24	21,88	20,92	20,23	19,557
	Amin	6,202	8,33	10,29	12,73	15,94	15,83	16,72	17,569	18,466
КПД	Pнагр	3,954	3,924	3,828	3,793	3,748	3,781	3,819	3,82	3,836
	Pист	10,435	10,34	10,26	10,217	10,064	10,01	9,986	9,961	9,951
	КПД	37,89	37,95	37,31	37,12	37,24	37,77	38,24	38,35	38,55
Глубина модуляции сигнала на входе %		74,9	62,1	50,0	37,2	24,6	20,7	15,8	9,9	4,3
Глубина модуляции сигнала на выходе %		64,4	52,7	42,4	30,4	18,6	16,0	11,2	7,0	2,9

Рис. 5. Таблица проверки корректности работы режима усилителя

По результатам был построен график зависимости глубины модуляции на выходе от входной (рис. 6).

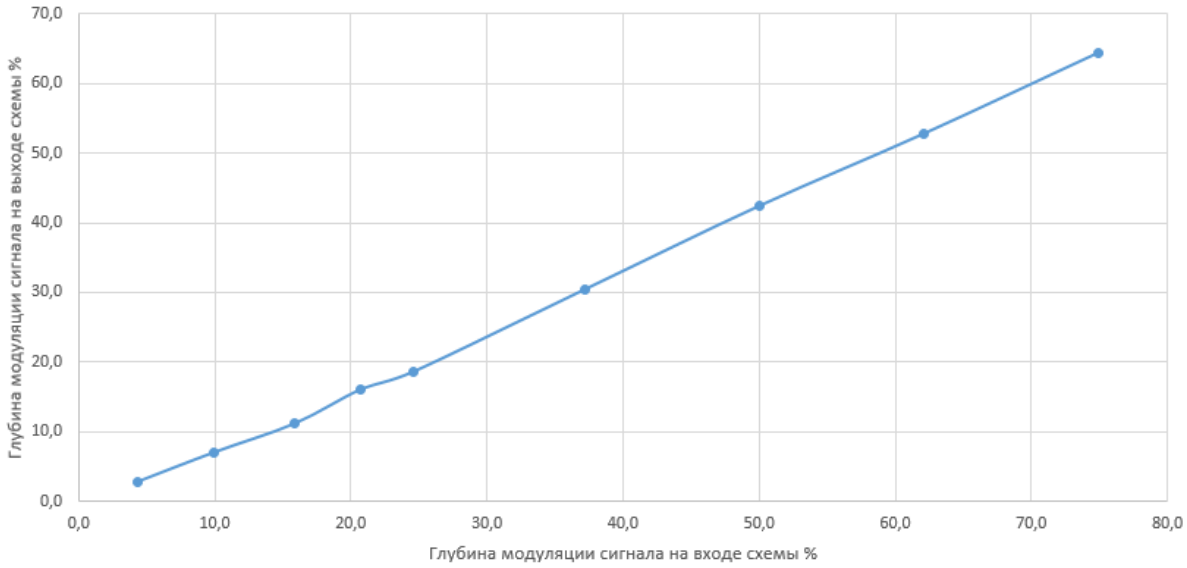


Рис. 6. График зависимости глубины модуляции сигнала на нагрузке, от глубины модуляции сигнала на входе схемы

Линейность данной зависимости свидетельствует о корректно работающей модели. Следовательно, следующим этапом является интеграция данной схемы в общую модель всего устройства, которая будет содержать остальные элементы усилителя мощности (рис. 7).

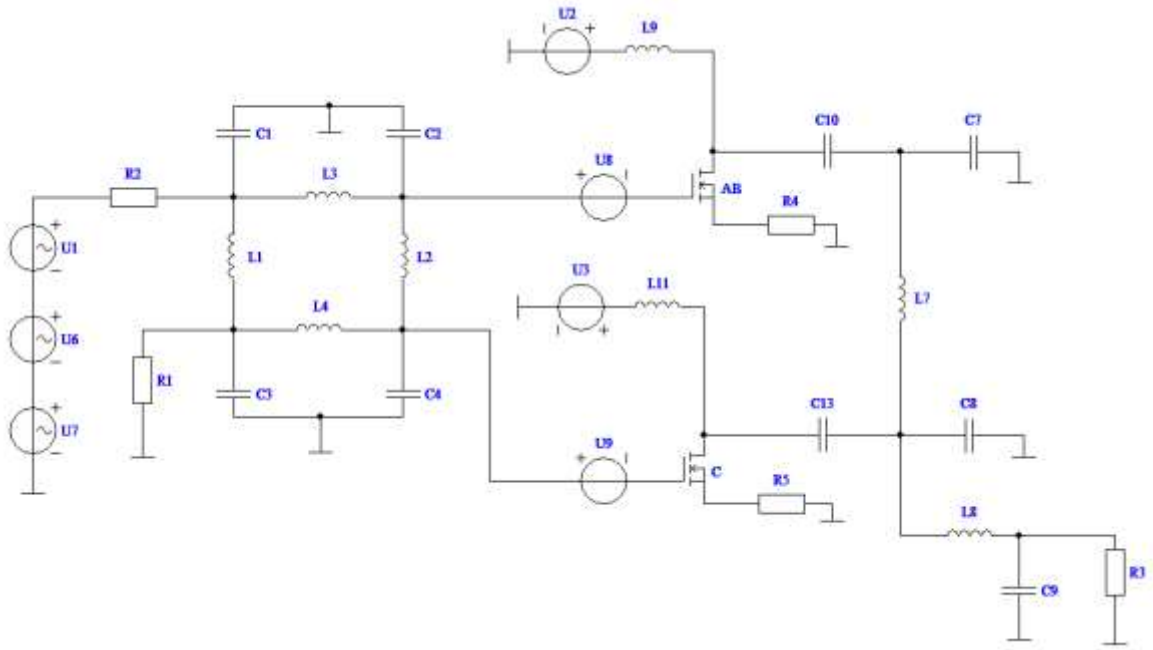


Рис. 7. Общая принципиальная схема усилителя мощности

На рис. 7 отсутствуют требуемые фильтры гармоник, а также стоит обратить внимание, что в представленной схеме в качестве делителя сигнала на входе устройства использовался квадратурный мост. Данное решение является “классическим” и одним из возможных. В рамках проекта был создан и исследован предложенный вариант делителя. Согласно полученным результатам следует провести ряд испытаний схемы с альтернативными вариантами деления с целью повышения уровня развязки по выходу делителя.

Список используемых источников

1. Slade B. The Basics of the Doherty Amplifier. URL: https://www.researchgate.net/publication/259583529 (дата обращения: 10.01.2022)

2. FASTMEAN. URL: https://www.fastmean.ru (дата обращения: 10.01.2022)

3. Ганбаев А. А., Филин В. А. Упрощенная динамическая модель мощных полевых транзисторов для исследования ключевых режимов радиочастотных устройств // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 66–75.

4. Wolfspeed. URL: https://www.wolfspeed.com/cgh40025 (дата обращения: 10.01.2022)

УДК 539.231, 621.383, 53.087
ГРНТИ 29.19.03, 29.19.31, 29.19.16

ОПТИМИЗАЦИЯ РЕЖИМОВ ВАКУУМНОГО НАПЫЛЕНИЯ НА СТРУКТУРАХ НИТРИДА ГАЛЛИЯ

В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Светодиодная техника в настоящее время широко распространена в различных областях электроники. Основные характеристики светодиодной структуры определяются свойствами материалов и особенностью её изготовления. В работе представлены результаты оптимизации технологического процесса формирования омических контактов светодиодной структуры на основе нитрида галлия.

светодиод, полупроводник, МДП-структура, оптоэлектроника, полупроводниковая технология, тонкопленочные технологии.

Для получения светодиодов (СИД) синего света используют, как правило, нитрид галлия и твердые растворы на его основе.

Однако основной проблемой существующих на данный момент гетероструктур на основе нитридов элементов III группы является проблема поддержания приемлемой однородности плотности тока накачки по площади излучающего *p*-*n*-перехода, т. к. проводимость тонкого (4–5 мкм) слоя *n*-GaN недостаточно высока для ее обеспечения, а требуемый диапазон рабочих токов составляет несколько ампер [1–3].

Для решения изложенных задач и создания мощных СИД наиболее перспективной представляется флип-чип конструкция излучающего кристалла, в которой обе контактные площадки к материалу *n*- и *p*-типа проводимости расположены с одной (лицевой) стороны и кристалл монтируется на теплоотвод лицевой стороной. Конструкция светодиода, выполненного по этой технологии представлена на рис. 1. При этом в качестве контакта к GaN используется комбинация металлов с высокой отражающей способностью и по возможности линейной ВАХ, а свет выводится через прозрачную сапфировую подложку.

Параметры светодиодов зависят от многих причин, в частности от качества контактов [1, 3–4]. В связи с этим в данной работе исследовались технологические условия нанесения контактных слоев, и проводилась оценка влияния свойств контактов на электрические и оптические характеристики светодиодной структуры в целом.

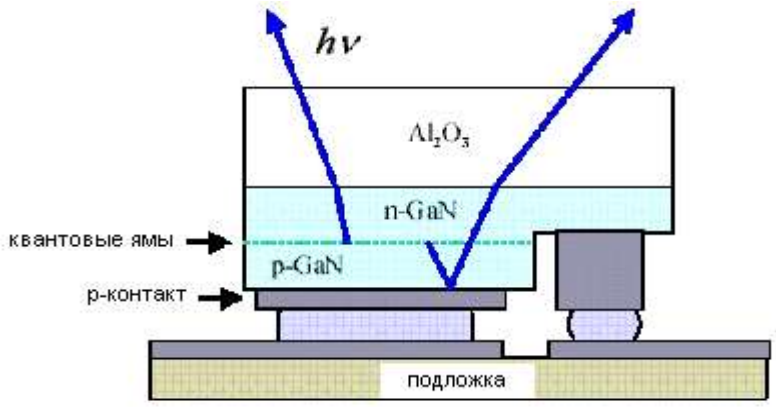


Рис. 1. Структурная схема типовой флип-чип конструкции светоизлучающего диода

Целью работы было изготовление омического контакта, который должен был отвечать следующим требованиям:

1) невыпрямляющий (т. е. создает обогащенный слой ПП; малое сопротивление приконтактной области ПП по сравлению с сопротивлением объема ПП);

2) малое сопротивление;

3) высокая механическая прочность;

4) высокая отражающая способность;

5) высокий квантовый выход получаемой структуры.

Контактные материалы выбирались на основании теории контактных явлений.

Для получения высококачественных контактов светодиодных структур необходимо обеспечить хорошую чистоту исходных материалов и получаемых пленок, высокий вакуум. Этим требованиям удовлетворяет метод термического вакуумного напыления, испарение материалов при котором осуществляется с помощью электронно-лучевого нагрева. В настоящей работе для напыления контактных материалов использовалась установка Temescal FC-1800 компании BOC Edwards (рис. 2).

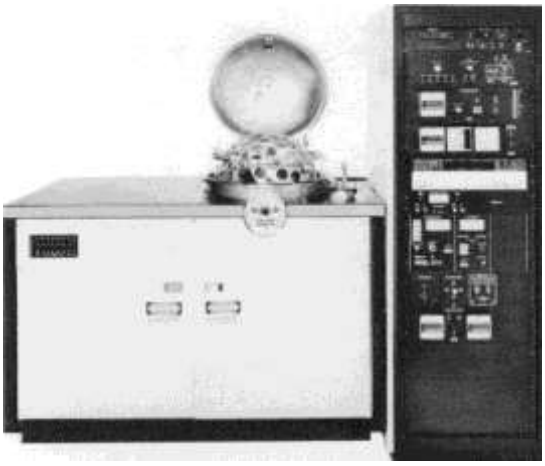


Рис. 2. Напылительная установка Temescal FC-1800

В работе проводили исследование влияния толщины слоя никеля на характеристики светодиода. В результате, которого выяснили, что самый высокий квант при наличии достаточно хорошей адгезии наблюдается у образца № 4 с толщиной слоя никеля 1,5 нм.

ТАБЛИЦА 1. Данные эксперимента по оценки влияния толщины слоя никеля на характеристики *p*-контакта

№ образца	Толщина слоя никеля, нм	Адгезия, балл	$R_{дин}$, Ом	Квантовый выход, %	$U_{пр}$, В	
					50 мА	100 мА
1	4,5	9	1,80	8,36	2,96	3,05
2	3,0	8	1,84	8,70	2,96	3,05
3	2,0	7	2,00	9,84	2,97	3,07
4	1,5	6 – 7	2,14	10,74	2,93	3,01
5	1,0	6	2,40	9,21	3,03	3,15

Произведено напыление *p*-контакта с различной толщиной верхнего слоя титана при температуре нагрева подложек 265ºС, величина остаточного давления составляла $3{,}8 \cdot 10^{-6}$ мм ртутного столба. Исследование проводилось для оценки влияния на электрооптические характеристики светодиодного элемента, потому что слой титана очень важен при пайке, т.к. служит барьером, ограничивая уход золота в ПОС (припой оловянно-свинцовый). При стандартном процессе напыления толщина верхнего слоя титана составляет 150 нм. Из результатов эксперимента, приведенных в таблице 2, следует, что влияние толщины верхнего слоя титана практически не сказывается на электрооптических параметрах светодиодного элемента.

ТАБЛИЦА 2. Данные экспериментов с различной толщиной верхнего слоя титана при напылении *p*-контакта

№ образца	Толщина слоя титана, нм	Квантовый выход, %	$R_{дин}$, Ом
1	15	4,09	1,8
	10	4,09	1,9
2	15	3,22	1,4
	30	3,63	1,6

Также была проведена оценка влияния скорости напыления слоя никеля при создании *p*-контакта. На трех участках образца произведено напыление *p*-контакта со скоростью напыления никеля 0,1; 0,2; 0,3 нм/сек. Основными показателями являются динамическое сопротивление $R_{дин}$ и внешний квантовый выход на длине волны излучения $\lambda = 460$ нм. Так как слой никеля определяет отражающие свойства контакта и оказывает влияние на электрические свойства светодиодной структуры. Результаты эксперимента по скорости напыления никеля приведены в таблице 3.

ТАБЛИЦА 3. Данные экспериментов напыления слоя никеля с разными скоростями

Скорость напыления, нм/сек	0,1	**0,2**	0,3
Квантовый выход, % (λ = 460 нм)	5,7	**6,0**	6,0
$R_{дин}$, Ом	1,7	**1,7**	1,9

Выбор режима напыления основывается на том, что при минимальном значении сопротивления квантовый выход должен иметь максимальное значение. Это условие выполняется при величине скорости напыления никеля для создания *p*-контакта, равной 0,2 нм/сек.

Таким образом, в работе были выбраны оптимальные скорость напыления и толщина слоя никеля, при которых контакты удовлетворяли установленным требованиям: невыпрямляющие, обладают малым сопротивлением, высокой механической прочностью и отражающей способностью. Полученные структуры имели высокий квантовый выход.

Список используемых источников

1. Громов Д. Г., Мочалов А. И. Металлизация ультрабольших интегральных схем: учебное пособие. М.: БИНОМ, 2009. 277 с.

2. Ordal M. A., Bell R. I., Alexander Ir. R.W., Long L.L., Querry M.R. Optical properties of fourteen metals in the infrared and far infrared: Al, Co, Cu, Au, Fe, Pb, Mo, Ni, Pd, Pt, Ag, Ti, V, and W // Appl. Opt. 1985. Vol. 24. pp. 4493–4499.

3. Щука А.А. Наноэлектроника. М.: Физматкнига, 2007. 464 с.

4. Пасынков В. В., Чиркин Л. К. Полупроводниковые приборы: учебник для вузов. 6-е изд. СПб.: Лань, 2002. 480 с.

A N N O T A T I O N S

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Averenkova M., Kopylov S. Review of Electronic Document Marking Approaches Based on Word Shift. – PP. 5–10.
The information and telecommunication networks development made it possible to move on to the electronic document management systems introduction in all areas of electron interaction. The shortcomings and vulnerabilities presence in the protection tools of these systems does not allow providing the required level of protection against documents leakage submitted in electronic form. To increase the electronic documents security, it is necessary to improve the existing marking information means. The article presents methods analysis for marking electronic documents containing text based on the steganography data embedding by shifting words. In the course of the analysis, an approaches description to marking based on horizontal word shift is given, the main parameters a quantitative assessment of existing research in the marking field is carried out, and their advantages and disadvantages are identified. The using methods possibility of steganography information embedding to improve the electronic documents security is substantiated. Directions for further research identified.
Key words: marking, text steganography, electronic documents.

Avramenko V., Kanchalan S., Kovalev A. Forecasting State Parameters of Computer Technology Based on a Recurrent Neural Network. – PP. 10–14.
The article proposes an approach to implementating the function of automatic prediction of failures of computing equipment based on recurrent neural networks of long short-term memory (LSTM). As a result of the operation of the system of artificial neural networks, the predicted values of the parameters of the technical condition of individual elements of the system are formed, then the degree of their compliance with acceptable values is determined.
Key words: neural networks, prediction, failure.

Akimov S., Amelchenko D., Marzaganov G. The Concept of Using Microcms in Open Digital Ecosystems. – PP. 14–18.
Presentation of the concept of using a micro content management system (MicroCMS) in an open digital ecosystem, a unique microservice architecture. The micro-context management system allows deep integration into protection and projected open water ecosystems, freeing up the possibilities of microservices, forming data ecosystems, from the implementation of decisions to regulate the wide distribution of volumes - from pollution and detection of rare pollution, to the creation of multi-page hypertext documents. Unlike fast context management systems and cloud editors, MicroCMS does not have redundant functionality, the necessary

deep integration into the digital documents of the ecosystem, and it also has the ability to use MicroCMS as a conditional (cloud) service, and deploy the MicroCMS service on servers.
Key words: microservice architecture, content management, MicroCMS, cyber environment, open digital ecosystems.

Alekseeva M., Bologova A. Comparative Analysis of Flow Cytometry and Automatic Microscopy in the Study of Urine Sediment. – PP. 19–23.
Currently, there are many methods for diagnosing various human diseases. A special place in clinical practice is occupied by laboratory research. In particular, in the treatment and prognosis of pathologies of the genitourinary system, urine analysis is of great practical importance. Urine analysis is widely used for monitoring urinary tract infections, determining the cause of bleeding in the urinary system, kidney diseases, etc. The process of manual urine examination is a long, time-consuming procedure. This does not correspond to the current flows in the laboratory and requires a fairly good practical training of a laboratory assistant. Given the large flow of analyses, the research process has become rapidly automated. This significantly improved the quality of diagnostics and optimized the workflow by reducing manual labor in the laboratory. One of the stages of urine analysis, which is of great practical importance in the clinical diagnosis, treatment and prognosis of pathologies of the genitourinary system, is the determination of shaped elements in the urine sediment. This article discusses the main advantages and differences of two technologies for the study of urine sediment, prevailing in the market of laboratory equipment, such as flow cytometry and automatic microscopy.
Key words: microscopy of urine sediment, flow cytometry, automatic microscopy.

Amelchenko D., Gvozdkov I., Gonyaev S. Analysis of the Effectiveness of Imaging Techniques in Video Games. – PP. 23–27.
For many PC users, modern computer components did not allow for luxury. This means that the success of the game will be very high, and in order to be effective on low-end PCs, it is necessary to resort to accurate image evaluation. Some methods are very time consuming during development, which means that depending on the content of the game, it is necessary to combine the most appropriate parameters for specific projects.
Key words: optimization, video games, pc games, rendering.

Andreev I., Nevrov A., Homichuk M. Analysis of Approaches Building Systems of Planning and Organization of Activities for State Structures on the Basis of Web Technologies. – PP. 27–30.
In now time level of process automation of planning and organization activities in state structures doesn't meet the needs officials. They solve problem of forming planning and reporting documents, collect and summarize information about level of it's realizations without specialized methods, technological methods and appropriate means of automating this activity.
Key words: information security, web applications, web server, client.

Arestov A., Kopylov S. Keypoint Detectors Application for Text Regions Location in Images. – PP. 30–35.
The task of protecting text documents containing confidential information and personal user's data is an actual research area. The paper considers the using keypoint detectors features to

text areas detection in images represented by photographs and monitor screen shots. During the experimental evaluation of the keypoint's extraction from photographs and screenshots, the quantitative values of keypoint's and their correspondence to the image text areas were obtained. The results obtained allow us to conclude that it is possible keypoint detectors use to detection of image text areas and protect text documents from leakage. In conclusion further research directions are presented.
Key words: text documents, information leakage protection, pattern recognition, key points detection algorithms.

Arkhipov P., Markin D., Sizov N. Security Analysis of Modern Instant Messaging Services. – PP. 35–39.
The article provides a comparative analysis of modern instant messaging services. Criteria for evaluating messengers are proposed. The functionality of an expanded list of existing instant messaging tools is analyzed. The conclusions justifying the choice of the most secure technical solutions providing secure instant messaging are formulated.
Key words: messenger, messaging service, security assessment model.

Baranauskas M., Tarasov V. Introduction of Information Technologies in the Field of Collecting. – PP. 40–44.
The technologies of creating Web applications aimed at people engaged in various kinds of collecting are considered. Aspects of the strategy of developing such applications are reflected, which will allow collectors to create a new collection and perform various operations with it without spending a lot of time on it, in addition, the user of such applications is less likely to make some mistake in the process of collecting. Modern technological means of Web design are analyzed. To create this kind of information systems, it is important not only to know a certain technology, but also to understand what advantages and disadvantages it has over other technological solutions, as well as whether it is suitable for creating a system that will have high performance and will not spend an excessive amount of system resources.
Key words: web application, design layout, layout, programming, database.

Bayagantaeva E., Musaeva T. Review and Analysis of Generative Adversarial Networks Models for Creating Unique Art Objects. – PP. 45–49.
This article presents an overview and analysis of generative adversarial networks models for creating unique art objects. In this article there are a description of their architecture features, representation of generated images, an analysis of their advantages in usage. Generative adversarial networks models are used not only for general creative self-expression, but also for commercial design of advertisement, book covers, clothing, etc.
Key words: neural network, generative adversarial network, image generation.

Bednyak S., Kuznetsova A., Fedulova A. Using Chatbots to Automate Business Processes. – PP. 49–53.
Chatbots are increasingly popular among ordinary people. Companies are increasingly seeking to turn routine processes into automatic mode and facilitate business by giving the chatbot at least answers to frequently asked questions from customers or partners. But the more business processes take place inside the company, the more difficult it is to control everything manually. This is where chatbots come to the rescue.

Key words: chatbot, automation, business.

Berestovsky P., Glebov A., Gusev A., Ivanov V. The Relevance of High-Frequency Monitors, How Human Vision Works. – PP. 54–58.
This article is devoted to exposing popular misconceptions about the operation of the monitor, the principle of operation of the human eye, the dependence of the lining of the screen and the computer graphics card. The influence of use in games is considered as a theory and examples of implementation, as well as an analysis of the further development of neural networks in various fields.
Key words: monitors, the number of frames per second, the work of human eyes.

Bovshik P., Litvinov V. Analyzing the Capabilities of PyAudio Allows you to Implement the Implemented Rich Content Library Model for Voices. – PP. 59–63.
The purpose of the work is to explore the possibilities of the PyAudio library using the example of creating a deep learning model for voice recognition. Recently, machine learning has become very popular, deep learning models are used in many areas of human life, for example, to minimize risks, downtime and identify security threats in enterprises and not only, to recognize objects on video surveillance cameras, voice recognition when creating a mobile operator -bot or voice assistant such as Siri or Alice. In this talk, one of the most popular and easy-to-use deep learning libraries, PyAudio, will be discussed. On the basis of this library, the simplest object recognition model in Python will be created.
Key words: deep machine learning, library, voice recognition.

Boyashova E., Melnikov M., Ushanova M. Infographics as a Form of Graphic and Communication Design. – PP. 63–69.
The work is devoted to the consideration of infographics as a form of graphic and communication design. Considering infographics from this position allows you to focus on the importance of the form of information presentation. The article pays special attention to the direction and importance of infographics in the presentation of a large amount of statistical data. The paper presents options for the classification of infographics, where information graphics are presented from different positions, and a new classification is proposed. In addition, the paper considers and analyzes examples of infographics from world practice.
Key words: infographics, information graphics, graphic design, communication design, information, data, data presentation.

Brazhnikov D., Gorokhov D. Detection of Web-Traffic Anomalies Using Neural Networks. – PP. 70–75.
Web traffic is the amount of data that circulates on a computer network over a period of time. With the development of computer technology, statistics on attacks on information resources are growing. Web traffic anomalies are certain changes in the flow of time series. For complex computer networks to operate reliably and securely, they must be detected quickly and accurately. This paper proposes a neural network linking convolutional neural networks (CNN), long-term short-term memory (LSTM), and deep neural network (DNN). It is superior to other current anomaly detection methods, resulting in an overall test data set accuracy of 96,8 % and a recall rate of 88,2 %.

Key words: deep learning, time series, anomaly detection.

Brylev M., Likar A., Povedaiko M. Development of a Mobile App for People with Disabilities. – PP. 75–79.

The purpose of the research is to review the principle of sign language and to create an application that will teach deafblind language to children. Since the application is developed specifically for children (up to 12 years old), the work pays a lot of attention to the perception of the world by children, that is, their thinking in images and bright colors and objects. After all, the same principle will be used to build the appearance of our application.

The article analyzes the existing analogues and takes into account their pros and cons. A comparison of existing analogues and your own idea is given.

This is followed by a section devoted to the development of the application-which technologies and development environment were used to create the application and an explanation of why we chose them. Due to the fact that the software product under development has a client-server purpose, special attention is also paid to the security of this application.

Key words: mobile application, psychology, children.

Bulgakov D., Dobrithin M., Shugurov D. Features of the Use of Security Analysis Tools in State Information Systems. – PP. 79–83.

The active and ongoing development of information systems in recent decades entails new threats to information security. At the same time, information systems are one of the reliable official sources necessary both for ordinary citizens and for information support of activities by public authorities. At the same time, state information resources located in open networks are quite often subject to computer attacks. In this regard, the problem arises of the possibility of reducing damage through the use of an information security monitoring system and the development of software tools that are able to detect vulnerabilities at various stages of the life cycle of information systems.

Key words: information system, vulnerabilities, security analysis tools, information security monitoring.

Vaganov A., Grigoreva E. Control Device for the Air Disinfection System in Closed premises of Enterprises. – PP. 84–88.

The article discusses with issues related to the development of a control device for a disinfection system designed to clean the air from biological pollutants in the premises of industrial enterprises. The relevance of developing such a class of systems is substantiated. A block diagram of the device and a variant of constructing a complete disinfection system are presented, and the choice of a modern element base for its implementation is justified. A special algorithm for the operation of the air disinfection system in the closed premises of enterprises has been developed, considering the safety of personnel. A choice of primary measuring transducers designed to control the cleaning process has been implemented. Recommendations on the use of the mathematical apparatus and the study of models are formed. The choice of mathematical apparatus for calculating the device is made. The simulation results are presented and their analysis is carried out. Recommendations for the design of the hardware are given.

Key words: control device, sensor, control algorithm, mathematical model, block diagram.

Vaganov A., Dmitrienko D. Intelligent Power Supply System for ACS Control Units. – PP. 88–92.
The article deals with issues related to the emergence of a power supply system designed for stable and reliable operation of electronic complexes of automatic control systems of modern industrial enterprises. The relevance of developing the idea of a class of systems is substantiated. block diagram of the system, the choice of a modern element base for its implementation is also substantiated. A special algorithm for the operation of the power supply system has been developed, taking, into account the following set: quality parameters of the supply voltage, external factors (temperature, humidity, etc.), frequency state of energy consumers. A selection of primary measuring transducers designed to control external manifestations has been made. The choice of mathematical apparatus for evaluating individual blocks of the system has been made. The simulation results are presented and their analysis is carried out. Recommendations for the design of the hardware are given.
Key words: intelligent system, sensor, control algorithm, mathematical model, block diagram.

Vasilev M., Verkhova G. And/or Tree Generation for Morphological Set Described in Structuralist Language. – PP. 93–98.
The article is devoted to a transformation of a description of a morphological set in the Structuralist language, into an AND/OR tree. The paper contains tree structures description corresponding to main Structuralist language constructions such as aggregation, classification features definition and classification features constraint. A transformation method is shown, which consists of two steps: morphological set model creation from a text in Structuralist language and and-or tree creation by that model. Procedures for these steps are specified. Block-diagram for the second step is presented. An object model used in transofrmation is described. An example of transformation is given.
Key words: structural-parametric synthesis, morphological set, and/or tree.

Vasilev N., Kudryavcev A., Rumyantsev M. Comparison of Microservice and Monolithic Approaches to the Implementation of Software Under the Conditions of Permanent Change of Its Developers. – PP. 98–104.
The article compares the microservice and monolithic approaches to software implementation, reveals their advantages and disadvantages. The possibility of long-term development and maintenance of monolithic and microservice software in the conditions of constant change of developers is analyzed.
Key words: software architecture, modular architecture, monolithic architecture, micro-service architecture, team development, authoring.

Verhova G., Krylova E. A Model for Automated Accounting of Personal Achievements of Individuals within the Framework of Integrated Interoperable Cyber-Physical Environments. – PP. 104–109.
One of the main goals of forming a unified cyber environment is to reduce routine operations when filling out all kinds of forms, which currently take up a significant part of the working time of employees and students. The report proposes a model of automated accounting of personal achievements of individuals carried out within the framework of the integrated interoperable cyber environment of virtual enterprises. A feature of interoperable cyber-physical environments is the possibility of seamless integration into the global cyber-physical environment. Personal achievements are accumulated in the electronic portfolio of an

individual, which is an open information system capable of interaction and deep integration with other information systems for data exchange using "one click" method.
Key words: cyber-physical environment, electronic portfolio, e-portfolio, virtual enterprises.

Verkhova G., Ovsyannikov D. Formation of a Graphical user Interface for Services of the Cyber-Physical Environment using Microfrontends. – PP. 110–113.
The article describes the formation of a graphical user interface for cyber-physical environment services using microfrontends. Specific examples of the implementation of custom html elements are described, as well as one of the possible examples of interaction between isolated parts of the user interface of cyber-physical environments.
Key words: microfrontends, user interfaces, cyber-physical environments, distributed systems.

Verkhova G., Prokofev P. SLAM Application in Multidimensional Geoinformation Modeling. – PP. 113–116.
The results of studies of methods of simultaneous localization and mapping for autonomous vehicles are presented. The ways of applying the methods of synchronous localization and building maps for collecting geoinformation are considered. The ways of integrating heterogeneous information in geoinformation services with the help of multidimensional models are considered. The concept of integration of methods of simultaneous localization and construction of maps into geoinformation services using multidimensional models is proposed. The ways of building libraries of software-algorithmic support for methods of localization, construction and updating of multidimensional geoinformation models are considered.
Key words: SLAM, GIS, multidimensional modeling, map building, autonomous vehicles.

Volostnykh V., Ostroumov O., Synuk A. Analysis of the objects criticality regulatory base in the Russian Federation. – PP. 116–119.
A lot of attention is paid to the security and sustainability ensuring issues of the critical information infrastructure facilities operation. The regulatory framework governing issues in this area is constantly being improved. The paper analyzes the current state of the regulatory framework in Russia in the safety ensuring field of the objects criticality in various society spheres.
Key words: critical information infrastructure, critical facility, functional stability, security, complex system.

Gavrilov I., Martynov D. Authenticated Encryption Software in Electronic Document Management Systems. – PP. 120–124.
The article presents the results of the development of a software tool for authenticated encryption for electronic document management systems. The main steps of the algorithm of this software tool for the implementation of the process of authenticated encryption when transferring graphic files are considered, indicating the structural elements of the jpg-format.
Key words: encryption, authentication, associative data, electronic document management system.

Galimova E., Khodanovich A. Features of the Intelligent Process in Software Testing. – PP. 124–127.

This article discusses the main trends in the intelligent software testing process. Important differences between software systems developed on the basis of an object-oriented approach and artificial intelligence systems are identified for the testing specialist.

Key words: software testing, artificial intelligence, intellectualization, regression testing, machine learning.

Gvozdkov I., Kildyaev I. Using NAT Vulnerabilities to Register Devices in Wan Networks. – PP. 128–132.

In the chosen number, every second there is a huge number of users in the global network, IP addresses are required, but there is a significant shortage of addresses on the IPv4 protocol, and that would be allowed to solve the problem and facilitate the transition to IPv6 created by NAT. This article provides information about NAT technologies, concepts to consider, problems that occur in collections, and the most popular solutions to problems related to registering devices in top collections.

Key words: NAT, perforation, wide area networks, peer-to-peer networks, end-to-end addressing, device registration.

Gvozdkov I., Mironenkova M. Application of the Threat Model to Protect Personal Data. – PP. 132–137.

All relations and actions related to personal data and their processing in personal data information systems are regulated by Federal Law of the Russian Federation No. 152 of 22.07.2006. The most important task in the processing of personal data is to ensure their security.

Key words: Federal Law of the Russian Federation No. 152, personal data, personal data information system, processing, leakage, Threat model.

Gvozdkov I., Orehov A., Sarantsev A. Prototype of Multilevel Access Control System. – PP. 137–142.

Information security is a strategically important goal of society. All processes of production, storage and exchange of information, all technical and software components involved in these processes must be safe. Multi-factor authentication is better than single-factor authentication. But if you look at the authentication methods in the access control systems of almost any organization, it turns out that most systems use one-factor authentication. The article presents a proposal for the implementation of a prototype of a multi-level access control system that improves the security of an object with minimal investment.

Key words: ACS, access control and management system, multi-factor authentication, TOTP, FaceID, MFA.

Golubenkov G., Gorokhov D. Host Anomaly Detection using Intellectual Data Analysis Models. – PP. 143–148.

A system call is a call by an application program to the kernel of a public system to perform some operation. Anomaly-based host intrusion detection system detects attacks based on system deviations from normal behavior. However, these systems have a high detection rate. This article uses neural networks as a way to implement solutions that use traces of system calls as

input. The ADFA-LD dataset is used for hypothesized intrusion detection models and testing their effectiveness.
Key words: deep learning, system calls, anomaly detection.

Gorbachev P., Makeev V., Solopov E. Crossarchitecture Obfuscation Tool Using the Intermediate Representation Language LLVM IR. – PP. 148–152.
In the context of the active development of modern society and the widespread introduction of new technologies in all spheres of human activity, the issue of ensuring information security is extremely relevant. The active introduction of proprietary software in information processing system at various levels, as well as the import substitution of used foreign software in favor of domestic analogues and implementations, make us seriously think about software protection issues.
Key words: LLVM IR, obfuscation, research protection, program code protection.

Gorbachev P., Makeev V., Solopov E. Transformation of Apple iOS Operating System Software into an Intermediate Representation of LLVM IR. – PP. 153–157.
iOS is the second most popular mobile operating system and is considered the "most secure" compared to Android. A significant part of this reputation is due to the fact that the application ecosystem is under the exclusive control of Apple. The opportunity for malware to spread is much higher due to the obligation to register with Apple's developer program, the AppStore verification process, and Apple's ability to centrally revoke applications. However, malware is not the only threat to the security and privacy of users, which necessitates a universal solution for analyzing the security of Apple iOS software.
Key words: apple iOS, LLVM IR, transformation of executable files, software analysis technology.

Gromova N., Nesterov A., Stepkina Yu., Shestakov A. Digital Transformation of Lecture Material on the Example of Geoinformation Disciplines. – PP. 158–163.
Further development of the methodology of variable location of the content of educational material is presented using the example of digital transformation of lecture material in geoinformation disciplines. Theoretical approaches are based on the author's spatial model of the transformation core in the form of static and dynamic QR codes, and practical ones – on the means of students' access to digital resources.
Key words: educational materials, educational and didactic content, QR codes.

Gubin A., Litvinov V., Filippov F. Selecting a Metric for Clustering Categorial Data. – PP. 163–167.
In real (and in scientific problems) there is a need for clustering data of a mixed type – for example, when one half of the data is numeric, and the other half is categorical. Separately, these problems are solved by standard methods, however, solving the mixed data clustering problem presents some difficulties, mainly due to the complexity of calculating the distance between observations. The paper investigates the issues of the optimal choice of metrics for solving the problem of clustering multidimensional vectors. Particular attention is paid to the presence of categorical components. The research is based on the analysis of existing approaches, such as the use of the Gower distance as a metric and their software implementations.

Key words: machine learning algorithms, clustering, vector similarity/difference, Gower distance.

Gubin A., Litvinov V., Filippov F. Using Partial Reserve Systems to Provide the Required Reliability Indicators. – PP. 167–173.
When analyzing the parameters of system reliability, the structure of the system, the composition and interaction of its constituent elements, the possibility of restructuring the structure and algorithms of its functioning in case of failures of individual elements are taken into account. The paper considers the issues of estimating the number of non-redundant elements of the system, allowing to obtain the required values of reliability indicators by redundant system remaining part. An estimate of the gain in terms of the number of elements in comparison with the use of traditional reservation methods is given.
Key words: reliability, non-failure operation, reliability indicators, system, redundancy.

Gubin A., Litvinov V., Filippov F. Decision Support Systems for Selecting Structured Financial Products. – PP. 173–178.
Making the right investment decision is a complex process that includes several stages: gathering information; search and finding solutions; choosing the best alternative. Modern advances in the field of information technology allow the decision maker to reduce the time and other costs of choosing the best alternative, and the investor to choose the best of the options received. The paper considers an intelligent decision support system, which was created specifically to work with such complex derivatives as options and helps a potential investor choose the best option from the proposed list of decisions.
Key words: financial analysis, technical analysis, fundamental analysis, intelligent decision support system.

Gunina A., Kotlova M. Forming a Model of the Information System of Staff Selection using Artificial Intelligence Methods. – PP. 179–182.
The key tasks of the information system for the selection of professional personnel are determined. The range of parameters necessary for solving the problem of choosing an applicant is presented. The main elements of the information system model are defined, which provides for the implementation of scenarios for placing a vacancy by the organization, submission of a resume by the applicant and comparison of the requirements of the employer with the knowledge, skills and competence of the applicant. The possibilities of using artificial intelligence methods for solving the problem of finding professional personnel are considered. An information system model is presented.
Key words: applicant, intelligent selection, cloud of parameters, models, array of vacancies.

Damdinov B., Ptitsyna L. Extended Object-Oriented Modeling of Schedulers for Controlling Coarse-Grained Processes. – PP. 182–185.
The prospects for the development and wide demand for soft architectures of intelligent information systems are highlighted. Various aspects of the importance of intelligent control of coarse-grained processes in information systems with a soft architecture are considered. The role of the action planner in intelligent information systems with a soft architecture is presented. Modern achievements in the field of research of action planners are analyzed. The

advantages of extended object-oriented modeling of action planners are revealed. The key features of the proposed object-oriented models of action planners are revealed.
Key words: architecture; coarse granular process; action planner; model; modeling.

Denisova U., Petrov D. MAC-address Usage for Identification and Prevention of Unknown Devices in the Network. – PP. 186–191.
Currently, the issue of implementation of network security systems on the enterprises is the most sought after, that is why the article is focused on implementation of network security system with MAC-address usage. Therefore, identification and prevention includes elements of network analysis with the use of different methods, such as found unknown devices notification and prevention of their function in the local area network. This aim at reducing amount of unknown devices and improvement of network security.
Key words: LAN, MAC-address, information security.

Diyazitdinova A. Homography Superposition of the Television Images with the Preliminary Feature Points Matching by the Log-Polar Coordinate System. – PP. 191–198.
The important issue of multicam machine vision is the homography superposition of the television images by the environmental test. The usual procedure of superposition is to use the aim object (as a rule, chessboard), but in some cases aim object is not available. The main problem of processing the environmental test images is point matching. The full-scan method defines the huge amount of matching. The processing time does not meet the requirements of video surveillance. The developed algorithm solves this problem. It includes the heuristic procedure for points selection and the procedure of the preliminary feature points matching by the log-polar coordinate system.
Key words: homography, superposition, *matching*, *log-polar*, image.

Dobryshin M., Levicheva Y., Reformat A. Suggestions for Improving the Effectiveness of the Choice of Corporate Security Strategies Communication Networks. – PP. 199–202.
Improving the methods of using computer attacks against corporate communication networks integrated into the global information space requires appropriate development and information security systems. An analysis of the general design approaches of such systems revealed a drawback: an insufficiently justified choice of the optimal composition and structure of this system. To eliminate this drawback, a sequence of efficiency evaluation based on the deviation of normalized values from the required values and a proposal for building a protection strategy based on a genetic algorithm is formulated.
Key words: information security system, efficiency, genetic algorithm.

Eliseev N., Shiyan A. Analysis of the Current Level of Development of Technologies for Creating Interactive Visual Content. – PP. 203–208.
Today's data technology allows you to view visual content on a variety of platforms, from terrestrial television to video services on the Internet. One way to increase user engagement when watching video is to add interactive components to video content. However, the difference in the interfaces of playback devices has led to the creation of different principles of human interaction with interactive content.
This article gives a classification of media content technologies, a comparative analysis of existing technologies for human interaction with interactive visual content on different

platforms, and examples of interactive video content implementation. The paper formulates the requirements for a universal interface for human interaction with interactive content. The results can be useful in creating interfaces based on common principles of interaction with interactive visual content.
Key words: interactivity, interactive media content, classification, interaction, human-machine interface, user interface.

Ermolaev D., Tarasov V. Universal File Interface to the System Instant Messaging. – PP. 208–212.
An overview of instant messaging systems with incompatible access interfaces is presented, the difficulties of creating an aggregator of these systems are touched upon. The development of a single access interface will allow abstracting these incompatible interfaces for the end programmer and simplify the creation of access programs to instant messaging systems. The concept of instant messaging systems that have a hierarchical structure is described, which determines the choice of the hierarchical file system interface as a universal interface to such products. The structure of instant messaging systems is analyzed and the organization of a universal file interface to them is proposed.
Key words: instant message, interface, container, programming.

Esalov K., Poponin A., Triandafilidi I. System for Automatic Text Annotation of Audiobooks and Other Audio Data. – PP. 212–216.
Audiobooks and audio podcasts are very popular these days. This allows you to collect audio data for training neural networks. Such data is great for training neural networks for tasks of automatic speech or speech synthesis. In this work, you can create a network of audiobook or audio podcast stores.
Key words: AI, neural networks, natural speech processing, neurocognitive architectures.

Zalesskii I., Denisova Yu. Design of Information System for Vaccination Certificates QR-codes Verification. – PP. 216–220.
In an atmosphere of ongoing pandemic several decisions dedicated to requirements for creating an access control to certain categories of public space and transport are being taken in the Russian Federation. Access control involves the use of QR-codes as basic document for existence of the right of access. Because of that the need for the Information System that could verify the presented document and prevent the possibility of presenting a fake certificate has increased. The article presents the implementation of the Information System demo version that solves the issue. All possible QR-code data options are considered. The fastest method of reading existing vaccination certificate data is defined. Advantages over existing solutions are identified.
Key words: QR-code, vaccination certificate data, JSON-object, download speed of data.

Zikratov I., Zikratova T., Khamov V. Robotics: Managing Social Communities of Robots. – PP. 221–225.
The solution of the problem of optimizing the actions of self-organizing groups of robots leads to attempts to use in robotics mechanisms for managing societies of living organisms. The formulation of the problem of choosing the optimal plan by a group (swarm) of robots is formulated. The tendencies of intelligent swarm management based on the paradigm of

"behavior intelligence" are shown. An analogy is drawn between social groups of living beings and groups of robots, which allowed us to introduce a new term for robot societies – robotics.
Key words: group robotics, behavioral models, trust, reputation, opinion, management of society, destabilizing factors.

Ivanov V., Korchevnoy P., Pesterev V. Securing the Virtual Control Center. – PP. 226–229.
This article talks about the virtual control point. The most popular method of organizing network security is described.
Key words: metaverse, virtual reality, VirPU structure, IPS system, cybersecurity, network connection.

Ivanov R., Musaeva T. Methods for Automatic Placement of Objects. – PP. 229–232.
Currently, there are many projects with virtual worlds in order to organize social interaction and business processes. The proposed projects have a list of problems that complicate the organization of the working virtual space, which affects the quality of optimization. For this, a method is proposed that allows for the automatic placement of physical objects within the premises, which will partially solve these problems.
Key words: automatic placement of objects, methods of placement of objects.

Izotov N., Makeev S., Markin D. The system for Identifying Information Containing extremist Materials` Features Based on Software-Controlled Browser. – PP. 233–238.
The article describes an automated system for collecting and identifying information materials containing extremist materials` features. The description of the collection subsystem based on the use of software-controlled browsers, as well as the subsystem of classification of information materials based on statistical measures TF-IDF is presented.
Key words: information gathering, classification, extremism, software-controlled browser, TF-IDF.

Izrailov K., Romanov N. Application of a Genetic Algorithm for Reverse Engineering of Machine Code. – PP. 239–243.
This article is devoted to the study of the possibility of using a genetic algorithm, which is a heuristic search algorithm, to solve the decompilation problem. The study examines the general scheme of the so-called genetic decompilation of machine code into pseudo-source code for subsequent static analysis in order to search for vulnerabilities. A significant part of the work concerns the analysis of the potential advantages and disadvantages of using such an approach in reverse engineering. As a result of the research, the authors concluded that the use of the proposed concept is justified and can significantly affect the development of reverse engineering, as well as information security in general.
Key words: information security, machine code, reverse engineering, decompilation, genetic algorithm.

Ilina O., Kupchinenko O., Skoropad A. On the Issue of Integrity Control. – PP. 243–248.
To solve the problem of integrity control, the functionality of the Astra Linux SE operating system has been expanded with a set of security tools that implements data integrity management functions. This complex allows you to control both the integrity of data and the

contents of executable files, which makes it possible to establish with high probability that there are no data and functions in the OS that have undeclared capabilities, and is a confirmation of the integrity and authenticity of the transmitted and stored data.
Key words: operating system, information security, a set of security tools, integrity control, checksum, closed software environment, routine integrity control.

Ilina O., Kupchinenko O., Skoropad A. Backup and Recovery of Information in Modern Protected DBMS. – PP. 249–252.
The analysis of methods of backup and recovery of information in a protected *DBMS PostgreSQL from the operating system of a special purpose Astra Linux SE is carried out. Advantages and limitations for each method are considered. Recommendations are given for scheduling backup and recovery of information in the database.*
Key words: operating system of a special purpose, database management system, database, information security, backup and recovery of information, archiving.

Kazancev A., Malukov V., Skakunov R. Description of Methods for Analyzing and Detecting Malware. – PP. 253–256.
Network and system security are incredibly critical issues now. Due to the rapid proliferation of malware, traditional analysis methods struggle with enormous samples.
Key words: reverse engineering, system security, encryption, obfuscation.

Kalashnikov O., Lipatnikov V., Sindeev M., Shevchenko A. Model of the Response Process of the Information Security Administrator to Network Security Violations. – PP. 256–261.
Known methods for managing the protection of VoIP telephony networks using special measures in modern conditions are not effective enough, since they do not consider ways to support decision-making and predict intrusion threats. The aim of the work is to develop a proposal to ensure the protection of the VoIP-telephony network by predicting and supporting decision-making in the face of intrusion threats. The article proposes a model of actions for an ITCN IS administrator in the event of an IS violation event.
Key words: information technology, information networks, cognitive maps, VoIP, information and telecommunication network (ITCN).

Kalashnikov O., Lipatnikov V., Sindeev M., Shevchenko A. Proposal for the Classification of Computer Attacks on Information and Telecommunication Network Resources. – PP. 261–266.
Traditionally, attacks are categorized according to the effect that they produce: breach of confidentiality of information, breach of integrity of information, and denial of service. The main disadvantage of such a division is its weak information content, since it is practically impossible to say anything about its features based on information about the attack class.
Key words: classification, attacks, networks, systematization, computer attacks.

Karaev D., Markin D., Pinin D. The Pegasus Program Model Based on Heuristic Features. – PP. 266–271.
The article presents a malicious software model of the Pegasus tool (a trojan program is able to performs unauthorized access and data collection), an algorithm for its detection, as well as

a software implementation of the algorithm operating under the Android operating system. The model is based on the heuristic features – a subset of the system privileges used and potentially dangerous API calls. An assessment of the effectiveness of the developed approach in analyzing data backups (dumps) from several devices is presented.
Key words: static analysis, signatures, Android Trojans.

Kiryanov A., Toroptsev A. Analysis of Identifying Features of Confidential Traffic. – PP. 272–275.
Interaction between distributed networks of organizations is currently organized mainly by means of packet-switched networks (PSN), using the network communication protocol IP. When organizing communication using the leased networks of the operator, to preserve privacy different kinds of tunnels are organized, in particular virtual private networks (VPN). VPN is a geographically distributed logical network organized on the basis of already existing networks, which has a similar set of services to the main network and is characterized by a high level of data protection using cryptographic equipment. With the help of this technology it is possible to transmit confidential information.
Key words: confidential traffic, MPLS L2 VPN, identifying features.

Knyazev E., Kolesnikov A. Modern Vulnerabilities in the Security of Web Applications. – PP. 276–280.
A huge number of web applications operate with a large amount of personal data. This data is between two opposing sides. On the one hand, these are companies and institutions seeking to preserve the confidentiality of data, as well as to secure their information systems. On the other hand, more and more experienced attackers, attracted by the bait of profit from the stolen data.
Key words: web application, vulnerability, information security, threat.

Kozhanov J. Methods for Improving the Cryptographic Strength of Messages. – PP. 280–283.
The general principles of symmetric encryption with private keys are considered. Methods for increasing the cryptographic strength of the system are proposed.
Key words: encryption, decryption, cryptographic strength.

Kozachok A., Kopylov S., Polekhin A. About Some Methods of Software Analyzing. – PP. 284–288.
Defects and errors in computer programs are one of the components of the software design, implementation and operation process. Software analysis methods are used to improve software security. The analysis methods application makes it possible to identify the development and debugging stages shortcomings, and the results obtained can be used in the eliminating process of detected defects and correcting the program source code. The article provides a description of the means for detecting development and operation errors in the program code analysis process. In the existing solutions analyzing process in the software analysis field, a program verification definition is given, an existing verification methods classification is presented, and their main advantages and disadvantages are described. The symbolic execution choice of programs to improve the program code security is substantiated. Directions for further research have been identified.
Key words: software analysis, secure software, symbolic program execution.

Kolbina O., Kushakov E., Matyukhin D., Yagotintceva N. Analysis of Methods of Visualization of Real World Objects in GIS. – PP. 289–294.
The article is devoted to the analysis of methods for visualizing objects of the real world in a geographic information system. The features of the use of each method, as well as time and quality requirements for the use of each of the methods are determined. The legislative base regulating the development of geoinformation systems for visualization of real world objects is considered. The purpose of the study is to formulate recommendations on the use of methods for visualizing objects of the real world in the development of a geographic information system. Objectives: to consider the current state of the principles for the development of geographic information systems and ways of visualizing information, the legal framework governing the development of geographic information systems, and to verify the unity of the principles of development, focusing on the legislative framework. Relevance of the work: to date, many methods have been created for visualizing objects of the real world in a geographic information system, but none of them can be called universal or breakthrough in their field of use.
Key words: geoinformatic system, analyze, modeling, visualization.

Kolesnikov A., Kosyrev N. Analysis of Possible threats Associated with Zero-Trust Architecture (ZTA). – PP. 295–298.
This paper briefly describes the zero-trust architecture and the possible threats when using this architecture. The purpose of this paper is to familiarize you with the security threats of a zero-trust architecture in order to better secure your transition to this architecture.
Key words: zero-trust architecture (ZTA), zero-trust (ZT).

Kolesnikov A., Prokopenkov V. Decentralized Applications and Web 3.0. – PP. 299–304.
This article reveals the concept of decentralized applications, describes the mechanisms of operation and the scope of their application. The main tool considered in the work is the Ethereum blockchain. It describes the auction application and partially parses its program code, as well as the main issues of decentralized applications. The purpose of this paper is to decentralize the basic services provided to people, with a further increase in security and reliability.
Key words: smart contract, blockchain, Ethereum, DApp application.

Kolesnikov A., Syachin K. Intelligence-Protected Access Management Tool Based on a Chain of Proxy Servers and VPN Services. – PP. 304–309.
The article reveals the concepts of a virtual private network (VPN), proxy server and Tor browser technology. The main ways of ensuring the security of the Internet connection using these technologies are described, and an example of the implementation of a chain of proxy servers as a means of managing intelligence-protected access based on the VPN service is also shown. The purpose of the work is to increase the reliability and security of traffic transmission for access to a target resource or server on the Internet.
Key words: anonymity on the Internet, VPN, chain of proxy servers, Tor browser.

Kolesnicov A., Chistyakova A. Approaches to Solution a Problem of Integration of Data in Information System. – PP. 310–314.
The paper lists and gives a brief description of the methods and approaches for implementing a data integration solution. The data integration process has become one of the main

components of the overall data management process, but there is no universal way of integration.
Key words: data integration, data management, security, data consolidation.

Kolesnikov A., Shendevitskiy I. Smart Contracts and Their Security. – PP. 314–319.
This article reveals the concept of smart contracts, describes the mechanisms of work and the scope of their application. The main means considered in the work is the Ethereum blockchain. The process of compiling a smart contract and converting it into bytecode using the Solidity high-level language is described, as well as the main security issues of smart contracts. The purpose of this work is to increase the reliability of relations between users when they make bilateral transactions on the Internet.
Key words: smart contract, blockchain, Ethereum.

Kolmakova D., Pletnev Y., Shestakov A. Prototyping Data Accounting Tasks in Intelligent Transport Systems. – PP. 319–323.
The problem of expanding the composition of accounting data on corporate vehicles and updating them by automating the equipment of highly automated transport, the availability of telecommunications infrastructure and aggregating data directly into the software of service departments is considered. The results of the formation of the required nomenclature of accounting data, the composition of the software product, the justification of the development environment and user interface options as a prototyping of data accounting tasks in intelligent transport systems are presented.
Key words: data accounting, development, transport.

Koloskov N., Paleeva E., Puzanov I., Rozhdestvensky D., Sergienko S., Fedorova A. Analysis of the Use of VR Technologies in Scientific and Educational Activities. – PP. 323–328.
The article describes the directions of application of VR technologies in educational and scientific activities, identifies the advantages of these technologies when they are used in universities. The results of a detailed comparative analysis of the introduction of VR technologies in advanced educational institutions in Russia and abroad are presented. Conclusions are drawn about the degree of prevalence of VR technologies in educational and research departments of universities at the present time.
Key words: education, science, high-tech projects, innovative technologies.

Krivolapov D., Frolova K., Shestakov A. Selecting a Framework for Analyzing and Assessing the Structural Risks of Projects. – PP. 328–333.
Ways to reduce costs with acceptable quality for decision support systems of complex infrastructure projects customer due to bundling system-technical solutions that implement various functional tasks, based on the operational use of standard freely distributed software tools of general application and their seamless interaction are considered. The procedures of analysis and choice of software tools to collect relevant spatial data in the attributes of specifications of deployable objects (linear and area), the generality of the controlled parameters of various projects and the level of mutual influence of the results of their phased implementation, as well as the procedures of analysis and choice of software tools of graph

modeling are investigated. The results of applying the option of combining the selected software tools are presented.
Key words: communication networks, infrastructure project, risk-parameters, graph model.

Kuzmina D., Rogozinsky G. Styles of Electronic Dance Music in the End of the XX Century: Structural and Technological Analysis. – PP. 334–338.
The first electronic instruments appeared at the beginning of the 20th century, but electronic music as an independent genre arose in the second half of the 20th century - the beginning of the 21st century and today covers dozens of areas from experimental academic music to popular electronic dance music. In this study, the authors consider styles and sub-styles that use pure electronic sound. A common feature of the styles under consideration is the Roland TB-303 instrument, which had a significant impact on the electronic culture of the 90s. Based on the study, the authors present a general model for the formation of electronic dance music styles.
Key words: modeling, petri nets, Roland TB-303, electronic music.

Kurnosov V., Pavlovich A. On the Issue of Ensuring Timely and Full Exchange of Information Resources in the Unified Information Space of Public Administration Bodies. – PP. 338–343.
The place and role of the unified information space in the public administration system, the requirements for the exchange of information resources and the rationale for choosing a distributed registry technology to ensure timely and complete information exchange are considered.
Key words: information space, public administration system, distributed registry technologies, database management systems.

Lapko A. The Analysis of PostgreSQL DBMS Capabilities for Access Control. – PP. 344–349.
The article is devoted to the analysis of the capabilities provided by the PostgreSQL DBMS for access control. SQL commands for managing roles, granting and revoking privileges from roles, and managing row level security are presented. The console utilities used for managing roles are highlighted. The role parameters used in SQL commands and console utilities are given. The interface of the pgAdmin graphical administration tool is described in terms of managing roles and privileges.
Key words: access control, PostgreSQL DBMS, roles, role parameters, privileges, granting and revocation of privileges, a policy of the row level security.

Lebedev N., Mamadaliev D., Markin D., Tezin A. Malicious Attachments in Microsoft Office Documents, PDF Files and Archives. – PP. 349–353.
The article describes the features of malicious attachments in files of various formats. Measures to counteract malicious attachments of the types under consideration, methods of detection are described. Recommendations for the safe use of the presented file formats have been developed.
Key words: malicious attachments, antivirus tools, virus protection measures.

Lipatnikov V., Lomanov A., Nizamov A. Digital Evidence and Volatile Data Analysis in the Linux Operating System. – PP. 354–358.
At present, there is a need to automate the process of digital evidence search in OS based on the Linux kernel, while keeping the processed data unchanged. The paper describes the

developed software package for automated search of digital evidence in OS based on the Linux kernel. Using the software package greatly accelerates the process of finding digital evidence, due to the fact that the collection of volatile data is quite long and time consuming. The program is characterized by the fact that it has all the necessary commands to extract volatile data.
Key words: information security, digital evidence, volatile data, operating system.

Lipatnikov V., Lomanov A., Nizamov A., Shevchenko A. Recognition and Analysis of Dynamics Scenarios of Multi-Stage Attacks in Network Traffic of Information and Computer Networks on the Basis of a Multi-Criteria Classifier. – PP. 358–363.
A method is proposed for adaptive control of the protection of an information-computing network based on the analysis of the dynamics of the intruder's actions by monitoring situational parameters in an opposing environment based on a multi-criteria classifier with stochastic uncertainty. The method includes: monitoring the situation, recognizing the sequence of actions of the intruder, the process of determining situational parameters with a reliable forecast of the intrusion strategy.
Key words: information security, intrusion detection, machine learning, classifier.

Litvinov V., Novikov E. Neural Networks Stability Analysis Methods. – PP. 363–366.
Neural network stability problem is examined. Specifically, two different approaches for defining that problem are compared.
First approach considers weight updating process of feedforward neural network as a nonlinear feedback connection in control system, i.e. control system stability is equivalent to learning process convergence. Second approach considers recurrent neural network as a control system, i. e. control system stability is equivalent to result function convergence.
For this two approaches problem statement and relevance given, also problem solving methods are described. Also, some relevant tasks given.
Key words: neural network, multilayer perceptron, gradient descent, dynamical systems, dynamical system identification, stability, recurrent neural network.

Litvinov V., Ruigo D. Application of Wasserstein Distance and Gradient Penalty in GAN in the Task of Facies Sampling Synthesis. – PP. 366–369.
This paper is aimed at analyzing the effect of modifying the model of synthesizer set of electrofacies based on the use of generative-adversarial neural networks through the introduction of Wasserstein distance and gradient penalty. The study showed that the synthesizer model based on WGAN-GP significantly improves the quality of the initial sample of facies, which in turn makes it possible to improve the accuracy of the control classifier model.
Key words: lithological-facies analysis, geological exploration, machine learning, classification, genera-tive adversarial neural networks, WGAN-GP.

Litvinov V., Tatukov D. Study of Simulation Tools in Automation Problems Airport Business Processes. – PP. 370–374.
When designing and implementing automation systems for airlines and airports, simulation plays an important role. It allows to determine with sufficient accuracy the costs and profits of the system and visually show the effect of the introduction of such a system at the airport. Simulation modeling allows you to build a model at the early stages of design and evaluate all the risks of the system. The market for business process modeling tools is quite large, and when

designing systems, it is necessary to choose the right tool that will best perform the tasks. The paper analyzes and selects business process modeling tools for designing an airport business process automation system.
Key words: information system, airport, business process, modeling, tools.

Logvinova E., Nikitin A., Pachin A. Conceptual Foundations of Reliability Management of Complex Internet of Things Systems Using Digital Twins. – PP. 375–379.
The modern technosphere is increasingly saturated with various devices that include means for collecting and processing data, influencing other objects and the environment. In addition, the combination of these devices in the network allowed us to formulate the concept of the Internet of Things as a spaced complex system, the elements of which are able to exchange data and function without human intervention. Such systems are being implemented in the most complex industrial production lines, safety management systems, in the field of space exploration, medicine and other branches of human activity. Their use is playing an increasingly significant role, and a malfunction of such a system as a result of equipment failure can lead to significant losses, both financial and reputational. Consequently, the task of managing the reliability of complex Internet of Things systems is of considerable relevance.
Key words: cyberphysical system, digital twin, Internet of things, analytics.

Makarov L., Protaseny S. Comparative Evaluation of Works of Creativity. – PP. 380–384.
A large number of observations of the manifestation of natural processes created an idea of the presence of certain laws that manifested themselves in phenomena and objects that were completely different in form and content, so massively represented in real space, the study of which was carried out through physical and mathematical formalisms.
Key words: entropy, information entropy, quantity of information.

Markin D. The Analysis of the Tools` Capabilities Used to Carry out Cyber Attacks on the Russian Federation Critical Information infrastructure. – PP. 384–389.
The article provides an analysis of the results of impacts on the information resources of the Russian Federation, the technical capabilities of the tools. Recommendations for improving the information systems protection system and the composition of a set of priority measures to respond to computer incidents are proposed
Key words: malware, cyber attacks, WAF, computer incident.

Markin D., Mishchenko A., Ho T. Research of Embedded Computer Software Based on Processors with Arm Architecture. – PP. 390–395.
The article presents an approach to research for the presence of potentially dangerous objects of embedded computer software based on processors with ARM architecture (trustlets). The model of the bracelet, the block diagram of the analysis tool, the clustering algorithm of binary files of trustlets are described. The aim of the work is to improve the tools for analyzing embedded software in order to identify vulnerabilities and undeclared opportunities in them. An assessment of the effectiveness of the developed approach in the analysis of trustlets is presented, indicating an increase in the completeness of information about the objects of analysis.
Key words: trustlet, TrustZone, ARM, vulnerabilities, undeclared features.

Markin D., Molchanov N., Shchukin A. The Means of Ensuring the Intelligence Security of Penetration Testing. – PP. 395–400.
The article describes the technology for ensuring the intelligence security of penetration testing tools based on the use of a chain of web proxy servers. The analysis of modern means of penetration testing, as well as anonymization technologies is given. It is shown that in order to transmit network packets through a chain of web proxy servers, it is necessary to implement auxiliary means of broadcasting network packets in an active data scenario in interpreted programming languages. A structural diagram of the intelligence security system is presented. Additional protection measures against compromise of web proxy server network nodes are proposed.
Key words: penetration testing, web proxy, active data, security analysis.

Markin D., Nekrasov D. The Identification Algorithm of Automated Tools that Analyze the Information System. – PP. 400–404.
The article is devoted to the study of approaches to the identification of automated tools (bots) that analyze information systems. The results of a comparative analysis of the known means of automated analysis of information systems are presented. A model of an automated tool and an algorithm for its recognition are proposed. An identification algorithm has been developed.
Key words: bot, analysis tool, information system, identification.

Markin D., Nikiforova E., Shulgin M. The System of Protection Against Unauthorized use of the Website Based on Hasp Technology. – PP. 404–408.
The paper lists and gives a brief description of the modules of the system of protection against unauthorized use of the information system, which is accessed remotely. The structural scheme of the system and the features of the implementation of access restrictions to the information system based on the use of a JaCarta USB key and a subsystem for intercepting system calls with subsequent access filtering and data protection are described.
Key words: USB token, HASP, system call interception, LD_PRELOAD.

Medvedev D., Pinegina I. Analysis of the Application of Systems for Processing of Citizens′ Appeals. – PP. 409–413.
In today's world, open and efficient communication between government agencies and citizens is important. The article presents the current state of the systems for processing citizens' appeals. The most significant problems of the digitalization process of institutions interacting with citizens are identified. The possible effects of the implementation of the system of appeals processing are marked. The prospects for the development of such systems are proposed.
Key words: system of appeals processing, citizens, government agencies, digitalization.

Mikhal G., Smorodin G. Usage of Semantic Models for Drawing up Technical Specifications for Software Development. – PP. 413–417.
A brief analysis of approaches to the preparation of technical specifications and preparation of documentation for software development was carried out. The advantages of the semantic approach to the formation of requirements for the stage of conceptual design and preparation of technical specifications are presented. An example of applying the semantic model at the first stages of the life cycle of application development project is given.
Key words: sketch modeling, semantic model, formalization of technical specifications.

Musaeva T., Urago A. Criteria for Markers of Qualitative Recognition of Augmented Reality Images. – PP. 417–422.
When constructing scenes in augmented reality on mobile devices, the main means of obtaining data about the surrounding world is optical recognition of key real-world objects through the device's main camera. One of the most common ways to identify key points in space is to use image markers. The quality of the projected augmented reality on the screen of a mobile device depends on the speed and quality of recognition of these markers. The purpose of this work is to determine the key criteria of marker images that affect the speed and quality of recognition in an augmented reality environment using the example of the Vuforia software library.
Key words: augmented reality, markers, user interface, Vuforia, visualization.

Ndikumana E. Geo-Information-Based Agricultural Risk management in the Republic of Burundi. – PP. 423–426.
This paper focuses on the challenges facing the agricultural sector in Burundi. It will also analyze possible solutions to reduce the impact pursued by the sector in order to increase the national economy, which is almost entirely based on the agricultural sector.
Key words: geo-informatics, development of a geo-information system for agricultural risk management in the Republic of Burundi.

Nesterov A. Analysis of the Level of Technical Solutions for Situation Centers. – PP. 427–431.
Based on the analysis of the information flow of patent documents of the Russian Federation and software included in the Unified Register of Russian Programs for Electronic Computers and Databases, the main technical solutions for situational centers of various levels and purposes are considered. The dynamics of the activity of registration of intellectual property objects is presented, as well as an assessment of the level of technical solutions. The main directions of development of technical solutions for the functional tasks of a decision support system of a wide class are identified.
Key words: situation center, technical level, decision support.

Nesterova A., Polkov A. Methods of Data Exfiltration. – PP. 431–435.
The paper lists the main types of APT attacks and common exfiltration methods. Their brief description and methods of protection, prevention and leveling the consequences of an attacker's attacks on an automated system are given. Cybercriminal attacks are happening more and more often, and companies need to work out a protection system in such a way as to prevent the maximum number of possible incidents.
Key words: data leakage, data exfiltration, privacy protection, traffic security.

Nogin S. Some Aspects of Constructing a System for Monitoring the Functioning of Computing Infrastructures. – PP. 436–441.
The article deals with the organization of monitoring the functioning of computer networks, the main controlled parameters of monitoring objects are given. Approaches to the construction of systems for monitoring the functioning of computing infrastructures are considered.
Key words: performance monitoring, performance monitoring system, monitoring parameters.

Okladnikov A., Ptitsyna L. Models of the Processes of Functioning of Intelligent Information Agents. – PP. 441–446.
The importance of intelligent information agents for the implementation of artificial intelligence systems in information infrastructures of various scales in the context of the development of the digital economy is shown. The features of the functioning of intelligent information agents in heterogeneous networks are described. Various approaches to the construction of models of the processes of functioning of intelligent information agents in heterogeneous networks are considered. The advantages of extended object-oriented models of intelligent information agents are highlighted. A technique for constructing extended object-oriented models of intelligent information agents is proposed to study the influence of the characteristics of digital communication paths on their dynamic profile.
Key words: artificial intelligence; information agent; model; net; extension; modeling.

Olimpiev A. Process Control System Emulator Architecture. – PP. 446–450.
The article describes the actual problems of creating an integrated automated lifecycle management system related to the heterogeneity of its subsystems. The features of the implementation of software products intended for the organization of joints between these subsystems are considered. The special complexity of the development of software modules interacting with the subsystem of technological process control is noted. The architecture of the emulator program is proposed, which can speed up the process of developing such modules.
Key words: automation of life cycle management, software development, integration of automated systems.

Olimpiev A. Method of Reducing the Diversity of Functionality Description Languages. – PP. 450–454.
The article describes an approach to managing the life cycle of a software product, in which the functionality description language of information systems is chosen as the main object of management. The main stages of the functionality description language life cycle are defined. The actual problems that a software developer faces when choosing this path of software development are formulated.The problem of the diversity of languages, which is observed in many modern systems and is a rather serious obstacle in the development of the described approach, is indicated. The method to solve this problem is proposed.
Key words: software life cycle, metacontrol of functionality, translation and compilation theory, functionality description languages.

Pavlov I. The Python Programming Language. Basic Operations. – PP. 455–460.
The article discusses the history of Python programming, the main distinctive features of the Python language. The basic operators of arithmetic operations, assignment of values and comparison of quantities are also considered. For general understanding, examples are given when working in the Python programming language with the result of execution.
Key words: Python, programming, operators, arithmetic operations, assignment of values, comparison of quantities.

Pelikh D., Filippov F. Review of Solutions for Specialized Automated Documentation Creation. – PP. 460–463.

In the modern world, automation of technological processes, logistics and other things is the most urgent task of many specialists. Automation has affected the information sphere no less. Frameworks with many ready-made solutions, no-code platforms greatly simplify the development of information resources. The creation of documents can also take place in automatic mode, difficulties arise only when the intellectual work of a person is needed. How to get around them will be discussed in this article.

Key words: document management automation, information system, database management, neural networks.

Petrova V., Ptitsyna L. Modeling Service-Oriented Systems with a Soft Architecture. – PP. 463–468.

The development of service-oriented systems with a soft architecture has been updated. Variations in the organization of intelligent service-oriented systems are considered. The conditions for prioritizing the use of majority logic in the organization of service-oriented systems with a soft architecture are described. Alternatives in the modeling of service-oriented systems are highlighted. The quality profile of a service-oriented system is defined. A technique for constructing an extended object-oriented model of service-oriented systems with majority logic is proposed. The results of modeling service-oriented systems with a soft architecture in the case of using the majority logic are presented.

Key words: service-oriented system, architecture, priority, majority logic, quality, modeling, analytics.

Povedaiko M., Chubarova Z. Analysis and Concept of a Browser Extension that Performs Parental Control. – PP. 468–471.

This article discusses the algorithm of the extension function that performs parental control, which will help improve its performance. Unlike other programs of this type, this function is based not on prohibition, but on the educational process. The current statistics of Internet use by children were studied, which showed the importance of the algorithm being developed.

Key words: algorithm, children, parental control, extension.

Pogadaeva O., Shiyan A. IT Product Positioning Strategy Based on the Example of the Device Instruction AR Application. – PP. 471–475.

The purpose of the research is to determine the specifics of developing an IT product positioning strategy. The article focuses on the fact that the product and marketing parts must act together. Positioning is the development of a brand offer and image, which are aimed at forming a competitive position of the brand. The main goal of positioning is to differentiate against the background of competitors, and strengthen their own positions. As a result of the study, the optimal positioning algorithm is presented.

Key words: positioning, it product, ASO, application, branding, user, competitor, smartphone, promotion.

Polyakov O., Shestakov A. Combined Monitoring of Technological Parameters of Oil Trunk Pipelines. – PP. 475–480.

The intellectualization of control tools for automation systems and process control in the oil and gas industry in the digital economy is relevant in a scientific sense and in demand in practice. The results of the study of options for the implementation of the subsystem for collecting technological parameters of the main oil pipeline based on combined wireless access of traditional sensors and means of intelligent video data preprocessing are presented. The system-technical solutions for the construction of an intelligent access point of the main pipeline monitoring facility are proposed.

Key words: sensor, intelligent data preprocessing, wireless access.

Rysiukov M. Color Image Segmentation Based on Different Color Space Models Using Automatic GrabCut. – PP. 481–484.

This paper presents a comparative study using different color spaces to evaluate the performance of color image segmentation using the automatic GrabCut technique. GrabCut is considered as one of the semiautomatic image segmentation techniques, since it requires user interaction for the initialization of the segmentation process. The automation of the GrabCut technique is proposed as a modification of the original semiautomatic one in order to eliminate the user interaction.

Key words: color space, segmentation, GrabCut technique.

Semenova V. Experience in Using the Software Laboratory for Ontological Data Analysis. – PP. 485–489.

Ontologies are one of the leading paradigms for structuring information content, the advantage of which as a means of cognition is a systematic approach to the study of the knowledge domain. Therefore, it is important to develop methods and tools for constructing ontologies, in particular, the automatic derivation of ontologies from given data.

Key words: object-attribute data, ontological analysis, software application.

Torshenko Yu., Yurmanova V. Relevance of Formalization and Development of Tools to Support Creative Processes. – PP. 490–493.

With the development of the digital environment, process automation is becoming increasingly important, there is a demand for means of supporting the professional activities of creative workers. To create such products, it is necessary to formalize all stages of the product life cycle.

Key words: formalization, automation, creative competencies.

Chuprin D. Information Modeling of the Functioning Processes of the Licensing System for the Technical Protection of Confidential Information. – PP. 493–498.

Based on static and technological information models of licensing authority activities at the basic stages of the licensing system functioning for technical protection of confidential information, a dynamic information model determining the possibility to develop automated components of decision-making subsystem of candidate organizations being ready for licensing is developed.

Key words: licensing, technical protection of confidential information, information model, dynamic model, graph, stochastic network model.

THEORETICAL FOUNDATIONS OF RADIO ELECTRONICS AND COMMUNICATION SYSTEMS

Alimov V., Busnyk A., Kuzenov S., Livshits A., Peredistov E. RF Plasma Source for Hydrogen in High-Vacuum Installations. – PP. 499–504.
A portable generator of low-temperature hydrogen plasma for the high-vacuum installation SUPMEM-1 for the study of super-permeability of metal membranes by hydrogen is presented.
Key words: RF low pressure gas discharge, high vacuum equipment.

Alli R., Sedyshev E., Filin V. Investigation of the Frequency Properties of an Ultra-Wideband Cellular Fractal Antenna Structure. – PP. 505–508.
Computer simulation of fractal structure antennas was performed. A study of their frequency properties and their dependence on the antenna power input method has been carried out. The optimization of matching fractal structures in a wide frequency band has been carried out.
Key words: microwave technologies, microwave, antenna systems, computer modeling, fractal antennas, ultra-wideband antennas, broadband antennas.

Alyshev Y., Nikolaev B. Variants of Interpretation of the Section "Transient Processes" in the Theory of Electric Circuits. – PP. 509–512.
The problematic issues of methodological substantiation of transient processes in linear electrical circuits are considered. A different interpretation of transients based on parametric circuits is proposed, as well as the introduction of appropriate experimental circuits into the laboratory practice.
Key words: transients, parametric circuits.

Arsirii A. Thermomechanical Stability of Zirconium-Periclase Dielectric Materials. – PP. 513–516.
One of the most important tasks in modern radioelectronics is obtaining new materials and studying their properties. Ceramic dielectric zirconium dioxide compounds can maintain their original characteristics for a long time, even at high temperature.
Key words: dielectric materials, zirconium ceramics, thermal aging, properties.

Bocharov E., Vasyatkin M., Sedyshev E. Investigation of a Microwave Frequency Selection Device on a Cylindrical Surface. – PP. 516–521.
The paper proposes two configurations of a microwave filter in a cylindrical design on two types of lines: coplanar and microstrip. The simulation of these devices in the RFSimm99 application package is carried out, two layouts and the results of the structure experiment on a microstrip line are presented.
Key words: coplanar waveguide, volumetric ring resonator, microstrip line, cylindrical surface.

Brusin E. Direct Spread Spectrum Signals Demodulator Acquisition based on Fast Fourier Transform. – PP. 522–527.
Direct spread spectrum signals are used widely in various communication and navigation systems. The acquisition problem on carrier frequency and delay is base such systems demodulators filcher. Suggested approach to acquisition problem base on joint estimation these parameters used the Fast Fourier Transform. The acquisition algorithm modeling results are introduced.
Key words: direct spread spectrum signals, acquisition, Fast Fourier Transform.

Vahrameeva V., Sedyshev Y. Problems of Coplanar Waveguide Synthesis and Methods for Estimating its Operating Parameters. – PP. 527–533.
The paper presents the main problems of coplanar waveguide synthesis. The methods of calculating the wave resistance of the transmission line of microwave integrated circuits are compared. Calculation methods are presented from various sources. The theoretical calculation was carried out using an approximating expression.
Key words: coplanar waveguide, calculation, wave resistance.

Velikoborets G., Yurova V. Schematic Solutions for the Design of an Anthropomorphic Robotic Arm Control System. – PP. 534–539.
Anthropomorphic limbs are designed and constructed to mimic human form and movements. Ultimately, they must resemble the size and physical abilities of human limbs in order to function in a human-centered environment. This is extremely important for prosthetics. The article presents the construction of an anthropomorphic arm with 21 degrees of freedom, applicable for use as prosthesis. The schematic implementation of the control system for the condition of the hand drives is presented, as well as an overview of the methods of controlling the limb when it is used as prosthesis.
Key words: semiconductor, medical electronics, semiconductor electronics, anthropomorphic prosthesis, robotics, automation.

Giniyatullin A., Nikitin Yu. Multiple Parallel First Type Digital to Analogue Converter. – PP. 539–542.
The main problems in the construction of parallel digital-to-analog converters (DAC) are the final accuracy of the implementation of analog elements (matrix R-2R, current-voltage switches) in the entire output range of frequencies, currents and voltages. The use of a vernier DAC of the first type makes it possible to circumvent or drastically reduce these contradictions.
Key words: digital-to-analogue converter, R-2R matrix, current keys, voltage keys, quantization step, arithmetic adder, analog adder, vernier, measuring scale.

Glukhov N., Sedyshev E., Fedorov S. Study of the Main Characteristics of the Frame Triangular Structure. – PP. 543–549.
This paper presents the results of modeling, experiment, and their comparison, of a modified triangular antenna to identify the dependences of the influence of geometric characteristics (rib length, length of the feed section) on its electrodynamic characteristics.
Key words: microwave, antenna, triangular antenna.

Golubenko N., Kubalova A. Microwave Filters Synthesis and Design. – PP. 549–553.
An algorithm for designing strip elliptical structures of decimeter and centimeter ranges is presented. A technique for creating a microwave Zolotarev filter by parallel connection of two arrays of coupled lines of the same and unequal electrical lengths using the theory of rod filters is presented. A numerical example of calculating microstrip elliptic filters implemented on a lattices of coupled strips using the theory of rod filters is considered.
Key words: Zolotarev-Kauer filter, narrow-band filter, rod filter, microwave filter, coupled microstrip lines, multi-wire line, electromagnetic simulation, finite element method.

Grishin V., Petrova E., Terushkina O., Trofimushkin M. Method of Calculation of Primary and Secondary Optics of Semiconductor Emitting Diodes to Ensure a Given Light Distribution. – PP. 553–556.
The objective of optical calculations in the design of semiconductor light-emitting diodes (LEDs) is to obtain an optical system that allows you to output the maximum possible amount of light energy from the primary source (p-n junction, at which electron-hole pairs recombine with the release of optical range energy proportional to the band gap width) to a given angle. Traditionally, this problem is solved by installing a polymer lens on a semiconductor crystal.
The use of algorithms for calculating the primary optics of LEDs allows us to numerically solve the problems of determining the profile of the lens dome when designing LEDs in order to increase their energy efficiency, to ensure the required distribution of the luminous flux emitted by the semiconductor structure. The paper considers the existing methods of such analysis, and evaluates their accuracy.
Key words: semiconductor, optics, semiconductor electronics, luminous flux, illumination.

Derzhavin M., Sedyshev E., Antenna Array on Dielectric Rods for Satellite Communication Systems. – PP. 557–562.
The paper compares mirror parabolic antennas and dielectric horns. The main problems of using antennas of these types in satellite systems are considered. Based on the results of the calculations, a layout was created, an experiment was carried out, conclusions were drawn about the possibility of optimizing the obtained characteristics of the device, the feasibility and prospects for using the proposed design in satellite communication systems.
Key words: *microwave, dielectric antenna, satellite communication*

Dorohin V., Sedyshev E. Input Power Divider for a Diplexer in a Volumetric Integral Design. – PP. 562–567.
The paper considers a method for implementing a power divider for a diplexer in a volumetric integral form. A block diagram has been proposed, and a working layout of the T-divider has been created.
Key words: microwave, power divider, volumetric integrated circuit.

Dunaeva R., Sedyshev E. Electrodynamic Simulation of a Planar System of 4 Slot Emitters. – PP. 567–572.
The paper considers the possibility of building a computer model of a planar system of 4 slot emitters using the MMana Gal electrodynamic package, proves the full performance of the antenna system, and evaluates the main parameters of the model that affect the characteristics of the system. Experiments were carried out and the results were evaluated.

Key words: planar system, slot radiator, electrodynamic modeling.

Ivanishcheva E., Sedyshev E. Investigation of the Properties of Distributed Capacity on the Strip Line. – PP. 572–578.
The paper considers the main characteristics of structural containers in the form of a planar line overlap and a collinear end gap. Prototyping of these tank designs is carried out, results of mathematical calculation, computer simulation and experiment are given. Based on the study, it is concluded that the real equivalents of the proposed structures have a number of features inherent in connected lines.
Key words: microwave, capacitance, microstrip line, frequency selection.

Illarionov A., Yurova V. Analysis of Ways Design Amplifiers for Autogenerators with Low Noise Level. – PP. 579–584.
Optoelectronic devices for various purposes are of particular interest and open up new prospects for the development of electronics, optics and circuitry. Optical information transmission systems have fundamental, competitive advantages, such as high information capacity of optical communication channels, small mass-dimensional dimensions in comparison with microwave waveguides, high noise immunity, exclusion of mutual interference and parasitic connections between functional nodes of the electrical circuit, etc. Important in the proper and stable operation of optoelectronic devices is the provision of protection from electric power. The paper considers the basic structures of diode drivers. Their classification, analysis of the structural construction of electrical circuits, their characteristics are carried out. The main advantages and disadvantages are shown.
Key words: optoelectronics, semiconductor LEDs, power supply, stabilization, semiconductor electronics.

Katkova T., Sedyshev E. Synthesis of a Microwave Generator Based on a Ring Elliptical Resonator According to Operating Parameters. – PP. 584–589.
The work is devoted to the study of the design of microwave ring resonators on planar transmission lines. The paper compares ring resonators on a balanced and unbalanced transmission line, evaluates the quality factor of two layouts, analyzes the effect of the ring width on the main characteristics. Produced mathematical modeling, mathematical calculation.
Key words: microstrip line, balanced line, ring resonator, resonance frequency, loss tangent, quality factor, dielectric losses.

Knyazev S., Kolgatin S., Urvantseva N. Determination of Parameters of an Unknown Planet Based on Indirect Mechanical Measurements. – PP. 590–593.
The paper defines the characteristics of an unknown planet – the acceleration of free fall, and through it – such global, and, it would seem, difficult to measure parameters as the mass and diameter of the planet. The acceleration of free fall is found from the results of computer experiments on the rolling of the body (solid and thin-walled cylinders and ball) along the inclined plane. The mass and diameter of the planet are determined on the basis of the law of universal gravitation and additional data on the density of the soil. Planet parameters can vary,

creating a bank of individual tasks for individual unknown planet students, deriving working formulas, accelerating free fall, mass and diameter of the planet.
Key words: unknown planet, derivation of working formulas, acceleration of free fall, mass and diameter of the planet.

Kniazev S., Kolgatin S., Sharikhina Yu. Processing of Measurement Results by Means of Integrating and Differencing Procedures. – PP. 593–599.
The advantage of measurement result processing by means of integrating and differencing procedures compared with traditional methods is shown on the examples of the presentation on the error theory, "The motion of objects in a viscous fluid" laboratory research, the method of poor signal filtration on the background of powerful noise and the analysis of electric current distribution of secondary electrons.
Key words: integrating and differencing procedures.

Knyazev S., Kolgatin S. Reproduction of the Cornerstone Experiment of Quantum Mechanics – the Davisson and Germer Experiment on Electron Diffraction. – PP. 599–603.
Davisson and Germer's experiments on electron diffraction, conducted in 1927, experimentally confirmed de Broglie's hypothesis of wave-particle duality, thereby laying the foundation for quantum mechanics. This paper reproduces this experiment on modern equipment in an ultra-high vacuum with control over the structure and chemical composition of the surface of the recrystallized nickel sample.
Key words: electron diffraction, wave-particle duality.

Knyazev S., Kolgatin S. Installation for Demonstration of Mutual Conversion of Electric and Magnetic Fields. – PP. 603–607.
The theoretical foundations of radio communication are laid down in Maxwell's equations: a time-varying magnetic field is the source of a vortex electric field, electric currents and an alternating electric field are a source of a vortex magnetic field. This work refers to the origins of the emergence of wireless energy transmission – the famous experiments of Hertz.
Key words: Hertz's experience, Maxwell's equations.

Knyazev S., Kolgatin S. Computer Modeling of Electrostatic Fields. – PP. 607–612.
The paper sets the task of reproducing a qualitative picture of the interposition of equipotentials for the flat capacitor system - a conductor with a triangular cross-section standing on the lower plate. Students are asked to reproduce this picture in a playful manner, taking into account the fact that away from the sharp-angled conductor, the set of equipotentials is a system of lines parallel to the plates, and near the tip these lines must "leak" through the gap between the upper plate and the apex of the tip. Next, it is proposed to estimate the distribution of charge density on the upper and lower plates, as well as on the surface of the conductor with a triangular cross-section.
Key words: electrostatic field, equipotentials, conductors in electric field.

Knyazev S., Obidov B. Diffraction on a Corrugated Surface in Kinematic Approximation. – PP. 613–619.
Within the framework of the kinematic theory of scattering, the features of diffraction on surface corrugated structures are considered. It is shown that these structural defects lead to significant changes in the intensity and shape of diffraction maxima compared to the diffraction pattern from an ideal surface.
Key words: diffraction, corrugated surface, kinematic approximation.

Knyazev S., Obidov B. Diffraction on a Structure of Disoriented Blocks in Kinematic Approximation. – PP. 619–624.
Within the framework of the kinematic theory of scattering, the features of diffraction on surface structures consisting of separate two-dimensional blocks lying in the same plane and oriented relative to each other are considered. It is shown that interference effects due to interblock scattering do not have a significant effect on the intensity of reflexes from each of the blocks and do not lead to the appearance of new diffraction maxima. The exception is the maximums of the mirror image.
Key words: the kinematic theory of scattering, two-dimensional blocks.

Knyazev S., Obidov B. Diffraction on a Step Structure in Kinematic Approximation. – PP. 624–630.
Within the framework of the kinematic theory of scattering, the features of diffraction on surface structures consisting of ordered and disorderly arranged steps are considered. It is shown that these structural defects lead to significant changes in the intensity and shape of diffraction maxima compared to the diffraction pattern from an ideal surface.
Key words: diffraction, stepped surface, kinematic approximation.

Konovalova E., Motrenko V., Sedyshev E. Use of Truncated Volumes as Microwave Resonators. – PP. 630–636.
The paper shows the stages of research of truncated resonators: hemispherical, semi-cylindrical, hemispheroidal. For these structures a comparative analysis of quality factors is made, experimental confirmation of their performance is given. Resonator in the form of flattened hemispheroid is described in most detail, since its study is a logical conclusion of a large series of works.
Key words: microwave resonator, half resonator, truncated resonator, microwave generator.

Kravets E. Sensivity of the Interferometric System for the Detection of Oscillations in High-Precision Crystal Resonators. – PP. 636–641.
Due to the fact that in the design of high-precision crystal oscillators deriving an analytic formula to rigorously describe oscillations proves impracticable, researches have been done into optical methods to control dynamic amplitude distribution across the surface of crystal. The order of magnitude of the amplitude of oscillations in high-precision crystal resonators in few to tens of angstroms. The scheme of Michelson interferometer-based measuring apparatus is presented in the paper, with the analysis of its parameters. Observations of how the parameters of the apparatus influence the interference pattern, as well as how noise affects the operation of the system, have been made to estimate sensitivity. The range of amplitudes to be possibly measured has also been ganged in this work.

Key words: resonator, Michelson interferometer, sensivity.

Landa A., Nikitina T., Sedyshev E. Generator with a Controlled Resonator on a Ferrospinel. – PP. 641–644.
This paper presented the development of a controlled generator on ring resonators on a ferrospinel substrate. A structurally complex line consisting of two different substrates was proposed. An experiment with the proposed model of controlled generator was carried out.
Key words: microwave, generator, ring resonator, ferrospinel, wave resistance, ferrite substrate, strip line.

Larionova A., Sedyshev E. Investigation of a Microwave Generator on an Annular Resonator Taking into Account the Equivalent of an Active Bipolar. – PP. 645–651.
The paper presents the results of a series of experiments aimed at increasing the power of the microwave generator. Two-pole devices with negative resistance (tunnel diodes) were used as active elements. Unfortunately, the studied models of generators showed themselves to be noise generators, while the noise mode with two two-poles gave a noticeable increase in the output noise level. The paper explains this effect (by creating an exact model of the generator) taking into account the equivalent circuit of the active element. The conclusion is made about the impossibility of installing diodes at one point.
In conclusion, a method is proposed to increase the power of the generator by adding the power from two identical ring generators located in different layers of a volumetric integrated circuit.
Key words: equivalent circuit, microwave, generator, active bipolar, resonator, noise.

Mezhevova M., Filin V. Investigation of Nonlinear Resonances in Class D Amplifiers with Negative Feedback. – PP. 651–654.
The technique of computer simulation of frequency characteristics of key (nonlinear) power amplifiers operating in Class D mode is described. The technique takes into account the spectra of real steady-state processes that occur under the influence of harmonic perturbation in a closed negative feedback loop. The results of calculations are presented and analyzed.
Key words: key power amplifiers, closed loop method, nonlinear closed systems.

Nikitin Yu. Reduction of the Level of Discrete Interference in the Synthesizer Rings of Pulse-Phase Frequency Auto-Tuning. – PP. 655–660.
The main methods of active digital-to-analog frequency synthesis are considered, which allow ensuring the required quality of the generated oscillations and minimizing the level of discrete side spectral components (DPSS). They are classified. The main advantages and disadvantages are shown.
Key words: ring of pulse phase-locked loop of frequency, pulse counter, accumulating adder, vernier, side spectral components (spurs).

Nikitin Yu. Passive Digital Synthesis Based on an Accumulator and a Divider with a Fractional-Variable Division Ratio. – PP. 660–666.
Passive methods of digital frequency synthesis based on an accumulator and a divider with a fractional-variable division ratio, supplemented by a controlled delay device, are considered. Such synthesizers are used in modern frequency synthesis systems and make it possible to

ensure the required quality of the generated oscillations. The main advantages and disadvantages are shown.
Key words: Passive digital frequency synthesis (DDS), finite state machine (FSM), modified two-level finite automaton (MFSM), impulse counter, accumulating adder (AA), controlled delay device (CDD).

Nikitin Yu. Using the Controlled Device of Delay «Code-Voltage-Time» in a Passive Digital Synthesis. – PP. 666–671.
Methods of passive digital frequency synthesis based on an accumulator and a divider with a fractional-variable division ratio, supplemented by a controlled delay device, are considered. Delay control is necessary to reduce the functional pulse-phase modulation inherent in this frequency synthesis method. The controlled delay device is built on the basis of intermediate transformations of the delay code into the time interval. The structure of the device and the requirements for its elements are considered.
Key words: passive digital frequency synthesis (DDS), finite state machine (FSM), modified two-level finite state machine (MFSM), pulse counter, accumulating adder (AA), controlled delay device (CDD), stable current generator, current (voltage) switch, digital-to-analog converter, comparator.

Nikitin Yu. Control of the Time Delay of Pulsed Signals in the Nanosecond Range. – PP. 671–676.
Methods for controlling the time delay of active transitions of digital devices - finite automata are considered. Controlled delay devices are used in modern frequency synthesis systems and make it possible to provide the required quality of the generated oscillations.
Key words: controlled delay device (CDD), modified two-level finite state machine (MFSA), stable current generator, current and/or voltage switch, pulse counter, accumulating adder (AA).

Nikitin Yu., Smotrov V. ADF4158 Fractional Synthesizer Chip and Signal Functions. – PP. 676–680.
The structure and description of the operation of the microcircuit of the ADF4158 broadband microwave frequency synthesizer, which operates in the frequency range from 0.5 GHz to 6.1 GHz with control over a three-wire serial interface and allows software scanning by frequency with specified parameters for the range and scanning time, are presented.
Key words: frequency synthesis, radio communication, spectrum, phase-locked loop, phase noise, control, interface, signal, register, scanning.

Oberti K., Yurova V. Ways of Designing Electronic Access Control and Management Systems. – PP. 681–685.
The paper considers modern ways of designing electronic access control and management systems. The analysis of the technical features of the implementation of the system of scanning and identification of the user is carried out, a concept for the development of an electronic access control and management system based on the registering of the user's biometric data is proposed. The method of reading in the form of biometric identification by the pattern of the veins of the palm is considered.
Key words: medical electronics, optoelectronics, diagnostic equipment, preventive medicine, laser technology, biomedicine, electronic access systems.

Rumyanceva A., Sedyshev У. Quasi-Lumped LC-Circuit in Hybrid for Microwave Devices. – PP. 686–689.

The paper describes a new element of integrated circuitry - a "hybrid" of helical inductance and planar capacitance. he calculation of the main electrical and geometric parameters of the elements of the LC-circuit is presented. One of the options for the execution of a hybrid integrated circuit with its further prototyping is proposed. The operation of a circuit consisting of a round planar capacitance and a spiral inductance has been investigated .

Key words: integrated circuits, microwave frequencies, flat circular spiral inductors, round planar capacitance.

Surkov E., Filin V. Development a Doherty Microwave Power Amplifier Model using the Parameters of a Real transistor. – PP. 690–694.

Described the mechanism of the Doherty power amplifier. The transistor tuning model was created in the Fastmean program using a piecewise linear scheme for replacing high-power GaN transistors. The amplifier operation modes were adjusted and checked.

Key words: power amplifier, Doherty, Fastmean, microwave transistor amplifier, class AB amplifier, class C amplifier.

Yurova V. Optimization of Vacuum Deposition Modes on Gallium Nitride Structures. – PP. 695–698.

LED technology is currently widespread in various fields of electronics. The main characteristics of the LED structure are determined by the properties of the materials and the peculiarity of its manufacture. The paper presents the results of optimizing the technological process of forming ohmic contacts of an LED structure based on gallium nitride.

Key words: LED, semiconductor, TIR structure, optoelectronics, semiconductor technology, thin-film technologies.

СВЕДЕНИЯ ОБ АВТОРАХ

АВЕРЕНКОВА Мария Анатольевна — сотрудник Академии Федеральной службы охраны Российской Федерации, s.kop@acdem.msk.rsnet.ru

АВРАМЕНКО Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АКИМОВ Сергей Викторович — кандидат технических наук, доцент, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov-sv@yandex.ru

АЛЕКСЕЕВА Мария Ивановна — старший преподаватель кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ma9217988064@gmail.com

АЛИМОВ Василий Николаевич — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alimov_vasilii@mail.ru

АЛЛИ Рашид Амидуевич — студент группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rashid.alli@yandex.ru

АЛЫШЕВ Юрий Витальевич — кандидат технических наук, доцент кафедры теоретических основ радиотехники и связи Поволжского государственного университета телекоммуникаций и информатики, alise-17@mail.ru

АМЕЛЬЧЕНКО Дарья Олеговна — студентка группы ИСТ-913 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dahenca001@gmail.com

АНДРЕЕВ Игорь Леонидович — сотрудник Академии Федеральной службы охраны Российской Федерации, ail@yandex.ru

АРЕСТОВ Антон Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, arestow@bk.ru

АРСИРИЙ Алла Ивановна — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ars-alla@rambler.ru

АРХИПОВ Павел Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

БАРАНАУСКАС Максим Эдвардасович — студент группы ИБ-72з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

БАЯГАНТАЕВА Екатерина Васильевна — студентка группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.bayagantaeva@mail.ru

БЕДНЯК Светлана Геннадьевна — кандидат педагогических наук, доцент, зам. заведующего кафедрой информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики, lanusik@mail.ru

БЕРЕСТОВСКИЙ Павел Андреевич — оператор 7 роты (научной) Главного управления связи вооруженных сил Российской Федерации, vas@mil.ru

БОВШИК Павел Павлович — магистрант кафедры информационных управляющих систем, студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pbovshik@mail.ru

БОЛОГОВА Анна Васильевна — студентка группы РБМ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bologova.ann@yandex.ru

БОЧАРОВ Евгений Иванович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, es.ffp@net.sut.ru

БОЯШОВА Елена Петровна — старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helen.glass@mail.ru

БРАЖНИКОВ Дмитрий Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, dmitry.brazh@yandex.ru

БРУСИН Ефим Александрович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; ведущий инженер АО «РИРВ», yefim07@inbox.ru

БРЫЛЕВ Михаил Евгеньевич — студент группы ИСТ-822 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mixa228227226@gmail.com

БУЛГАКОВ Дмитрий Олегович — сотрудник Академии Федеральной службы охраны Российской Федерации, bylgakov46@gmail.com

БУСНЮК Андрей Олегович — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreibusnyuk@mail.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut-ispiu@mail.ru

ВАСИЛЬЕВ Матвей Александрович — студент группы ИСТ-041м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, waytokey@mail.ru

ВАСИЛЬЕВ Никита Алексеевич — командир взвода (научного) – младший научный сотрудник роты (научной) Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

ВАСЯТКИН Михаил Андреевич — студент группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasyatkinmix@yandex.ru

ВАХРАМЕЕВА Валентина Сергеевна — студент группы ФП-11м Санкт-Петербургского университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, valentina.vaxrameewa@yandex.ru

ВЕЛИКОБОРЕЦ Глеб Сергеевич — студент 4 курса факультета радиотехнологий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, velikoborecz90@mail.ru

ВЕРХОВА Галина Викторовна — доктор технических наук, профессор, заведующая кафедрой интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina500@inbox.ru

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник Научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного; сотрудник специализированной группы подразделения проректора по безопасности Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ra1alo@mail.ru

ГАВРИЛОВ Илья Вячеславович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, ilya_vch@pisem.net

ГАЛИМОВА Екатерина Юрьевна — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galim81@mail.ru

ГВОЗДКОВ Игорь Вячеславович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gvozdkov@rambler.ru

ГИНИЯТУЛЛИН Александр Эдуардович — студент группы ФП-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kompot26452@mail.ru

ГЛЕБОВ Александр Витальевич — оператор 7 роты (научной) Главного управления связи вооруженных сил Российской Федерации, vas@mil.ru

ГЛУХОВ Николай Иванович — старший преподаватель кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, es.ffp@net.sut.ru

ГОЛУБЕНКО Наталья Ивановна — старший преподаватель кафедры теоретических основ телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aeb@hotbox.ru

ГОЛУБЕНКОВ Георгий Леонидович — сотрудник Академии Федеральной службы охраны Российской Федерации, g.g.first@yandex.ru

ГОНЯЕВ Степан Сергеевич — студент группы ИСТ-913 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Scorpion1999@mail.ru

ГОРБАЧЕВ Павел Николаевич — сотрудник Академии Федеральной службы охраны Российской Федерации, png@academ.msk.rsnet.ru

ГОРОХОВ Денис Евгеньевич — сотрудник Академии Федеральной службы охраны Российской Федерации, gde@inbox.ru

ГРИГОРЬЕВА Елена Николаевна — студентка группы ИСТ-841 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lana.pilot@yandex.ru

ГРИШИН Валерий Валерьевич — студент группы ФП-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, valeriy.01@bk.ru

ГРОМОВА Наталья Николаевна — кандидат экономических наук, главный специалист отдела организации научной работы студентов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nn_gromova@bk.ru

ГУБИН Александр Николаевич — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gan50_60@mail.ru

ГУНИНА Ангелина Александровна — студентка группы ИСТ-812 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gellgunya765@gmail.com

ГУСЕВ Андрей Сергеевич — оператор 7 роты (научной) Главного управления связи вооруженных сил Российской Федерации, vas@mil.ru

ДАМДИНОВ Баир Булатович — студент группы ИСТ-112м кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, damdinov99@mail.ru

ДЕНИСОВА Юлия Вячеславовна — ассистент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, All0122@yandex.ru

ДЕРЖАВИН Михаил Валерьевич — студент группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, derzhavin.mv@yandex.ru

ДИЯЗИТДИНОВА Альфия Асхатовна — старший преподаватель кафедры информационных систем и технологий Поволжского государственного университета телекоммуникаций и информатики, alphiya.diyazitdinova@gmail.com

ДМИТРИЕНКО Данила Сергеевич — студент группы ИСТ-841 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, over900051@gmail.com

ДОБРЫШИН Михаил Михайлович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, dobrithin@yandex.ru

ДОРОХИН Вячеслав Николаевич — студент группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dorohin.vn@yandex.ru

ДУНАЕВА Регина Игоревна — студентка группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sokovih_regina@mail.ru

ЕЛИСЕЕВ Никита Константинович — студент группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, nikita.eliseev998@gmail.com

ЕРМОЛАЕВ Данила Андреевич — студент группы ИСТ-812 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

ЕСАЛОВ Кирилл Эдуардович — начальник научно-образовательного центра «Инфокоммуникационных технологий и нейрокогнитивных архитектор» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yk@bonch-ikt.ru

ЗАЛЕССКИЙ Иван Андреевич — студент группы ИСТ-921 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivan_zal@inbox.ru

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, декан факультета информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zikratov.ia@spbgut.ru

ЗИКРАТОВА Татьяна Викторовна — преподаватель кафедры информационных технологий Военного института (Военно-морского политехнического) ВУНЦ ВМФ «Военно-морская академия», ztv64@mail.ru

ИВАНИЩЕВА Елизавета Федоровна — студентка группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elizaveta.ivanischeva@yandex.ru

ИВАНОВ Василий Геннадьевич — кандидат военных наук, доцент, заместитель начальника 20 кафедры «Боевое применение войск связи» Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

ИВАНОВ Роман Сергеевич — студент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, romaiv99@gmail.com

ИЗОТОВ Никита Вадимович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Konstantin.Izrailov@mail.ru

ИЛЛАРИОНОВ Александр Михайлович — студент группы ФП-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, illarionov_alexandr00@mail.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, доцент, старший преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

КАЗАНЦЕВ Андрей Олегович — оператор роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

КАЛАШНИКОВ Олег Эдуардович — оператор 7 роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

КАНЧАЛАН Сергей Дмитриевич — курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, ser.kan241298@gmail.com

КАРАЕВ Даниил Викторович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

КАТКОВА Татьяна Олеговна — студентка группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tatyana.katkova.98@mail.ru

КИЛЬДЯЕВ Иван Валентинович — студент группы ИСТ-923 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kildyaev.ivan@gmail.com

КИРЬЯНОВ Александр Владимирович — кандидат технических наук, сотрудник кафедры безопасности сетевых технологий Академии Федеральной службы охраны Российской Федерации alex1175@rambler.ru

КНЯЗЕВ Егор Иванович — сотрудник Академии Федеральной службы охраны Российской Федерации, knyazev_egorushka@yandex.ru

КНЯЗЕВ Сергей Александрович — доктор физико-математических наук, профессор кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, knyazef@yandex.ru

КОВАЛЕВ Алексей Андреевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, marinakova817@gmail.com

КОЖАНОВ Юрий Федорович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juriy.kozhanov@mail.ru

КОЗАЧОК Александр Васильевич — доктор технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, a.kozachok@academ.msk.rsnet.ru

КОЛБИНА Ольга Николаевна — кандидат технических наук, доцент кафедры «Прикладная информатика» Российского государственного гидрометеорологического университета, lolikkolbik@gmail.com

КОЛГАТИН Сергей Николаевич — доктор технических наук, профессор кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КОЛЕСНИКОВ Александр Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, alexlion@inbox.ru

КОЛМАКОВА Дарья Андреевна — студентка группы ИСТ-841 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kolmakova2011@mail.ru

КОЛОСКОВ Никита Андреевич — студент группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikita.koloskooov@gmail.com

КОНОВАЛОВА Елизавета Александровна — аспирантка кафедры электроники и схемотехники Санкт Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч Бруевича, konowalowa.elizaweta@yandex.ru

КОПЫЛОВ Сергей Александрович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, gremlin.kop@mail.ru

КОРЧЕВНОЙ Павел Павлович — курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

КОСЫРЕВ Никита Дмитриевич — сотрудник Академии Федеральной службы охраны Российской Федерации, nekitkosyrev@gmail.com

КОТЛОВА Мария Владимировна — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkotlova@gmail.com

КРАВЕЦ Елена Валентиновна — кандидат технических наук, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helen-kravetz@yandex.ru

КРИВОЛАПОВ Даниил Антонович — студент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkrivola@ya.ru

КРЫЛОВА Элеонора Ринатовна — аспирантка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eleonora.davletshina@mail.ru

КУБАЛОВА Анна Рудольфовна — кандидат технических наук, доцент кафедры теоретических основ телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kubalovaap@mail.ru

КУДРЯВЦЕВ Алексей Олегович — командир роты (научной) – старший научный сотрудник роты (научной) Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

КУЗЕНОВ Сергей Ризабекович — аспирант кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skuzenov@ya.ru

КУЗНЕЦОВА Анастасия Александровна — студентка группы ИСТ-92 Поволжского государственного университета телекоммуникаций и информатики, anastaskuz16@yandex.ru

КУЗЬМИНА Дарья Денисовна — студентка группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ddkuzmina@yahoo.com

КУПЧИНЕНКО Ольга Павловна — преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, k-olga102@yandex.ru

КУРНОСОВ Валерий Игоревич — доктор технических наук, профессор кафедры автоматизации предприятий связи Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, vi-kurnosov@mail.ru

КУШАКОВ Евгений Александрович — студент группы ПИ-Б19-1 Российского государственного гидрометеорологического университета, kushakov.evgenii@gmail.com

ЛАНДА Александр Эдуардович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, es.ffp@net.sut.ru

ЛАПКО Александр Николаевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, lan46@mail.ru

ЛАРИОНОВА Александра Константиновна — студентка группы ФП-11М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 06012000larionova@gmail.com

ЛЕБЕДЕВ Никита Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ЛЕВИЧЕВА Юлия Андреевна — сотрудник Академии Федеральной службы охраны Российской Федерации, zusha@bk.ru

ЛИВШИЦ Александр Иосифович — доктор физико-математических наук, профессор кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, livshits@sut.ru

ЛИКАРЬ Александр Иванович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, likar_a@mail.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

ЛИТВИНОВ Владислав Леонидович — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича vlad.litvinov61@gmail.com

ЛОГВИНОВА Екатерина Александровна — студентка группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, logvinova.katua@gmail.com

ЛОМАНОВ Александр Александрович — оператор 7 роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

МАКАРОВ Леонид Михайлович — кандидат технических наук, доцент кафедры интеллектуальные системы автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, biopet@mail.ru

МАКЕЕВ Владимир Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, png@academ.msk.rsnet.ru

МАКЕЕВ Сергей Михайлович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, maksm57@yandex.ru

МАЛЮКОВ Владислав Олегович — старший оператор роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

МАМАДАЛИЕВ Дамир Ринатович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

МАРЗАГАНОВ Георгий Игоревич — студент группы ИСТ-913 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marzaganov.g.i@gmail.com

МАРКИН Дмитрий Олегович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

МАРТЫНОВ Даниил Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mart_da@yandex.ru

МАТЮХИН Демитрий Сергеевич — студент группы ПИ-Б20-1-1 Российского государственного гидрометеорологического университета, dimmat99@gmail.com

МЕДВЕДЕВ Дмитрий Сергеевич — студент группы ИСТ-812 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ds1000one@gmail.com

МЕЖЕВОВА Мария Александровна — ассистент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.kondrashova2010@yandex.ru

МЕЛЬНИКОВ Максим Владиславович — студент группы ИСТ-932 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxim.mel4985@gmail.com

МИРОНЕНКОВА Мария Александровна — студентка группы ИСТ-831 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mironenkovva@mail.ru

Михаль Георгий Андреевич — студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, georgemihal@yandex.ru

МИЩЕНКО Артем Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

МОЛЧАНОВ Николай Николаевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

МОТРЕНКО Валентин Иванович — студент группы ФП-01м Санкт Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч Бруевича, motrenko mw@yandex.ru

МУСАЕВА Татьяна Вагиф кызы — кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru

НДИКУМАНА Элиас — аспирант кафедры прикладной информатики по направлению «геоинформатика» Российского государственного гидрометеорологического университета, eliasndikuman@gmail.com

НЕВРОВ Алексей Александрович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, newrow@mail.ru

НЕКРАСОВ Дмитрий Олегович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

НЕСТЕРОВ Алексей Альбертович — начальник управления организации научной работы и подготовки научных кадров Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aanest@rambler.ru

НЕСТЕРОВА Анна Алексеевна — сотрудник Академии Федеральной службы охраны Российской Федерации, Nanny99@bk.ru

НИЗАМОВ Асхат Ринатович — старший оператор 7 роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

НИКИТИН Алексей Владимирович — Студент группы ИКВТ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikitin2012alex@gmail.com

НИКИТИН Юрий Александрович — кандидат технических наук, старший научный сотрудник, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; начальник лаборатории Санкт-Петербургского филиала ФГУП НИИР-ЛОНИИР, yuriyan@list.ru

НИКИТИНА Татьяна Владимировна — студентка группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxita1507@yandex.ru

НИКИФОРОВА Екатерина Алексеевна — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

НИКОЛАЕВ Борис Иванович — доктор технических наук, профессор кафедры теоретических основ радиотехники и связи Поволжского государственного университета телекоммуникаций и информатики, ibn41@mail.ru

НОВИКОВ Егор Анатольевич — студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egoredmc@gmail.com

НОГИН Сергей Борисович — кандидат технических наук, доцент, старший преподаватель кафедры Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, sprintnsb@mail.ru

ОБЕРТИЙ Карина Вячеславовна — студентка группы РБМ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k.v.oberti@gmail.com

ОБИДОВ Барзу Абдувахобович — кандидат физико-математических наук, научный сотрудник лаборатории физики прочности Физико-технического института АН РФ им. А. Ф. Иоффе, barzu61@mail.ru

ОВСЯННИКОВ Даниил Владимирович — студент группы ИСТ-041м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danya_ovsyannikov@mail.ru

ОКЛАДНИКОВ Артем Романович — студент группы ИСТ-011м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemch@inbox.ru

ОЛИМПИЕВ Алексей Александрович — кандидат технических наук, доцент кафедры интеллектуальные системы автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aao_82@mail.ru

ОРЕХОВ Аркадий Андреевич — студент группы ИСТ-831 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arckadyor1@yandex.ru

ОСТРОУМОВ Олег Александрович — кандидат технических наук, докторант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ПАВЛОВ Иван Иванович — академик МАС, кандидат технических наук, доцент, заведующий кафедрой систем автоматизированного проектирования, доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, iipavlov02@mail.ru

ПАВЛОВИЧ
Артур Александрович
кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, fathertal@mail.ru

ПАЛЕЕВА
Екатерина Ильинична
студентка группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paleeva_k@mail.ru

ПАЧИН
Андрей Владимирович
кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pachin.andrej@bk.ru

ПЕЛИХ
Дмитрий Александрович
студент 2 курса магистратуры кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elektronstandart@bk.ru

ПЕРЕДИСТОВ
Евгений Юрьевич
кандидат технических наук, и.о. заведующего кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч- Бруевича, peredistov.eu@net.sut.ru

ПЕСТЕРЕВ
Владислав Евгеньевич
курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, pesterev0202@mail.ru

ПЕТРОВ
Даниил Юрьевич
студент группы ИСТ-913 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Danyape@yandex.ru

ПЕТРОВА
Вера Евгеньевна
студентка группы ИСТ-111м кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrova.vera.ev@gmail.com

ПЕТРОВА
Екатерина Дантесовна
старший преподаватель кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konferenciya.4@mail.ru

ПИНЕГИНА Ирина Витальевна — преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pineginaiv@bk.ru

ПИНИН Дмитрий Владимирович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ПЛЕТНЕВ Ярослав Андреевич — аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pletnevyaroslav@gmail.com

ПОВЕДАЙКО Максим Дмитриевич — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 89119854561@yandex.ru

ПОГАДАЕВА Ольга Павловна — студентка группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgakoelliker14@gmail.com

ПОЛЕХИН Александр Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, s.kop@acdem.msk.rsnet.ru

ПОЛКОВ Анатолий Анатольевич — кандидат технических наук, доцент кафедры безопасности сетевых технологий, сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ПОЛЯКОВ Олег Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vrnu2000@yandex.ru

ПОПОНИН Антон Сергеевич — студент группы ИСТ-111М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, apoponin@naint.ru

ПРОКОПЕНКОВ Владислав Игоревич — сотрудник Академии Федеральной службы охраны Российской Федерации, prokopenkovvlad@yandex.ru

ПРОКОФЬЕВ Павел Александрович — аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pprokfv@gmail.com

ПРОТАСЕНЯ Сергей Витальевич — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saitvodabur@yandex.ru

ПТИЦЫНА Лариса Константиновна — доктор технических наук, профессор, заведующая кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru

ПУЗАНОВ Иван Сергеевич — студент группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivan.puzanov140@icloud.com

РЕФОРМАТ Андрей Николаевич — сотрудник Академии Федеральной службы охраны Российской Федерации, zusha@bk.ru

РОГОЗИНСКИЙ Глеб Гендрихович — доктор технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb.rogozinsky@gmail.com

РОЖДЕСТВЕНСКИЙ Дмитрий Борисович — студент группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitriifoxqq2@gmail.com

РОМАНОВ Никита Евгеньевич — студент группы ИКБ-84 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikitaromanoov@gmail.com

РУЙГО Даниил Иванович — студент группы ИСТ-012м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, smolldru@gmail.com

РУМЯНЦЕВ Максим Александрович — оператор роты (научной) Главного управления Связи Вооруженных Сил Российской Федерации, vas@mil.ru

РУМЯНЦЕВА Анастасия Максимовна — студентка группы ФП-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amrumyanceva@yandex.ru

РЫСЮКОВ Максим Игоревич — старший оператор 7 роты (научной) Главного управления связи вооруженных сил Российской Федерации, vas@mil.ru

САРАНЦЕВ Алексей Андреевич — студент группы ИСТ-832 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alxsar98@gmail.com

СЕДЫШЕВ Эрнест Юрьевич — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, laboratoria-mw@yandex.ru

СЕМЕНОВА Валентина Андреевна — аспирантка кафедры прикладной математики и информатики Самарского государственного технического университета, младший научный сотрудник ИПУСС РАН – СамНЦ РАН, queenbfjr@gmail.com

СЕРГИЕНКО София Сергеевна — студентка группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ssssofisss@gmail.com

СИЗОВ Никита Дмитриевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

СИНДЕЕВ Максим Александрович — старший оператор 7 роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

СИНЮК Александр Демьянович — доктор технических наук, доцент, профессор кафедры «Общепрофессиональных дисциплин» Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, eentrop@rambler.ru

СКАКУНОВ Руслан Сергеевич — старший оператор роты (научной) Главного управления связи Вооруженных Сил Российской Федерации, vas@mil.ru

СКОРОПАД Александр Витальевич — ведущий инженер НИЛ № 4131, НИО № 413, НТЦ № 41 Санкт-Петербургского филиала «Ленинградское отделение научно-исследовательского института радио» (Филиал ФГУП НИИР-ЛОНИИР), sav01236@yandex.ru

СМОРОДИН Геннадий Николаевич — кандидат технических наук, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsmorodin@gmail.com

СМОТРОВ Владислав Юрьевич — Студент группы ФП-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsmotrov52@gmail.com

СОЛОПОВ Егор Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, png@academ.msk.rsnet.ru

СТЕПКИНА Юлия Александровна — кандидат экономических наук, доцент, Санкт-Петербургский государственный экономический университет, yulessa@yandex.ru

СУРКОВ Эдвард — студент группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, edvard11@mail.ru

СЯЧИН Константин Ильич — сотрудник Академии Федеральной службы охраны Российской Федерации, syachinkostya@yandex.ru

ТАРАСОВ Владимир Анатольевич — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-liquidator@bk.ru

ТАТУКОВ Данила Андреевич — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tatukov.danila@mail.ru

ТЕЗИН Александр Васильевич — кандидат технических наук, доцент сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ТЁРУШКИНА Ольга Борисовна — кандидат технических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konferenciya.3@mail.ru

ТОРОПЦЕВ Антон Юрьевич — студент Академии Федеральной службы охраны Российской Федерации, toroptsev.an@gmail.com

ТОРШЕНКО Юлия Александровна — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ulka.torshenko@gmail.com

ТРИАНДАФИЛИДИ Иоанис Иванович — студент группы 5823 Санкт-Петербургского государственного университета аэрокосмического приборостроения, mr.ioanis@gmail.com

ТРОФИМУШКИН Максим Дмитриевич — студент группы ФП-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maks.trofimuschkin@gmail.com

УРАГО Андрей Владимирович — студент группы ИСТ-031м Санкт Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, andrey.urago@gmail.com

УРВАНЦЕВА Наталья Львовна — кандидат технических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, N.Urv@yandex.ru

УШАНОВА Маргарита Андреевна — студентка группы ИСТ-932 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tomae.concordia@rambler.ru

ФЕДОРОВ Сергей Игоревич — студент группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича, es.ffp@net.sut.ru

ФЕДОРОВА Алина Владимировна — кандидат экономических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fav111@yandex.ru

ФЕДУЛОВА Анастасия Александровна — студентка группы ИСТ-91 Поволжского государственного университета телекоммуникаций и информатики, fedulova.nastya2018@mail.ru

ФИЛИН Владимир Алексеевич — доктор технических наук, профессор, заведующий кафедрой электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filin_vladimir@mail.ru

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru

ФРОЛОВА Кристина Александровна — аспирантка кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frolkris988@gmail.com

ХАМОВА Виктория Олеговна — студентка группы ИСТ-012м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vikahamova@gmail.com

ХО Тхай Чунг — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ХОДАНОВИЧ Александр Иванович — доктор педагогических наук, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akhodanovich@yandex.ru

ХОМИЧУК Михаил Владимирович — сотрудник Академии Федеральной службы охраны Российской Федерации, misha.homi@gmail.com

ЧИСТЯКОВА Анастасия Максимовна — сотрудник Академии Федеральной службы охраны Российской Федерации, Stultusmidge@yandex.ru

ЧУБАРОВА Зинаида Витальевна — студентка группы ИСТ-822 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zina.chubarova@gmail.com

ЧУПРИН Дмитрий Владимирович — старший научный сотрудник 42 отдела, аспирант Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, chups@ya.ru

ШАРИХИНА Юлия Валерьевна — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kjval@mail.ru

ШЕВЧЕНКО Александр Александрович — научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

ШЕНДЕВИЦКИЙ Игорь Максимович — сотрудник Академии Федеральной службы охраны Российской Федерации, shendivitsk.2001@gmail.com

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandr.shestakov01@yandex.ru

ШИЯН Андрей Анатольевич — кандидат педагогических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1001digit@gmail.com

ШУГУРОВ Дмитрий Евгеньевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, shdevg@mail.ru

ШУЛЬГИН Михаил Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ЩУКИН Артем Владимирович — сотрудник Академии Федеральной службы охраны Российской Федерации, mdo@academ.msk.rsnet.ru

ЮРМАНОВА Вероника Павловна — студентка группы ИСТ-011м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, veronika_yurmanova@inbox.ru

ЮРОВА Валентина Александровна — кандидат физико-математических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, va-yurova@mail.ru

ЯГОТИНЦЕВА Наталья Владимировна — кандидат технических наук, доцент кафедры «Прикладная информатика» Российского государственного гидрометеорологического университета, yagotintceva@yandex.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))

Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича