VII

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

▪ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ ▪

СБОРНИК НАУЧНЫХ СТАТЕЙ

2018

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2018. Т. 2. 670 с.

ГЕНЕРАЛЬНЫЙ СПОНСОР

СПОНСОРЫ КОНФЕРЕНЦИИ

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.

ISBN 978-5-89160-169-7

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

COMNEWS

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

linkmeup
первый подкаст для связистов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
научное рецензируемое издание • электронный научный журнал
Telecom IT — ISSN 2307-1303

НАУЧНЫЙ ЖУРНАЛ
ТУЗ
«ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ»

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Д. В. Ушаков
Верстка Е. М. Аникевич
Подписано в печать 02.07.2018.
Вышло в свет 31.07.2018. Формат 60×90 1/8.
Уст. печ. л. 41,88. Заказ № 043-ИТТ-2018.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.89

МОДЕЛИ И АЛГОРИТМЫ АВТОМАТИЗИРОВАННОГО ПРОФИЛИРОВАНИЯ ВАКАНСИЙ И АНАЛИЗА РЫНКА ТРУДА

Р. А. Аверченков, С. В. Акимов, Г. В. Верхова

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

В статье выделена актуальность и целесообразность разработки системы поиска вакансий и анализа рынка труда. Рассмотрены базовые проблемы реализации и методы их решения. Описаны основные модели и структуры данных наилучшим образом отражающие содержимое вакансий и навыков соискателя в представленной системе анализа. Выделены главные этапы работы системы, а также представлен вариант ее дальнейшего развития.

искусственный интеллект, рынок труда, биржа вакансий, профилирование, нейролингвистическое программирование, математическая статистика.

В наше время, все больше задач перекладывается на вычислительную технику. Уже сейчас некоторые интеллектуальные системы не только успешно решают задачи, традиционно решаемые исключительно человеком, но и с огромным перевесом справляются с задачами лучше хорошего специалиста [1]. Это стремление к автоматизации не только сокращает рабочие места, но и требует от текущих специалистов знаний значительно более высокого уровня.

Сейчас получить престижную и высокооплачиваемую работу становится все более сложной задачей, поэтому очень важно правильно понимать, какие навыки наиболее необходимы для той или иной профессии. Однако понять, что именно на данный момент наиболее актуально на рынке труда – не простая задача. Не обошла эту проблему и система образования, учебные заведения хотели бы обучать специалистов давая им наиболее необходимые и актуальные знания.

Одним из решений данной проблемы является ручной мониторинг и анализ сервисов поиска вакансий. Но и это не позволит получать актуальную информацию оперативно в связи с сложностью ручной обработки и объемом информации для анализа. Логичным решением является автоматизация данного процесса с использованием современных технологий автоматизации – методов искусственного интеллекта. Проблемой данного подхода является то что на текущий момент интеллектуальные системы имеют специфические особенности применения и позволят достаточно легко решить только часть требуемых задач. Полное решение проблемы анализа рынка труда на основе вакансий с использованием исключительно искусственного интеллекта чрезвычайно сложное и дорогостоящее решение, реализация которого нецелесообразна.

Выходом из данной ситуации является использование математической статистики [2], как основного элемента анализа навыков соискателя. Однако для этого также необходимо сформировать системы множеств, на которые и будет действовать данный математический аппарат.

Данные системы множеств должны качественно отражать суть каждой из вакансий и иметь простой и удобный формат для их дальнейшего анализа. Наиболее подходящем элементом для данной системы множеств являются навыки, знания и умения, требуемые от соискателя работодателем конкретной вакансии. Одной из моделью представления вакансии могут являться множество состоящее из лексем, кратко описывающих тот или иной навык, умение или знание требуемое от соискателя (рис. 1).

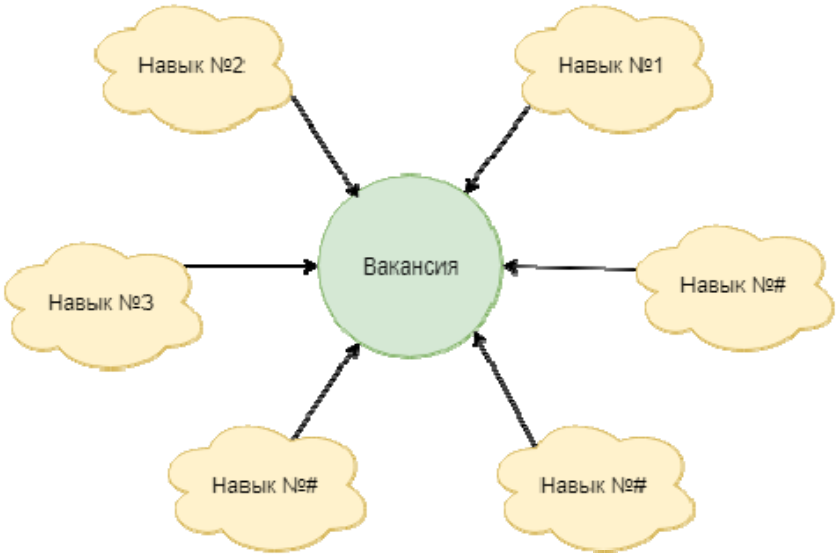


Рис. 1. Модель вакансии в системе

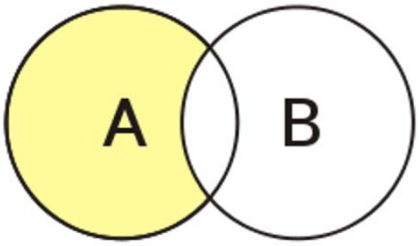
На данном этапе стоит рассмотреть задачу по выделению этих данных из актуальных вакансий на рынке труда. Для решения этой задачи можно

использовать уже имеющиеся теги навыков, которые представлены в описании вакансии. Их можно расширить путем частичного анализа описания вакансии, что на данный момент является успешно решаемой задачей для нейролингвистического программирования [3].

Таким образом анализируя список вакансий определенной профессии можно получить необходимое множество требуемых навыков, что в дальнейшем позволит статистически определить наиболее требуемые навыки для соискателя.

Остается задача отображение имеющихся множеств навыков на текущие знания соискателя, что позволит автоматически определять недостающие навыки соискателя. Ее решением может являться формирование списка имеющихся навыков у соискателя вручную самим соискателем с использованием системы рекомендаций на основе коллаборативной фильтрации [4], что упростит и улучшит конечный результат процесса ввода навыков.

Имея множество требуемых навыков A и имеющихся у соискателя B можно произвести разность этих множеств и таким образом определить недостающие навыки соискателя (рис. 2).



$$A \setminus B = \{x \in A \mid x \notin B\}$$

Рис. 2. Сравнение навыков соискателя и профессии

В результате общий алгоритм работы системы анализа рынка труда принимает вид, представленный на рис. 3. Стоит так же отметить очередность этапов «Поиска вакансий» и «Определение навыков соискателя». В данном случае подразумевается, что изначально пользователь системы анализа определил свои навыки, а затем приступил к этапу «Поиск вакансий» и получению соответствующего результата. В дальнейшем при получении недостающих навыков пользователь может повторно определить свои навыки основываясь на полученном результате анализа.

Рис. 3. Основные этапы работы системы анализа навыков

В дальнейшем можно сформировать множество навыков/знаний для электронных учебно-методических комплексов, которые данный курс предоставляет его участнику. Используя информацию о недостающих знаниях соискателя и то множество навыков/знаний полученных о курсах, можно построить систему рекомендаций [4] курсов, которые позволят соискателю подтянуть недостающие знания.

Представленная в данной работе система поможет соискателю существенно помочь в анализе текущих знаний и требований конкретной профессии, что дальнейшем позволит работодателям нанимать более квалифицированных специалистов в требуемых областях.

Список используемых источников

1. Слэйгл Дж. Искусственный интеллект. М. : Мир, 2016. 320 с.

2. Гмурман В. Е. Теория вероятностей и математическая статистика: учебное пособие для бакалавров. М. : Юрайт, 2013. 479 с.

3. Russell J, Rovere A, eds. (2009). "Neuro-linguistic programming". American Cancer Society Complete Guide to Complementary and Alternative Cancer Therapies (2nd ed.). American Cancer Society. pp. 120–122. ISBN 9780944235713.

4. Adomavicius, Gediminas; Tuzhilin, Alexander (2015-01-01). Ricci, Francesco; Rokach, Lior; Shapira, Bracha, eds. Recommender Systems Handbook. Springer US. pp. 191–226. doi:10.1007/978-1-4899-7637-6_6. ISBN 9781489976369.

УДК 004.056

АНАЛИЗ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

В. С. Авраменко, Д. И. Бобрешов-Шишов, А. В. Маликов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Для анализа компьютерных инцидентов, обусловленных нарушениями безопасности, необходим комплексный подход к обработке информации о событиях и процессах, зафиксированных в процессе функционирования средств защиты и автоматизации, а также других элементов защищаемой инфокоммуникационной системы. Одним из путей решения данной задачи является применение искусственных нейронных сетей.

компьютерный инцидент, нарушение безопасности информации, искусственные нейронные сети, анализ, средства защиты.

В настоящее время одной из актуальных направлений развития систем защиты информации в инфокоммуникационных системах является автоматизация процесса комплексного анализа компьютерных инцидентов на предмет выявления нарушений безопасности и идентификации их характеристик, выработки вариантов реагирования.

В соответствии с [1] компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки

В общем случае компьютерные инциденты подразделяются на инциденты, обусловленные нарушениями безопасности информации (компьютерные инциденты безопасности) и инциденты, обусловленные программными или техническими сбоями и неисправностями, ошибками персонала и другими факторами, не связанными с нарушениями безопасности информации. Под нарушением безопасности информации понимается событие, заключающееся в появлении или реализации угрозы безопасности информации [2]. Таким образом компьютерный инцидент безопасности – это зафиксированное средствами автоматизации и (или) защиты информации нарушение безопасности информации.

В настоящее время средства защиты информации в основном ориентированы на выполнение функции автоматического обнаружения нарушений безопасности, в большинстве случаев формируют недостаточное количество информации для принятия решения на реагирование и проведения оперативного расследования, что требует ручной работы администратора, значительных временных затрат. Частично задачу автоматического анализа компьютерных инцидентов выполняют SIEM-системы, проводятся исследования по идентификации отдельных характеристик нарушений безопасности [3], но в целом вопросы разработки методологических основ комплексного анализа компьютерных инцидентов требуют дальнейшего исследования.

Таким образом, одним из проблемных вопросов защиты информации в инфокоммуникационных системах является комплексный всесторонний анализ компьютерных инцидентов безопасности (КИБ) на предмет выявления типа (нарушение конфиденциальности, целостности, доступности), цели (объекта атаки), причин, источников нарушения, результатов атаки, последствий (уровень риска, ущерб), способов реализации, идентификаторов, ролей и местоположения участников нарушения и других характеристик нарушения с целью повышения обоснованности решения на реагирование. Фактически такого рода анализ можно назвать диагностированием КИБ. Таким образом, диагностирование КИБ представляет собой процесс

сбора и анализа данных о нарушениях безопасности информации с целью идентификации существенных, для принятия решения на реагирование характеристик нарушений безопасности [2]. Результаты диагностирования, в свою очередь, служат основой для выработки варианта реагирования на нарушения безопасности информации. В общем случае перечень характеристик нарушений безопасности должен соответствовать возможностям системы защиты по реагированию.

В качестве исходных данных для комплексного анализа КИБ в первую очередь целесообразно использовать журналы событий, происходящих в системе. Также могут быть использованы данные из других источников информации о состоянии инфокоммуникационной системы в период реализации нарушения безопасности информации.

Применяемые в современных инфокоммуникационных системах средства автоматизации и защиты информации генерируют и сохраняют в журналах большое количество служебной информации, обусловленной, в том числе и компьютерными инцидентами безопасности. Служебная информация содержит различного рода признаки КИБ, такие как типы событий, номера портов, адреса, идентификаторы процессов, время обнаружения и другие.

Пусть H – множество характеристик нарушений безопасности $H = \{h_i\}$, $i = \overline{1, N_{хар}}$, где $N_{хар}$ – число известных характеристик нарушений безопасности, а $X = \{x_j\}$ $j = \overline{1, m}$ – множество признаков КИБ, используемых для диагностирования в m-мерном евклидовом пространстве R^m, где m – количество признаков, доступных для анализа. Тогда в общем случае результат анализа КИБ на предмет идентификации характеристик нарушения безопасности определяется функциональной зависимостью вида $H = F(X)$.

Рассмотрим задачу идентификации одной характеристики нарушения безопасности – преднамеренности. Преднамеренному и непреднамеренному нарушению соответствуют области значений векторов признаков. Пусть $Q_{\text{пред}}$ – класс преднамеренных нарушений, а $Q_{\text{непр}}$ – класс непреднамеренных нарушений. Тогда результат анализа вектора диагностических признаков $\overline{X}$ в информационной системе на предмет преднамеренности можно представить в виде:

$$h_i = \begin{cases} преднамеренное, если\ X \in Q_{пред}, \\ непреднамеренное, если\ X \in Q. \end{cases}$$

Многообразие средств автоматизации и защиты обуславливает возможность получения большого количества различного рода признаков КИБ, что требует решения проблемы эффективной обработки данной информации.

Подобные классификационные задачи успешно решаются с применением аппарата искусственных нейронных сетей (ИНС) [4]. На входе ИНС подаются предварительно обработанные данные из журналов событий, на выходе – значения характеристик нарушения безопасности. Предварительная обработка данных из журналов событий заключается в отборе из всего множества событий, регистрируемых в каждом конкретном журнале, множества информативных событий для диагностирования компьютерных инцидентов безопасности: $X^{'} = \{x_i^{'}\}, i = \overline{1,z}$, где z – количество информативных событий. Также при необходимости проводится нормализация диагностических признаков.

Например, значение бинарных характеристик нарушения безопасности, таких как преднамеренное нарушение или непреднамеренное, можно определить путем обработки многослойной нейронной сетью вектора диагностических признаков, сформированных из множества X. Для идентификации одной характеристики нарушения безопасности h_i целесообразно использовать трехслойный персептрон, состоящий из z нейронов входного слоя, n нейронов скрытого слоя, число которых определяется в процессе обучения ИНС ($n < z$), и одного нейрона выходного слоя (рис.).

Задача классификации решается следующим образом. На этапе обучения на вход ИНС подаются векторы диагностических признаков, позволяющие однозначно судить о том, какое произошло нарушение (преднамеренное/непреднамеренное). Корректировка весовых коэффициентов производится методом обратного распространения ошибки [5].

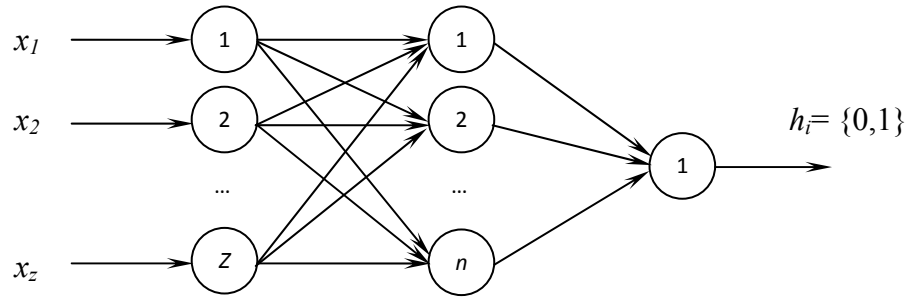


Рисунок. Структура искусственной нейронной сети для идентификации бинарной характеристики нарушения безопасности

После обнаружения компьютерного инцидента безопасности фиксируется вектор диагностических признаков на основе всех доступных журналов событий. В полученном векторе признаки принимают значение 1 при наличии значимого события, 0 – в противном случае. Затем этот вектор подается на вход трехслойного персептрона. Предварительно обученный персептрон позволяет минимизировать среднеквадратичную ошибку расхождения между значением классификационной функции F и требуемым значением выхода h_i.

Данный подход к анализу компьютерных инцидентов безопасности позволит в автоматическом режиме в близком к реальному масштабу времени идентифицировать максимально возможное число характеристик нарушений безопасности, что в свою очередь позволит обеспечить оперативное и обоснованное реагирование на КИБ.

Список используемых источников

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: офиц. текст. М. : Российская газета – Федеральный выпуск № 7333 (167), 2017.
2. Авраменко В. С., Пантюхин О. И., Маликов А. В. Автоматизация диагностирования нарушений безопасности в АССН // Труды XVII Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности» (1–4 апреля 2014 г.). СПб. : РАРАН, 2014. С. 123–126.
3. Авраменко В. С. Способы идентификации нарушителя безопасности информации в автоматизированных системах на основе информационного почерка // Сборник трудов II межвузовской конференции «Проблемы технического обеспечения войск в современных условиях». СПб. : ВАС, 2017. С. 36–40.
4. Осовский С. Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. М. : Финансы и статистика, 2002. 344 с.
5. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. 2-е изд., стереотип. М. : Горячая линия – Телеком, 2002. 382 с.

УДК 004.056

ТЕХНОЛОГИЯ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭКСПЛОЙТОВ

В. С. Авраменко, Д. И. Бобрешов-Шишов, А. В. Маликов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Разработка методов, способов и средств защиты информации в современных инфокоммуникационных системах от реализации атак с использованием новых для защищающейся стороны эксплойтов и уязвимостей является актуальной задачей. В данной статье предлагается технология защиты от подобных атак, основанная на анализе порождённых эксплойтом процессов.

эксплойты, уязвимости, компьютерные атаки, защита информации.

Под эксплойтом принято понимать компьютерную программу, фрагмент программного кода или последовательность команд, использующие

уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Эксплойт после запуска повышает привилегии или загружает дополнительные вредоносные программы с сервера нарушителя. В настоящим время ежедневно создаются десятки новых эксплойтов, примерно такое же количество ежедневно «устаревает». Наблюдаемая закономерность обусловлена тем, что большинство эксплойтов создаются для реализации компьютерных атак «нулевого дня», которые основаны на новых или ранее неизвестных для защищающейся стороны уязвимостях. По этой причине традиционные методы и средства неэффективны для обнаружения новых эксплойтов.

Для решения задачи обнаружения ранее неизвестных уязвимостей на основе анализа поведения эксплойтов целесообразно классифицировать эксплойты.

По методу получения доступа к уязвимому программному обеспечению эксплойты подразделяются на удаленные (работают через сеть и используют уязвимость без предварительного доступа к системе) и локальные (требуют предварительного доступа к уязвимой системе и запускаются непосредственно в ней).

По типу механизма использования уязвимости выделяются следующие классы эксплойтов: реализующие атаку «переполнение буфера»; межсайтовый «скриптинг»; SQL инъекции; атаку возврата в библиотеку.

По видам используемых приложений выделятся следующие классы эксплойтов: эксплойты для операционных систем (ОС); пользовательских приложений (проигрыватели, офисные пакеты и т.п.); браузеров; вебсайтов.

По используемому при создании эксплойта языку программирования эксплойты делятся на созданные в C/C++; JAVA; Perl; Piton; PHP; HTML+JavaScript.

По применяемым в процессе загрузки сетевым протоколам выделяются следующие классы эксплойтов: использующие http; FTP; SSH; TelNet; RDP; их комбинации.

Подавляющее большинство эксплойтов (порядка 90 %) загружают на машину жертвы нагрузку управления. В роли такой нагрузки как правило выступает шелл-код или meterpreter. Это разновидности кода оболочки или двоичного исполняемого кода, который обычно передает атакующему управление командной оболочкой. Наиболее распространенный вид шелл-кода – реверс-шелл. Он осуществляет доступ к определённому в шелл-коде порту атакуемого компьютера с целью обхода брандмауэра.

Полезная нагрузка – это главная часть шелл-кода, представляет собой участок кода, осуществляющий вредоносную активность. Как правило, в этой части находится исполняемая часть кода, а в некоторых случаях и ссылка на компьютер атакующего. Зона адресов возврата – это часть

шелл-кода, указывающая процессу на расположение полезной нагрузки. Код выполнен на низком уровне и поэтому его сложно выделить из трафика.

Существуют признаки, способные с приемлемой достоверностью обеспечить обнаружение шелл-кода по «следам» его работы в системе. Для этого применяются специальные утилиты, использующие такие признаки как необоснованное расходование оперативной памяти, подозрительные процессы, аномальный трафик, операционные ошибки и другие. Кроме того, правильно настроенная система обнаружения атак (СОА) также может своевременно сообщить администратору о возможной реализации атаки с применением эксплойта.

Предлагаемый способ обнаружения уязвимостей основан на изучении выявленного «подозрительного» процесса. В информации о процессе обязательно находятся ссылки на переменные (или их адреса в оперативной памяти), которые были использованы в эксплойте. По адресу переменных возможно определить файл, в котором они были инициализированы. Собственно, текст файла и является основным объектом исследования, так как изучение кода дает информацию об эксплойте и имеющейся уязвимости. Например, СОА (или средство антивирусной защиты) обнаружила некорректные действия какой-либо программы, возможно обусловленные реализацией ранее неизвестной атаки. На следующем этапе определяется процесс, порожденный возможной атакой. При этом в качестве признаков может использоваться время запуска процессов, их размер, применяемые средства и соединения. В случае обнаружения шелл-кода, породившего данный процесс, неопределенность информации об уязвимости уменьшается (подтверждается наличие в системе уязвимости). На следующем этапе следует определить переменные по их адресу и определить файл, в котором они были инициализированы. Для предварительной проверки файла на наличие вредоносного кода может использоваться подход, предложенный в [1]. После обнаружении файла возможно изучение его кода: поиск ссылок, анализ открываемых файлов и библиотек. Также определенные сведения об уязвимости может передать формат файла и используемый язык. Для повышения оперативности и достоверности процесса поиска новой уязвимости целесообразно использовать подход к распознаванию нарушений на основе информационных образов [2]. В частности, на основе характеристик эксплойтов представляется возможным сформировать эталонные образы эксплойтов, использующих уязвимости в определенных приложениях и системах. Это существенно сужает область поиска уязвимости, одновременно позволяя начать параллельно разрабатывать меры по ее устранению.

Реализация предлагаемой технологии защиты предполагает выполнение следующих этапов.

1. Определение с помощью СОА или антивирусного средства подозрительного процесса (прямого или косвенного процесса реализации атаки), определение его ID.

2. Определение с помощью специальных дополнительных утилит областей памяти, занятые этим процессом.

3. Определение адресов переменных, задействованных в рассматриваемых областях памяти.

4. Выявление адреса файла, в котором происходит объявление найденных переменных.

5. Просмотр содержимого исполняемого файла, изучение подключаемых библиотек, анализ функций, выполняемых эксплойтом.

6. Определение приложения, содержащего уязвимость, идентификация уязвимости, актуализация базы данных сканера уязвимостей, поиск уязвимостей в других элементах защищаемой системы с помощью сканера.

7. Оценка уровня опасности обнаруженной уязвимости, оценка уровня защищенности инфокоммуникационной системы с учетом выявленных уязвимостей в соответствии с [3] или [4] в зависимости от вида неопределенности информации о выявленных угрозах.

8. Принятие решения по защите, выполнение мероприятий по нейтрализации выявленных уязвимостей, а также источников и каналов реализации соответствующих угроз (блокировка соответствующего приложения, реконфигурация межсетевых экранов и др.).

Таким образом, использование предлагаемой технологии позволяет собственными силами и средствами защиты оперативно обнаруживать уязвимости «нулевого дня» и принимать меры по ее устранению, не дожидаясь обновлений внешних баз данных уязвимостей и обновлений программ от производителей средств защиты.

Список используемых источников

1. Авраменко В. С., Баранов В. А., Бочков М. В. Метод контроля безопасности содержимого файлов // Телекоммуникации. 2004. № 11. С. 41.

2. Авраменко В. С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45–49.

3. Козленко А. В., Авраменко В. С., Саенко И. Б., Кий А. В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. № 2 (21). С. 41–55.

4. Авраменко В. С. Методы оценки защищенности информации от несанкционированного доступа в условиях нечеткости // Проблемы информационной безопасности. Компьютерные системы. 2007. № 2. С. 27–31.

УДК 004.896:621.865

РАЗРАБОТКА МОБИЛЬНОГО РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА ДЛЯ АВТОМАТИЗИРОВАННОГО МОНИТОРИНГА ОКРУЖАЮЩЕЙ СРЕДЫ В РАЙОНЕ ОПАСНЫХ ОБЪЕКТОВ

А. М. Адуевский, К. В. Белоус, Е. А. Пиликина

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

Представлен прототип мобильного робототехнического комплекса, построенного на базе аппаратной платформы Arduino. Рассмотрены базовые алгоритмы работы робота, проанализированы каналы управления роботом.

мониторинг, автоматизация, Arduino, вредные производства, управление.

В настоящее время промышленные предприятия и производства в своей деятельности активно используют различные сложные технические средства автоматизации и управления технологическими процессами и производствами, системы управления которыми, в большинстве случаев, функционируют в составе Единого информационного пространства предприятия или организации [1]. Технологические процессы части предприятий сопряжены с работой или получением опасных веществ, которые могут оказывать негативное влияние на внешнюю окружающую среду или здоровье человека, в связи с чем возникает объективная необходимость разработки технических устройств контроля параметров внешней среды в районе опасных объектов.

Промышленные программно-технические комплексы, позволяющие проводить мониторинг различных параметров внешней среды с автоматизированными подсистемами анализа и выдачи предупреждений в случае, если концентрация или значение некоторого параметра превысит заранее установленное значение, несмотря на свою эффективность и высокое быстродействие, имеют один существенный недостаток, который заключается в их высокой стоимости.

Одним из возможных решений вопроса снижения стоимости оборудования для построения автоматизированных систем мониторинга параметров внешней среды является разработка собственного программно-аппаратного комплекса, способного решать поставленные перед ним задачи.

Ядром данного комплекса, разработанного в учебных целях для кафедры автоматизации предприятий связи СПб ГУТ является плата семейства Arduino (*Arduino Mega*), имеющая следующие характеристики [2]:

- микроконтроллер: ATmega2560;
- тактовая частота: 16 МГц;
- рабочее напряжение: 5 В;
- предельные напряжения питания: 5–20 В;
- рекомендуемое напряжение питания: 7–12 В;
- максимальная сила тока с одного вывода: 40 мА;
- цифровые входы/выходы: 54;
- цифровые входы/выходы с поддержкой ШИМ: 15;
- аналоговые входы: 16;
- FLASH–память: 256 Кб (8 Кб используются загрузчиком);
- SRAM: 8 Кб;
- EEPROM: 4 Кб.

Наличие на плате большого количества цифровых и аналоговых портов ввода-вывода позволяет подключать к ней всю необходимую периферию, среди которых наиболее важными элементами будут являться датчики – датчики температуры и влажности, датчики давления, датчики вредных газов и др. [3]. В качестве основы для размещения всех необходимых элементов используется колёсная база (рис. 1).

Рис. 1. Колёсная база

Питание может осуществляться от 4-х батарей типоразмера AA или от источника автономного питания, способного обеспечить требуемые параметры по току и напряжению. Разработанный прототип снабжен системой технического зрения, позволяющей ему ориентироваться в пространстве без участия человека. Для хранения информации о параметрах внешней среды используется СУБД MS SQL сервер. Обобщенная структура робототехнического комплекса показана на рис. 2.

Работа системы возможна в двух режимах: ручной и автоматический.

В ручном режиме управление работой робототехнического устройства производится с участием оператора путём направления ему необходимых команд через web-интерфейс в режиме реального времени. При этом происходит двухсторонний обмен информацией между оператором (через web-интерфейс), в котором выполняется вывод информации о текущем состоянии устройства с параллельной записью результатов измерения в базу данных.

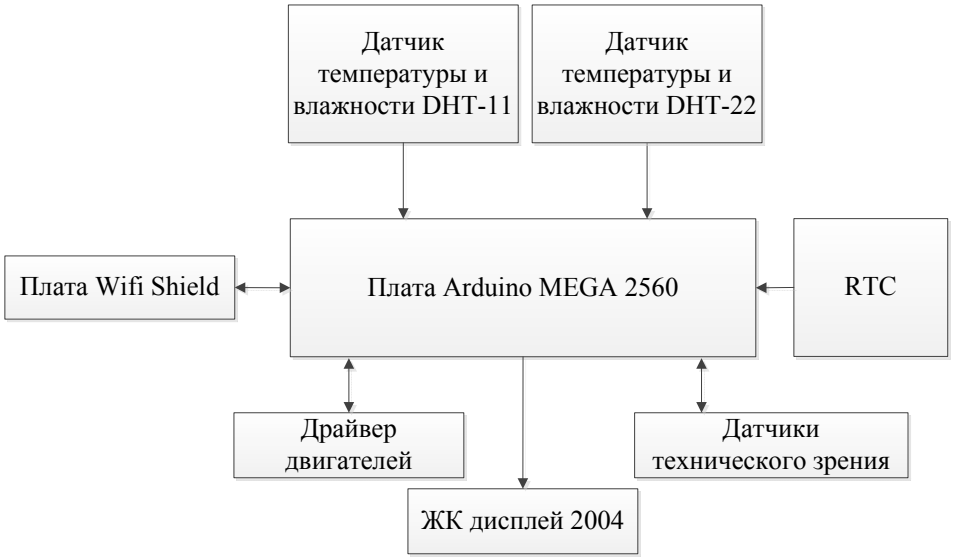


Рис. 2. Обобщённая структура робототехнического комплекса

В автоматическом режиме оператор не имеет возможности воздействовать на устройство за исключением случаев возникновения внештатной ситуации, о которой будет получено уведомление.

Список используемых источников

1. Рыкунов В. Д. Охранные системы и технические средства физической защиты объектов. М. : Секьюрити Фокус, 2011. 288 с.

2. Блум Д. Изучаем Arduino. Инструменты и методы технического волшебства : пер. с англ. СПб.: БХВ-Петербург, 2016. 336 с.

3. Монк С. Программируем Arduino: основы работы со скетчами. СПб. : Питер, 2017. 208 с.

УДК 004.94; 004.896

АВТОМАТИЗАЦИЯ ПОДДЕРЖКИ ЖИЗНЕННОГО ЦИКЛА МОДУЛЬНЫХ СИСТЕМ

С. В. Акимов, Г. В. Верхова, Х. М. Кходер

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

Модульная технология построения сложных систем представляет собой выгодное решение для многих компаний, благодаря ей возможен ускоренный выход на рынок при быстро комплексирования систем из унифицированных модулей и значительно

меньших затратах ресурсов на разработку системы. В связи с этим, в данной работе представлены специальные многоаспектные модели для автоматизации поддержки модульных систем на этапах жизненного цикла, таких как маркетинговые исследования, проектирование, производство, эксплуатация с составлением электронного паспорта изделия.

модульная технология, сложные системы, автоматизация, жизненный цикл, CAD/PLM, многоаспектное моделирование, комплексная модель.

Для современных компании и предприятий модульная технология может быть использована в качестве стратегии, обеспечивающей: более низкие издержки производства в результате более эффективного использования ресурсов, меньшую рабочую нагрузку, в связи с многократным использованием некоторых решений, и большую степень гибкости, используемую для контроля возрастающей сложности проектирования и производства.

Концепция модуля заключается в том, чтобы определять различные независимые функции, а также инкапсулировать эти функции, тем самым абстрагируя внутреннюю механику модуля от системы в целом. Для создания модульной системы потребуются по крайней мере, три вещи: модули, интерфейсы и набор протоколов для соединения модулей на интерфейсах (рис. 1).

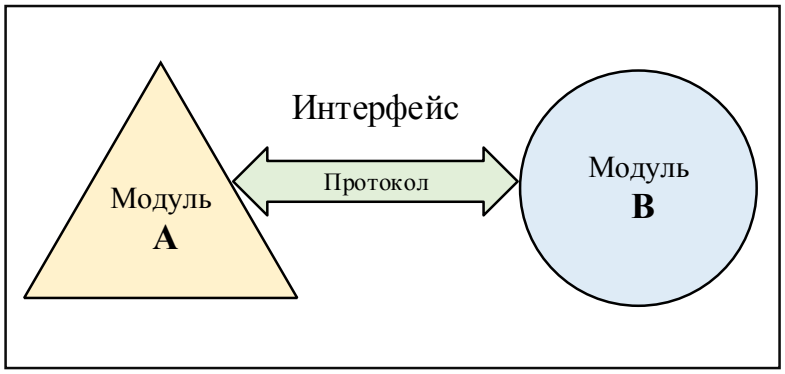


Рис. 1. Модульная система

В модульной системе [1, 2] модуль представляет собой черный ящик, который можно просматривать с точки зрения характеристик ввода, вывода и передачи без каких-либо знаний о его внутренних функциях. Входы, выходы и функциональные характеристики определяются и перемещаются с помощью интерфейса, сообщающего другим модулям в системе, что может сделать этот модуль. Не имеет значения, как внутренне реализуется модуль, но необходимо знать, как им пользоваться.

Жизненный цикл модульных систем включает ряд этапов, начиная от зарождения идеи новых составных частей системы, до их утилизации

по окончании срока использования. К жизненному циклу модульных систем относятся такие этапы как: маркетинговые исследования, проектирование, подготовка к производству, производство, эксплуатация (электронный паспорт изделия). Модульные архитектуры генерируют множество данных, и необходимо внедрять эти данные в свои PLM-системы (*Product Lifecycle Management)* [3]. Фирмы надеются улучшить организацию данных модульных архитектур и упростить их поиск и извлечение. Они также ищут способы визуализации данных для, благодаря чему значительно легче станет их понимание. В маленьких и средних компаниях PLM-системы используются недостаточно широко, но у этих компаний имеются одинаковые потребности, когда речь идет о модульной архитектуре. В результате образуется рыночная нагрузка на системы CAD и PLM, заключающаяся в необходимости добавления функциональности для модульной архитектуры.

Модульные архитектуры внедряются в PLM с ограниченной сложностью и интеграцией. При их внедрении есть возможность столкнутся с некоторыми проблемами, и что бы процесс был эффективен необходимо учитывать различные аспекты модулей (функциональные, конструктивные, экономические и т. д.), но все основные CAD-системы используют модели, отражающие отдельно взятые аспекты. Объединение моделей, отражающих различные аспекты проектируемой системы, осуществляется с помощью PDM-систем, но такие системы не обеспечивают необходимые манипуляции с моделями непосредственно на уровне системных аспектов, не обращаясь к моделям, хранящимся в базе данных проекта.

Параметрическое многоаспектное моделирование представляет собой методологию, которая может быть использована для решения задач моделирования модульных систем. Эта методология, в основу которых положены комплексные модели, может играть роль своеобразной PDM/PLM-системы, органично объединяющей различные виды знаний об модуле [4]. Для описания множество технико-экономических характеристик (ТЭХ), которые полностью определяют все существенные свойства модуля, используются параметры комплексных моделей [5]. Множество технико-экономических характеристик группируется по аспектам:

$$\text{ТЭХ} = \bigcup_{i=1}^{n} P_{A_i},$$

где P_{Ai} – множество параметров, i-го аспекта.

На рис. 2 показано представление модульной системы на основе параметрического многоаспектного моделирования.

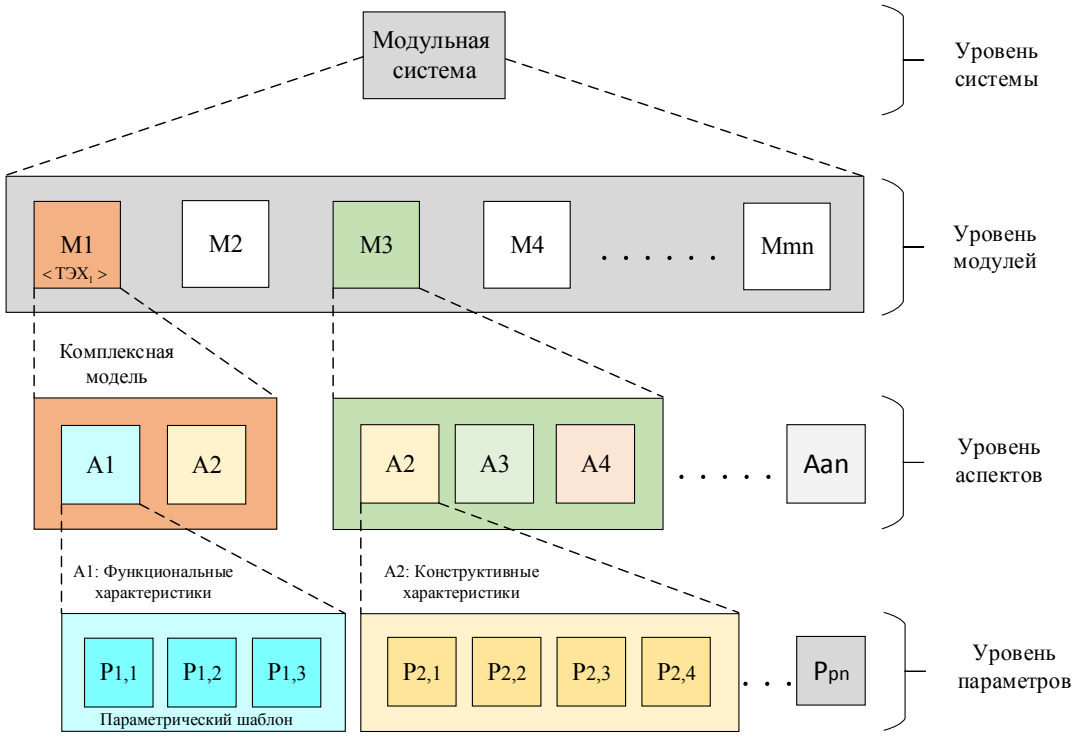


Рис. 2. Модульная система и её представление
на основе параметрического многоаспектного моделирования

Параметры комплексной модели являются удобным способом представления информации о многоаспектных характеристиках модуля, а также определенных видах обработки этой информации, в том числе многокритериальный поиск и могут быть использованы на всех этапах жизненного цикла системного объекта (маркетинговые исследования, проектирование, производства, эксплуатация (электронный паспорт изделия)). Для представления модульных систем на основе параметрического многоаспектного моделирования необходимо сформулировать параметры комплексной модели, в рамках основных типов, которые представлены ниже [6]:

Целочисленный параметр (*Integer parameter*):

$$Int \stackrel{\text{def}}{=} \langle name, symbol, type, unit, v, v_{min}, v_{max}, init, dim \rangle;$$

$$v, v_{min}, v_{max} \in Z;$$

$$type = Int.$$

Вещественный параметр (*Real parameter*):

$$Real \stackrel{\text{def}}{=} \langle name, symbol, type, unit, v, v_{min}, v_{max}, init, dim \rangle;$$

$$v, v_{min}, v_{max} \in R;$$

$$type = Real,$$

где *name* – имя параметра, *symbol* – обозначение параметра, *type* – тип параметра, *unit* – единица измерения параметра, *v* – текущее значение параметра, *dim* – размерность параметра, *init* – значение параметра по умолчанию, v_{min}, v_{max} – минимальное и максимальное значение параметра.

В заключение, на основании анализа современного рынка, в данном докладе приведена проблема поддержки жизненного цикла модульных систем в CAD/PLM-системах. Представленные многоаспектные модели могут быть положены в основу единых информационных сред, обеспечивающих автоматизацию поддержки модульных систем на этапах жизненного цикла.

Список используемых источников

1. Vasawade R., Deshmukh B., Kulkarni V. Modularity in design: A review // International Conference on Technologies for Sustainable Development (ICTSD), 2015. P. 1–4.

2. Кходер Х. М, Верхова Г. В., Акимов С. В. Модульная технология проектирования гибких сложных систем // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. № 9. С. 86–90.

3. Hans P. B., Niels H. M., Ulf H., Michael W., Mikkel P. PLM system support for modular product development // Computers in Industry. 2015. Volume 67. P. 97–111.

4. Акимов С. В., Демидов А. А, Никифоров О. Г. Методология комплексных моделей системных объектов // Вопросы радиоэлектроники. Серия «Системы отображения информации и управления спецтехникой (СОИУ)». 2012. Вып. 2. С. 138–149.

5. Günther S., Michael R., Elisabeth S., Merle-Hendrikje J. Structuring Information of Modular Product Platforms // ASME 2017 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 2017. P. 1–9.

6. Акимов С. В., Меткин Н. П., Верхова Г. В. Параметрическое многоаспектное моделирование системных объектов // Радиопромышленность. 2017. № 1. С. 110–118.

УДК 004.422

АВТОМАТИЗИРОВАННАЯ СИСТЕМА МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

С. В. Акимов, Г. В. Верхова, Н. В. Полпудникова

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

В статье приведены результаты разработки прототипа автоматизированной системы мониторинга вычислительной техники. Разработанная система обеспечивает сбор и обработку информации о компьютерах, включая конфигурацию, расположение, данные о сервисном обслуживании. Автоматизированная система реализована в виде веб-службы и предполагает интеграцию в единую киберсреду постиндустри-

ального общества. Действующий прототип системы написан на языке программирования C# в виде приложения ASP.NET. Служба может использоваться по модели SaaS (программное обеспечение как услуга), что обеспечивает удобство сопровождения, так как не требует от пользователя установки дополнительного обеспечения.

автоматизация мониторинга, вычислительная техника, ASP.NET, веб-служба.

В статье представлены результаты разработки прототипа автоматизированной системы мониторинга вычислительной техники «PC-Monitor». Такая система обеспечит сбор и обработку оперативной информации о парке вычислительной техники организации.

Разработанная система мониторинга персональных компьютеров предназначена для автоматизации следующих функций:

– учёт персональных компьютеров (ноутбуков);
– мониторинг работоспособности вычислительной техники;
– подачу заявок на сервисное обслуживание;
– учёт выполненных сервисных работ.

В системе «PC-Monitor» предусмотрены роли системного администратора и сервисного инженера. Системный администратор отвечает за следующие функции: управление информацией о вычислительной технике и помещениях, в которых она располагается. Сервисный инженер отвечает за управление конфигурацией компьютеров, добавление заявок на обслуживание, добавление информации о выполнении сервисных работ. Диаграмма вариантов использования системы представлена на рис. 1.

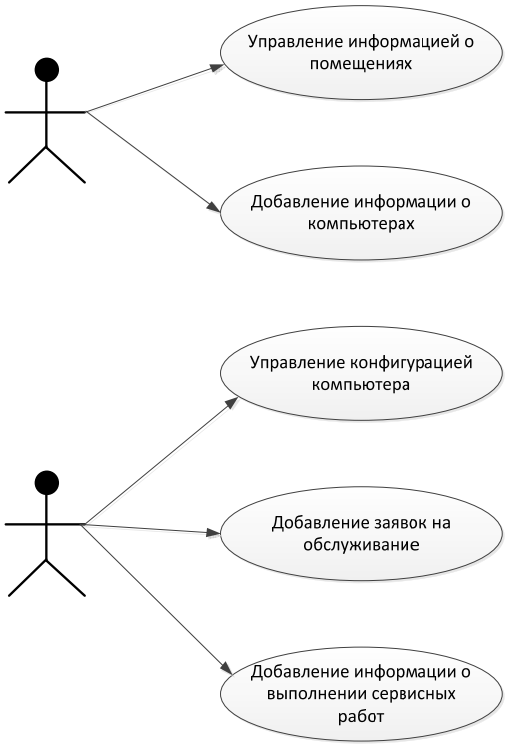


Рис. 2. Варианты использования системы

Система реализована в виде веб-приложения ASP.NET, написана на алгоритмическом языке объектно-ориентированного программирования C#, в роли сервера баз данных выступил MS SQL Server, объектно-реляционное преобразование осуществлялось с помощью ADO.NET Entity framework.

Объектная модель является основной составляющей современного программного обеспечения, отражает структуру данных и бизнес-правила. Объектная модель описывает обязанности, отношения и структуру различных объектов предметной области, представляет системные сущности, их классификацию и агрегирование.

Объектная модель системы PC-Monitor (рис. 2) была разработана в рамках платформы ADO.NET Entity Framework, обеспечивающей возможность сохранения объектов предметной области в реляционной базе данных MS SQL Server 2014. Описание свойств основного сущностного класса Computer представлено в таблице.

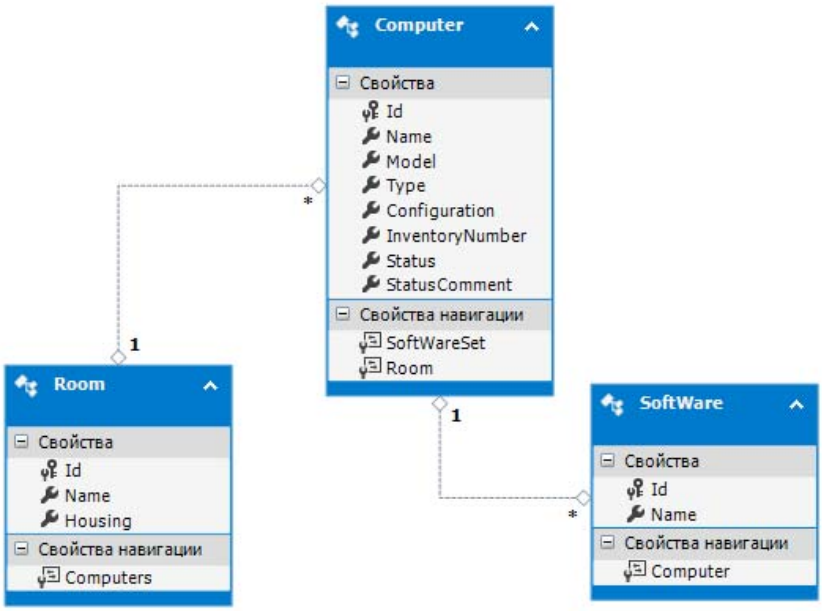


Рис. 2. Объектная модель

ТАБЛИЦА. Свойства классаComputer

Свойство	Тип	Назначение
Скалярные свойства		
Id	Guid	Идентификатор сущности
Name	String	Имя компьютера
Model	String	Модель компьютера
Type	Int	Тип компьютера
Configuration	String	Конфигурация компьютера
InventoryNumber	String	Инвентарный номер компьютера
Status	Struct	Статус работы компьютера
StatusComment	Class	Комментарий о работе компьютера
Свойства навигации		
SoftWareSet		Программное обеспечение
Room		Аудитория

Созданный прототип системы имеет дружественный к пользователю, интуитивно понятный интерфейс (рис. 3). Стартовая страница приложения список аудиторий, вычислительная техника в которых подлежит мониторингу. На странице определенной аудитории доступна информация о компьютерах, их состоянии, установленном программным обеспечением. При возникновении проблем с конкретными компьютерами, возможна оперативная подача заявки на сервисное обслуживание.

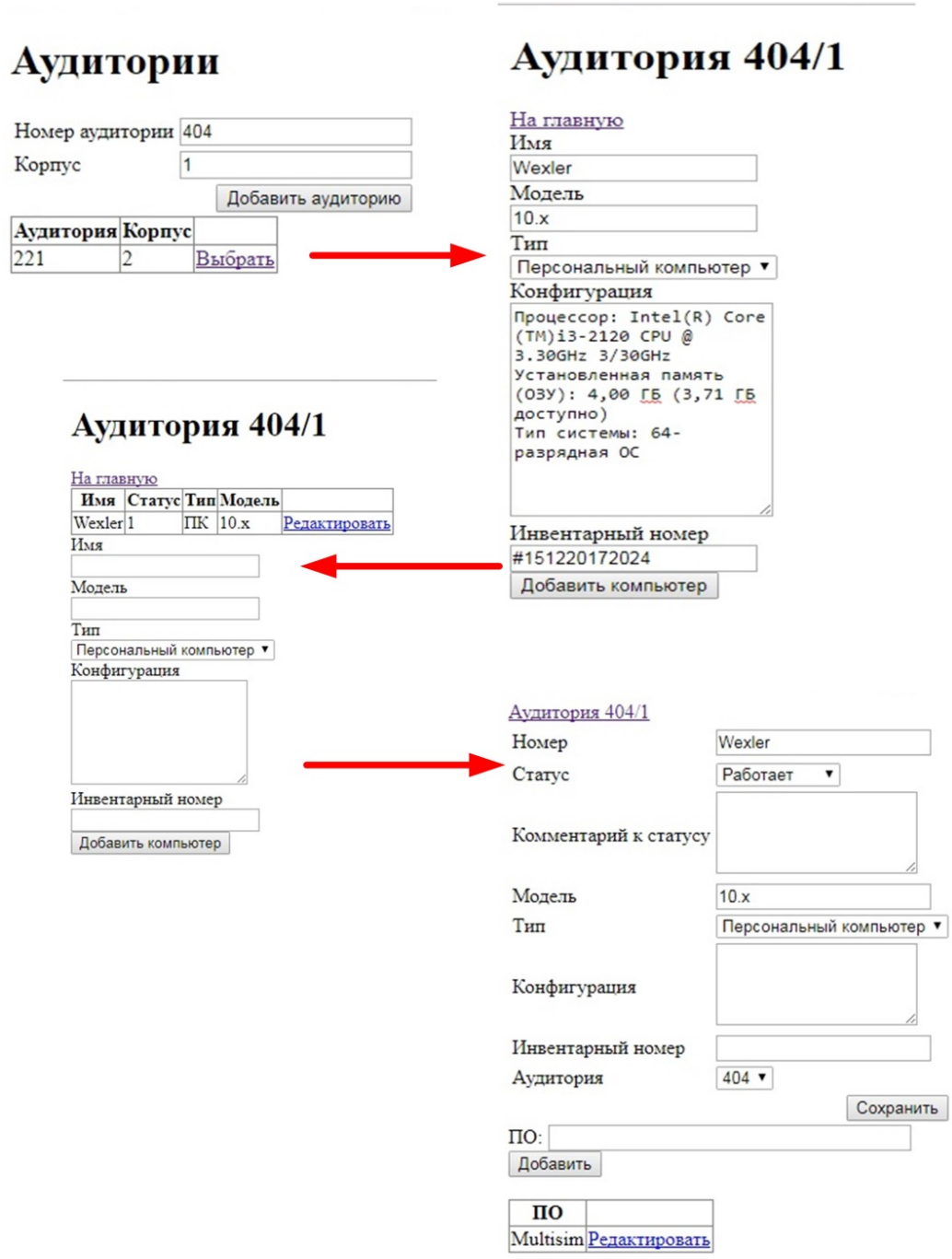


Рис. 3 Интерфейс приложения мониторинга вычислительной техники

Внедрение автоматизированной системы мониторинга персональных компьютеров «PC-Monitor» обеспечит повышение качества обслуживания и эффективности использования вычислительной техники [1, 2]. Кроме того, система может быть интегрирована в единую киберсреду предприятия.

Список используемых источников

1. Акимов С. В., Верхова Г. В. Распределенная информационно-аналитическая система комплексной автоматизации академической деятельности // Телекоммуникации. 2014. № 5. С. 15–19.

2. Панюкова С. В. Комплексная система автоматизации управления университетом // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2011. № 2. С. 71–77.

УДК 004.42

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ В ОПТИМИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

С. В. Акимов, А. В. Купцов, Н. С. Фёдоров, М. А. Хвостов

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

Оптимизация перемещения головки станка лазерной резки является важной задачей производства, так как позволяет экономить время и механический ресурс станка. Нахождение оптимального пути можно свести к решению «задачи коммивояжёра», которая является NP-полной, и для более эффективного её решения можно применить биоинспирированные методы.

генетические алгоритмы, задача коммивояжёра, оптимизация.

Описание проблемы и постановка задачи

Станки для лазерной резки металлов отличаются высокой точностью и скоростью работы, однако имеют несколько недостатков. При лазерной резке станком потребляется большое количество электроэнергии, что сказывается на себестоимости продукции. Ещё один недостаток такого метода производства заключается в том, что запасные части к оборудованию имеют высокую цену и производятся за границей. Для устранения недостатков такого рода и повышения общей эффективности производства важна оптимизация всех его аспектов.

Описание генетического алгоритма

Исходя из условия задачи видно, что она аналогична задаче коммивояжёра [1], решаемой с помощью генетических алгоритмов [2, 3], за исключением добавления направленности прохождения сегментов. Так как генетические алгоритмы показали свою эффективность при решении задачи коммивояжёра, то имеются все основания полагать, что они окажутся эффективными и для решения задачи оптимизации траектории движения обработке излучением.

1. Ген. В качестве гена будем использовать список всех сегментов траектории обработки.

2. Фитнесс-функция. Определим фитнесс-функцию, как функцию, обратную расстоянию T_{xx} холостого хода каретки.

$$f(gene) = \frac{1}{T_{xx}}.$$

3. Кроссовер. В качестве кроссовера будем использовать циклический кроссовер, или CX-crossover. Алгоритм, порождающий одного потомка, можно определить так:

представим родителя в виде перестановки $(S_{(1,)}, S_{(2)} \dots S_{(n)})$, где $S_{(x)}$ – сегмент, стоящий на месте x.

пусть первый родитель будет (1, 2, 4, 3), а второй – (2, 1, 3, 4). Общим циклов, начинающимся с первого элемента, будет (1, 2). Тогда порожденный потомок будет выглядеть (1, 2, 3, 4).

4. Мутация. Мутация будет проходить в два этапа. На первом выберем случайные сегменты и перевернем их, то есть поменяем их направления прохода. На втором выберем последовательность сегментов и поменяем порядок прохода по ним. Это соответствует хромосомной мутации инверсии, когда вырезанный фрагмент хромосомы присоединяется на прежнее место, но будучи повёрнутым на 180 градусов [4].

5. Отбор. Отбор осуществляется с использованием метода «рулетки» (рис. 1), заключающегося в создании отрезка, разделённого на сектора, размеры которых пропорциональны значениям фитнесс-функций соответствующих секторам особей и дальнейшим случайным выбором позиции на этом отрезке для определения конкретной особи.

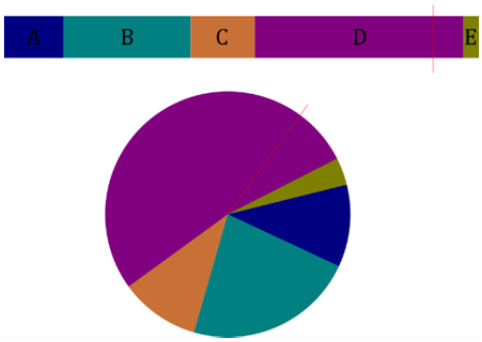


Рис. 1. Иллюстрация алгоритма отбора рулеткой

Принцип работы такого отбора полагается на то, что особи с большим значением фитнесс функции будут занимать большие части отрезка, и вероятность их

выбора будет выше, чем для особей с меньшим значением фитнесс-функции.

Модификация программной реализации алгоритма

Для упрощения работы программы и более наглядного представления результатов работы алгоритма с целью облегчения разработки, отладки и дальнейшего использования программы были реализованы:

– графический интерфейс;

– загрузка конфигурации оптимизируемого объекта из файла.

Такой интерфейс позволяет явно отличать неоптимальные результаты работы алгоритма (рис. 2).

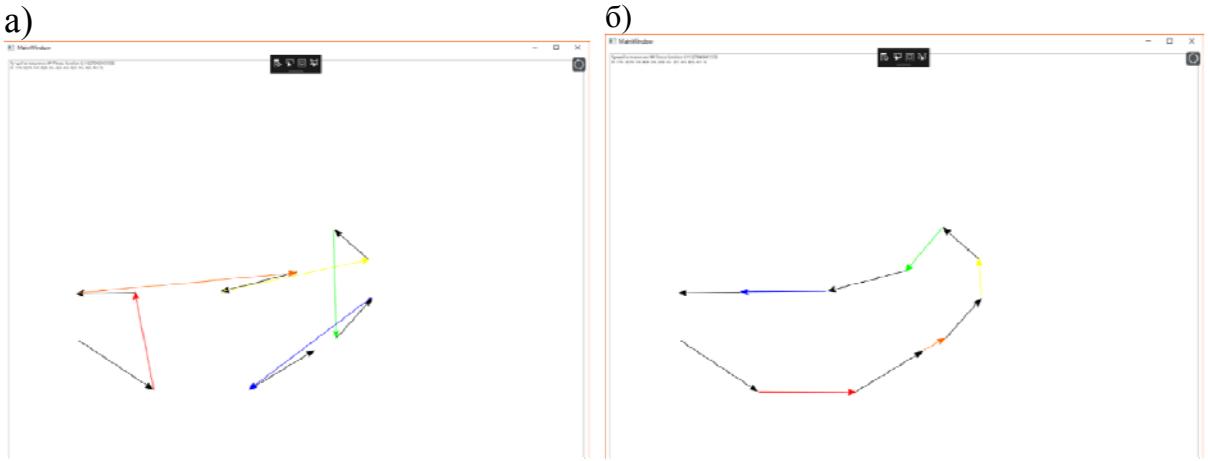


Рис. 2. Графическое отображение работы программы:
а) неоптимальный вариант; б) оптимальный вариант

Загрузка объекта оптимизации из файла осуществляется путём считывания XML разметки и преобразования значений в параметры оптимизируемого объекта (рис. 3).

Оптимизация алгоритма проведена путём разделения визуализации результатов работы алгоритма и рабочего процесса самого алгоритма на два параллельных потока.

Рабочий поток передаёт информацию потоку визуализации при помощи потокобезопасной коллекции ConcurrentQueue<T>, что обеспечивает безопасную асинхронную работу программы, представленную на рис. 4.

```
<?xml version="1.0" encoding="utf-8"?>
<picture>
  <segment id="0" direction="true">
    <point x="2" y="3"/>
    <point x="4" y="2"/>
  </segment>
  <segment id="1" direction="true">
    <point x="6" y="2"/>
    <point x="8" y="3"/>
  </segment>
  <segment id="2" direction="true">
    <point x="9" y="4"/>
    <point x="10" y="5"/>
  </segment>
  <segment id="3" direction="true">
    <point x="10" y="6"/>
    <point x="9" y="7"/>
  </segment>
  <segment id="4" direction="true">
    <point x="7" y="5"/>
    <point x="5" y="4"/>
  </segment>
  <segment id="5" direction="true">
    <point x="3" y="4"/>
    <point x="1" y="4"/>
  </segment>
</picture>
```

Рис. 3. XML – файл объекта

Рис. 4. Схема передачи данных между частями программы

Использование таймера задержки позволяет регулировать скорость выдачи результатов работы алгоритма пользователю программы.

Заключение

Предложенная модификация программной реализации алгоритма должна значительно повысить её эффективность. Графическое представление результатов работы облегчает отладку, а независимость частей программы по потокам повышает эффективность её работы.

Список используемых источников

1. Моров В. А. Применение генетического алгоритма к задачам оптимизации. Реализация генетического алгоритма для задачи коммивояжера [Электронный ресурс] // Вестник Амурского государственного университета. Режим доступа: https://vestnik.amursu.ru/wp-content/uploads/2017/12/N57_4.pdf

2. Емельянов В. В., Курейчик В. В., Курейчик В. М. Теория и практика эволюционного моделирования. М. : Физматлит, 2003. С. 432.

3. Гладков Л. А., Курейчик В. В, Курейчик В. М. и др. Биоинспирированные методы в оптимизации: монография. М.: Физматлит, 2009. С. 384.

4. Северин Е. С. Биохимия: учеб. для вузов. М. ГЭОТАР-МЕД, 2003. 779 с. ISBN 5-9231-0254-4.

УДК-004.56.53

ЗАЩИТА ИНФОРМАЦИИ КРИПТОГРАФИЧЕСКИМ МЕТОДОМ РАЗДЕЛЕНИЯ СЕКРЕТА

А. Ф. Алмадатова, С. Г. Вердиев, А. Ф. Нагиева

Азербайджанский Технологический Университет

В работе приводятся системы безопасности передачи данных и рассматриваются методы обеспечения безопасности информационных систем с использованием криптографии, в частности, пороговой схемы Шамира. Перечислены свойства криптографического протокола, описывается криптографический протокол разделения секрета и методика его использования. В качестве примера решена задача разделения секрета. Результаты проведенных расчетов наглядно иллюстрируются кривой, представляющей собой пороговую схему с 8 участниками, между которыми делится секретный ключ.

защита информации, системы безопасности, передача данных, криптография, разделение секрета, секретный ключ, криптографический протокол, пороговая схема.

При нынешнем уровне развития интернет технологий и связанным с ней ростом обмена данными, вопросы информационной безопасности выходят на передний план и требуют разработки новых методологий в этом направлении. Разрабатываются и непрерывно внедряются всевозможные методы и системы безопасности данных. Системы безопасности передачи данных наглядно описываются структурной схемой на рис. 1 [1].

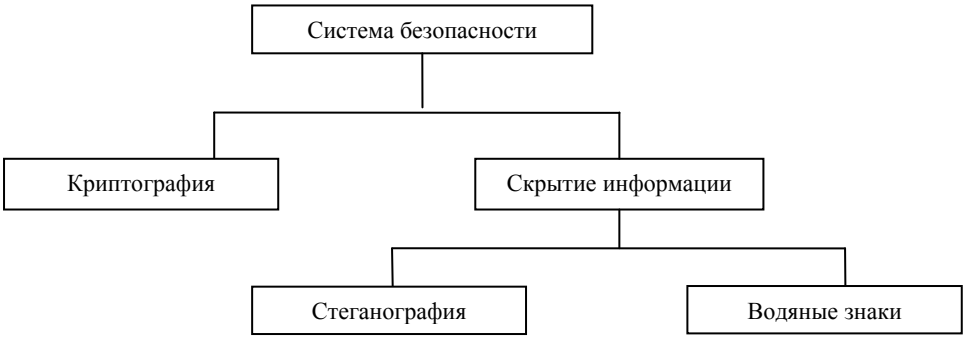


Рис. 1. Структурная схема системы безопасности передачи данных

Рассмотрим 2 направления в развитии информационной безопасности – криптографию и стеганографию.

1) Криптография. Отправитель (данных) используя шифровальный ключ К (*Key*) шифрует передаваемый текст (или аудио, видео) и передает этот текст по открытому для общего пользования каналу связи, а получа-

тель (тех же, но уже зашифрованных данных) при помощи специального алгоритма расшифровывает этот текст, при обязательном условии наличия у него дешифровочного ключа (К).

2) Стеганография. Стеганография в переводе с греческого языка означает «тайнопись» (стеганос – тайна, секрет, графия – писание) [2]. При этом методе секретное послание прячется в другом. Постоянный рост пользователей интернета диктует необходимость увеличения методов обеспечения безопасности обмена данными с использованием стеганографии. При обеспечении информационной безопасности компьютерных систем наиболее важную роль играют обе перечисленные выше криптографические методы. Наряду с этим на основе криптографического подхода с открытым ключом формируются структуры доверия, а конфиденциальность коммуникации между участниками обмена данными обеспечивается криптографией с секретным ключом, а надежность трансакций в электронных услугах с помощью технологии электронной подписи [3].

Криптографические методы используются как базовые технологии при ряде случаев обеспечения информационной безопасности компьютерных сетей. В криптографии используются криптографические протоколы. Криптографический протокол (КП) представляет собой последовательность действий двух или более сторон для решения определенной криптографической задачи. Криптопротокол отображает содержание каждой операции, выполняемой действующими субъектами или же циркуляцию информации между ними.

Криптографические протоколы обладают следующими свойствами:

1. Каждый участник предварительно должен знать протокол и все необходимые действия.

2. Каждый участник должен быть согласен с условиями протокола и обязан их выполнять.

3. Протокол должен быть определен корректно и однозначно.

4. Протокол должен быть законченным и всеохватывающим, отражающим в себе действия для всех возможных ситуаций.

Объектом исследований теории криптографических протоколов являются абоненты, расположенные на достаточном расстоянии и связанных между собой посредством открытых каналов связи.

Одним из видов криптографических протоколов являются протоколы разделения секрета. Основу метода составляет криптография.

Для криптографического разделения секрета используются соответствующие схемы. Термин разделение секрета и одноименная методология сохранения секретных данных относится к области защиты информации с условным допуском к ней только определенного числа лиц, которые должны иметь возможность пользования этими данными и несущими ответственность за неразглашение секрета, т. е. за информационную безо-

пасность. В структурной схеме 2 (рис. 2) в общем виде сгруппированы и представлены схемы разделения секрета и свойственные им проблемы [4].

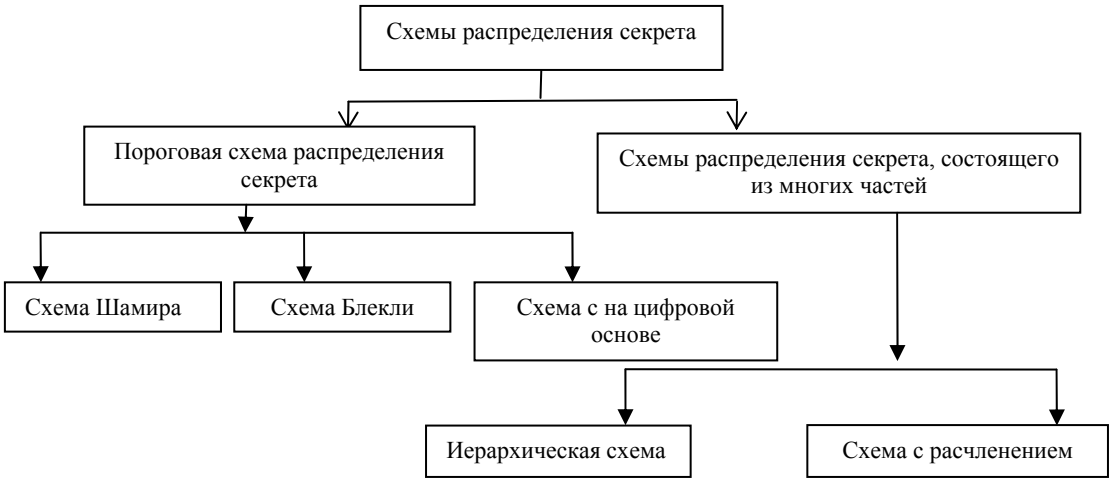


Рис. 2. Структурные схемы разделения секрета

Например, если имеется необходимость разрешения доступа к защищаемым данным, например, к тексту, с длиной n среди группы из t членов, то при любом из всевозможных методов разделения секрета каждому из членов группы участников выдается своя, предварительно условленная доля. В одиночку ни один из участников не способен воссоздать текст. Это могут сделать только участники коллективно.

Наряду с разделением возникает и необходимость в обратном в восстановлении секрета.

Схемы криптографического разделения секрета независимо друг от друга были предложены Шамиром А. М. и Блекли Г. Р.

Основным назначением этих схем является распределение ключей.

Протоколы разделения секрета позволяют разделить секрет между участниками протокола таким образом, чтобы корни многочленов, предварительно выданные участникам, могли однозначно восстановить секрет, а недозволенные же лица не могли заполучить информацию о возможных значениях секрета. В схемы разделения секрета входят 2 протокола: протокол формирования частей (разделение секрета) и протокол распределения их между пользователями, протокол восстановления секрета.

Схема Шамира

Примером граничной (t, n) схемы разделения секрета является схема Шамира [5]. Для построения граничной (t, n) схемы Шамир предложил использовать множество, в которой конечная предельная площадь со степенью $t - 1$ имеет достаточно большое количество элементов. Где n –

общее количество участников разделения секрета; t – число участников, которым предполагается выдать долю секрета.

Известно, что множество со степенью $t - 1$ однозначно можно восстановить по значениям различных t точек, однако при этом невозможно использовать меньшее количество точек для интерполяции.

Допустим, n количество участников протокола. Выберем площадь с пределом F и зафиксируем отличные от 0 n различных $r_1, r_2, \ldots, r_n$ элементов площади F. Каждый i-ый элемент обозначим соответственно тому участнику $i = 1, n$. Одновременно выберем случайные элементы $a_0, a_1, \ldots, a_{t-1}$ площади F в количестве $t + 1$ и на их основе составим множество $f(x)$ в степени $t - 1$ на площади F.

$$f(x) = \sum_{i=0}^{t-1} a_i x^i. \quad (1)$$

Примем, что $s = f(0) = a_0$ и рассчитаем значения $s_1 = f(r_1)$, $s_2 = f(r_2)$, …, $s_n = f(r_n)$ и в виде долей секрета (r_i, s_i) как пары распределим между участниками $i = 1, 2, \ldots, n$. В этой схеме свободный предел множества $f(x)$ это a_0 или секрет. Для восстановления секрета S используется формула интерполяции Лагранжа. Предположим, что имеются пары в количестве $t(x_i, f(x_i))$ где $x_1, \ldots, x_t$ являются различные попарные элементы площади F. Тогда формула Лагранжа имеет следующий вид:

$$f(x) = \sum_{i=0}^{t} f(x_i) \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

При $a_0 = f(0)$, уравнение Лагранжа будет:

$$a_0 = \sum_{i=0}^{t} f(x_i) \cdot \prod_{j \neq i} \frac{x_j}{x_i - x_j}.$$

Здесь значения $\prod \frac{x_j}{x_j - x_i}$ не зависят от значений множества $f(x)$ и поэтому могут быть предварительно рассчитаны. Преимуществом схемы Шамира является то, что допускает изменения числа участников, задействованных в процедуру разделения секрета. Для изменения числа участников разделения секрета достаточно дополнить множество $\{r_1, r_2, \ldots, r_n\}$ новыми элементами $r_n, r_{n+1}, \ldots, r_{n+w}$.

Рассмотрим пример решения задачи разделения секрета между тремя участниками в группе, состоящей из 8 членов, методом Шамира. При этом в схеме Шамира (3,8) в граничной схеме секрет $S = 19$ при $p = 23$. Требуется рассчитать значения долей, выданных участникам. Согласно (1) подставляя значения a_1 и a_2 в многочлен $f(x) = 19 + 6x + 11x^2$, находим

значения долей, выдаваемых участникам группы из 8-ми лиц, которые рассчитываются следующим образом

$$f(1) = (19 + 6 + 11) \bmod 23 = 13 \qquad f(5) = (19 + 30 + 275) \bmod 23 = 2$$
$$f(2) = (19 + 12 + 44) \bmod 23 = 6 \qquad f(6) = (19 + 36 + 396) \bmod 23 = 14$$
$$f(3) = (19 + 18 + 99) \bmod 23 = 21 \qquad f(7) = (19 + 42 + 539) \bmod 23 = 2$$
$$f(4) = (19 + 24 + 176) \bmod 23 = 12 \qquad f(8) = (19 + 48 + 704) \bmod 23 = 12$$

Решим поставленную задачу следующим образом.

На базе рассчитанных и приведенных выше значений многочлена (1) строим пороговую схему с 8-ю участниками (рис. 3).

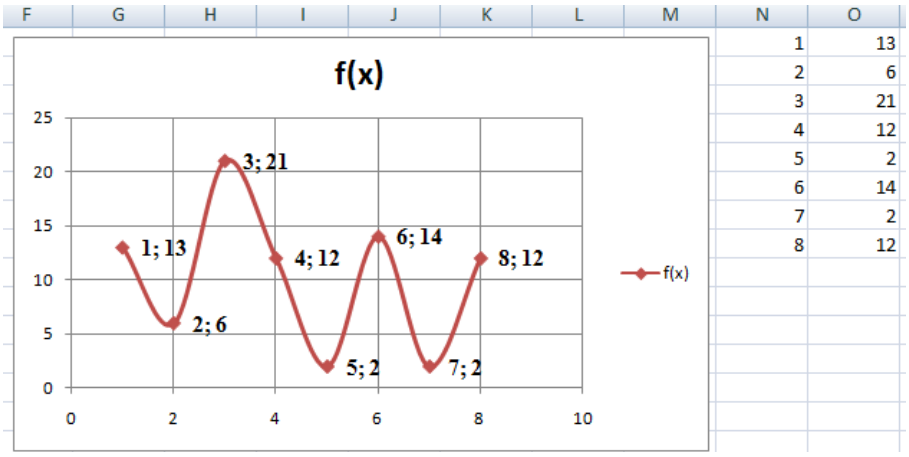


Рис. 3. Пороговая схема с 8-ю участниками

Здесь, функция $f(x) = S + a_1x + a_2x^2$ задания (1) представляет собой кривую, легко восстанавливаемую по 3 точкам.

Для восстановления секрета S достаточно минимум 3-х точек, включающих в себе свободный член s, расположенный на кривой, как точка пересечения с осью Y, т. е. $f(0) = S$.

Список используемых источников

1. Mandal P. C., Poddar B. P., Modern Steganographic technique // A survey International Journal of Computer Science & Engineering Technology (IJCSET), 2012, vol. 3, N 9. pp. 444–448.

2. Verdiyev S. Q, Nağıyeva A. F, İnformasiyanın steqanoqrafik gizlədilməsi metodlarının eksperimental analizi // İnformasiya təhlükəsizliyinin actual problemləri: III respublika elmi-praktiki seminarı., Bakı, 8 dekabr 2017. s. 51–55.

3. Əliquliyev R. M., İmamverdiyev Y. N. Rəqəmsal imza texnologiyası. Bakı: Elm, 2003, 132 s.

4. Nebiyev V. D, Suleymanzade X. A. Çok parçalı sır paylaşım şemaları ve uygulamaları.Trabzon, 2012, s. 68.

5. Shamir A. M. How to Share a Secret // Communications of the Acm. 1979. N 22. pp. 612–613.

УДК 336.711.2

ПРЕДПРИЯТИЕ ПАО «ПОЧТА БАНК». АНАЛИЗ ДЕЯТЕЛЬНОСТИ

А. Д. Андреев, К. В. Белоус, А. В. Бычихина Е. А. Пиликина

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

В представленной статье рассмотрены причины создания, анализ деятельности предприятия ПАО «Почта Банк», на основании годового отчёта за 2017 год. Отражены преимущества и недостатки в его деятельности, внесены предложения по улучшению качества предоставления услуг клиентам банка.

ПАО «Почта Банк», предприятие, клиент, вклады, кредит.

Заглянем в историю появления данной кредитной организации. ПАО «Почта Банк» был создан на базе ПАО «Лето Банк», входившего в банковскую группу ВТБ. Решение о создании «легкого банка» было принято руководством ПАО «ВТБ 24» в декабре 2011 г. [1].

В задачи нового банка входило завоевание клиентов, благодаря экспресс-кредитованию наличными и с помощью кредитных карт. Объём инвестиций в «Лето Банк» в 2012 г. составил более 1,2 млрд руб. В октябре 2012 г. состоялась официальная презентация бренда «Лето Банк» и запуск официального сайта.

По итогам 2012 г., было выдано более 12 000 кредитов на сумму 700 млн руб. Для работы с клиентами «Лето Банк» начал использовать систему процессинговой компании «МультиКарта», позволяющую получить POS-кредит наличными через банкомат.

До 2015 г. «Лето Банк» занимался потребительским кредитованием физических лиц: кредиты наличными и на товары, кредитные карты, банковский франчайзинг, а в 2015 г. запустил собственную программу вкладов. «Лето Банк» имел почти 640 клиентских центров и стоек продаж в Российской Федерации. В 2014 г. единственным акционером ПАО «Лето Банк» становится «ВТБ 24» [1].

В сентябре 2015 г. Группа ВТБ объявила о создании почтового банка совместно с «Почта России». Почтовый банк был организован путем вхождения дочерней организации ФГУП «Почта России» – ООО «Почтовые финансы» в капитал ПАО «Лето Банк». «Почта России» будет принадлежать 50 % минус одна акция, а группе ВТБ будет принадлежать 50 % плюс одна акция. Свою работу новый банк начал в 2016 г.

Банком было заявлено, что он будет присутствовать в 15 тыс. из 42 тыс. отделений «Почты России» и будет ориентирован на обслуживание массового и нижне-массового сегмента. Подписание документов между «ВТБ 24» и «Почта России» о создании «Почта Банка» и презентация бренда банка состоялись в январе 2016 года.

Услуги, которые предоставляет своим клиентам ПАО «Почта Банк» отражены в таблице 1.

ТАБЛИЦА 1. Виды услуг «Почта Банка»

Услуга	Виды услуги
Кредит	– Наличными (на любые цели); – Рефинансирование; – Льготный (на освоение «Дальневосточного гектара»); – На образование; – Для пенсионеров; – На оплату товаров и услуг.
Кредитные карты	– Для покупок «Элемент 120»; – Для экономных покупок «Карта «Пятерочка»»; – Со ставкой 0 % «Почтовый экспресс»; – Карта «Зеленый мир».
Дебетовые карты	– Для экономных покупок «Карта «Пятерочка»; – Карта «VISA PLATINUM»; – Карта «МИР»; – Виртуальная предоплаченная карта «Онлайн карта»; – Виртуальная карта «Онлайн карта 2.0»
Сберегательный счет	Проценты по одному из действующих тарифов распространяются на остаток по счету за определенный расчетный период: – Тариф «Базовый»; – Тариф «Зарплатный»; – Тариф «Пенсионный»; – Тариф «Зарплатный пенсионер».
Вклады	– Капитальный; – Доходный; – Накопительный.
Переводы	– Международные (Western Union); – С карты на карту (P2P).
Платежи	– Оплата коммунальных услуг; – Оплата связи; – Оплата образования; – Оплата услуг охраны.

В своей деятельности «Почта Банк» предусматривает снижение операционных издержек за счет масштабирования модели доступного розничного обслуживания и широкого использования цифровых каналов.

Для реализации данной цели Банк планирует развивать каналы дистанционного банковского обслуживания, увеличить сеть банкоматов (до 8 тысяч устройств) и POS-терминалов [1].

По данным официального сайта, распределение отделений «Почта Банка» на начало 2017 г. по федеральным округам [2] представлено на рис. 1.

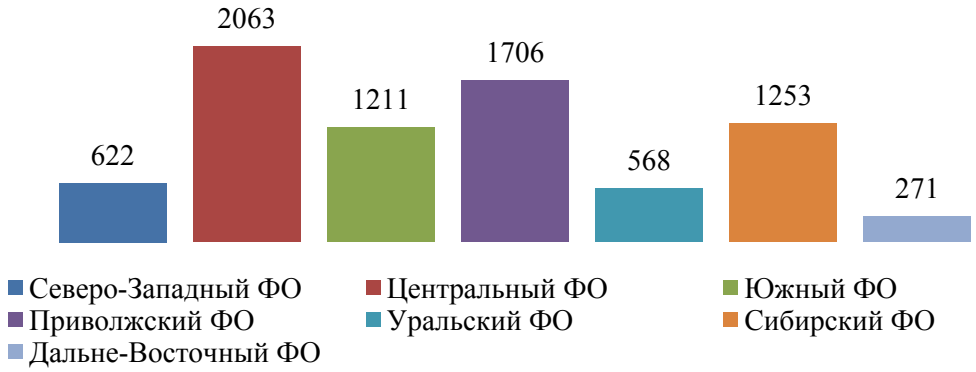


Рис. 1. Региональное распределение точек Почта Банка на начало 2017 года

Развитие Банка с момента образования по настоящее время можно проанализировать по следующим показателям: чистая прибыль, ROA (отношение прибыли к средним активам), ROE (отношение прибыли к среднему капиталу). Сравнение данных за период деятельности «Почта Банка» (2015–2017 гг.) [3] приведено в таблице 2.

ТАБЛИЦА 2. Результаты развития «Почта Банка»

Показатели	На 01.01.16, тыс. руб.	На 01.01.17, тыс. руб.	На 01.01.18, тыс. руб.	Изменение (+, –) 2016–2017	Изменение (+, –) 2017–2018
Чистая прибыль	1 416 771	84 181	5 596 963	–1 332 590 –94 %*	+5 512 782 +98 %*
ROA, %	2,12	0,76	3,01	–1,36	+2,25
ROE, %	21,22	8,41	31,06	–12,81	+22,65

* *Примечание.* Изменение чистой прибыли указано в тысячах рулей и %.

Динамика активов – один из основных показателей эффективности банка, по которому, в том числе, можно оценить его кредитоспособность, стабильность и надежность (рис. 2, см. ниже). Ниже, в таблицах 3–5 приведён анализ данных по активам, вкладам и кредитам за 2017 год [2].

По данным на январь 2018 г. Почта Банк занимает 31 место по размеру активов среди банков России. В начале 2017 г. – Банк занимал 54 место по данному показателю [3].

ТАБЛИЦА 3. Активы

Месяц/год	Размер активов, тыс. руб.	Изменение за месяц		Место по России
		абсолютное, тыс. руб.	относительное, %	
Январь 2017	131 590 327	+4 844 750	+3,68	54
Февраль 2017	136 435 077			
Март 2017	139 546 085	+12 918 043	+9,26	51
Апрель 2017	152 464 128			
Май 2017	160 436 196	+11 937 194	+7,44	47
Июнь 2017	172 373 390			
Июль 2017	194 046 339	+7 113 714	+3,67	43
Август 2017	201 160 053			
Сентябрь 2017	218 303 972	−8 757 102	−4,01	43
Октябрь 2017	209 546 870			
Ноябрь 2017	217 866 854	+16 453 068	+7,55	33
Декабрь 2017	234 319 922			
Январь 2018	263 843 928	+29 524 006	+12,60	31

ТАБЛИЦА 4. Вклады

Месяц/год	Размер вкладов, тыс. руб.	Изменение за месяц		Место по России
		абсолютное, тыс. руб.	относительное, %	
Январь 2017	35 369 880	+5 352 802	+17,83	53
Февраль 2017	30 017 078			
Март 2017	43 076 148	+3 544 461	+8,23	35
Апрель 2017	46 620 609			
Май 2017	51 228 563	+11 578 465	+22,60	30
Июнь 2017	62 807 028			
Июль 2017	85 954 868	+9 575 828	+11,14	23
Август 2017	95 530 696			
Сентябрь 2017	105 218 473	+9 967 502	+9,47	23
Октябрь 2017	115 185 975			
Ноябрь 2017	124 274 842	+12 313 081	+9,91	20
Декабрь 2017	136 587 923			
Январь 2018	165 780 010	+29 192 087	+17,96	18

По объему вкладов «Почта Банк» в январе 2018 г. находится на 18-ом месте. Стоит отметить уверенный рост по этому показателю в 2017 г., таким образом, можно говорить о тенденциях роста доверия населения к «Почта Банку» [3].

ТАБЛИЦА 5. Кредиты

Месяц/год	Размер кредитов, тыс. руб.	Изменение за месяц		Место по России
		абсолютное, тыс. руб.	относительное, %	
Январь 2017	104 914 294	+ 7 882 998	+7,51	14
Февраль 2017	112 797 292			
Март 2017	121 734 272	+8 840 800	+7,26	10
Апрель 2017	130 575 272			
Май 2017	137 844 643	+ 7 854 279	+5,70	8
Июнь 2017	145 698 922			
Июль 2017	153 348 799	+8 285 038	+5,40	7
Август 2017	161 633 837			
Сентябрь 2017	172 359 869	+5 366 197	+3,11	7
Октябрь 2017	177 726 066			
Ноябрь 2017	184 030 831	+ 6 614 806	+3,59	7
Декабрь 2017	190 645 637			
Январь 2018	173 154 780	–17 490 857	–9,17	8

По сумме выданных кредитов на текущий период (январь 2018 г.) «Почта Банк» занимает 8 место среди банков России [3].

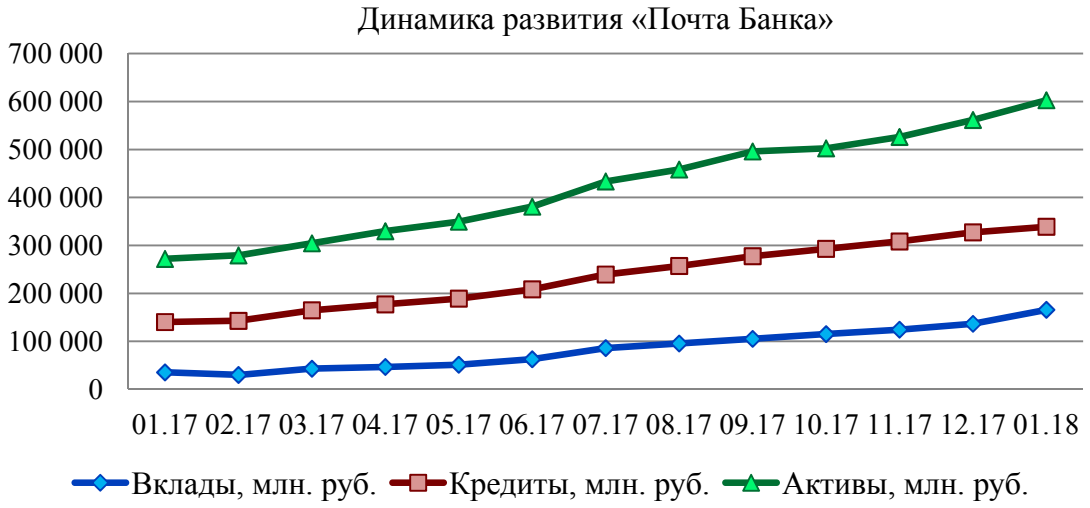


Рис. 2. Основные показатели деятельности «Почта Банка» за 2017 г.

Рейтинг надежности банковских организаций формируется, исходя из всевозможных финансовых аспектов [3]. Относительно коэффициентов, предложенных в таблице 6, а также места, занимаемого учреждением в своей отрасли по стране, можно судить о надежности «Почта Банка».

ТАБЛИЦА 6. Данные для рейтинга надежности

Финансовый аспект	Размер показателя, тыс. руб.	Место по России
Размер собственного капитала	27 473 500	40
Состояние кредитного портфеля	200 203 723	23
Чистая прибыль	5 596 963	21

Проанализировав деятельность ПАО «Почта Банка», можно выделить следующие преимущества и недостатки.

Преимущества:

- косвенное государственное участие;
- использование партнерской сети банкоматов;
- наличие online-банкинга.

Недостатки:

- активы менее 500 млрд рублей;
- скромный возраст банка – менее 10 лет;
- наличие скрытых комиссий.

«Почта Банк» является относительно новым участником рынка банковских услуг, и на данный момент менее 1 % всего населения России пользуются услугами данного банка. Несмотря на это, существует внушительное количество отделений по стране.

Но не смотря на ряд недостатков, можно сказать, что у ПАО Почта Банк есть будущее и неплохое. Это надежный и качественный финансовый партнер.

Список используемых источников

1. Официальный сайт ПАО «Почта Банк». [Электронный ресурс]// Почта Банк. URL: https://www.pochtabank.ru/

2. Годовой отчёт Публичного акционерного общества «Почта Банк» за 2016 год [Электронный ресурс] // Почта Банк. URL:https://www.pochtabank.ru/upload/images/documents/annual_report_2016.pdf

3. Рейтинг Почта Банка. [Электронный ресурс]. URL: http://1000bankov.ru/bank/650/?rating

УДК 004.056.5

ВОПРОСЫ БЕЗОПАСНОСТИ СТАНДАРТНЫХ АРХИТЕКТУР ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Я. В. Андреянов, В. И. Андрианов, Ю. А. Головлева, И. Ю. Сергеева

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

В статье рассматриваются вопросы безопасности государственных информационных систем, вопросы сохранности информационных ресурсов и защищённости, в инфокоммуникационных системах государственных органов власти. Авторы в своей работе отталкиваются от того, что информационная безопасность – это сохранность информационных ресурсов и защищённости, законных прав личности и общества в информационной сфере, это процесс обеспечения: конфиденциальности, целостности и доступности.

ГИС, класс защищённости, уровень значимости, информации, угрозы безопасности информации.

Вопросы безопасности государственных информационных систем сегодня актуальны. Текущие организационные и технические мероприятия, проводимые организациями для защиты конфиденциальной информации с одной стороны достаточно широкие, с другой стороны их недостаточно как показывает практика. Так, например, антивирусы не уберегли многие государственные организации от вирусов шифровальщиков в 2017 г., в частности от WannaCry Petya.A, ExPetr, NotPetya, GoldenEye и т. д.

Анализ

На сайте ФСТЭК России опубликованы документы в области защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [1, 2] и для обеспечения защиты информации, содержащейся в ГИС, предлагается проводить следующие мероприятия:

– формировать требования к защите информации, содержащейся в ГИС;

– разрабатывать систему защиты информации ГИС;

– внедрять систему защиты информации ГИС;

– проводить аттестацию ГИС по требованиям защиты информации и вводить ее в действие;

– обеспечивать защиту информации в ходе эксплуатации аттестованной ГИС;

– обеспечивать защиту информации при выводе из эксплуатации, аттестованной ГИС или после принятия решения об окончании обработки информации.

Большинство организаций в государственном секторе работает по принципу: «Не трогай, пока работает», а такие проблемы как текучка кадров и нехватка финансирования, длительность согласования изменений в бюджет приводят к тому, что вышеперечисленные мероприятия ограничиваются бумагами или частично реализуются для прохождения проверок со стороны контрольно-надзорных органов власти.

Одновременно с этим сегодня разработаны методические указания, направленные на классификацию ГИС и помощь в выборе соответствующих мер защиты. Документами ФСТЭК России установлены четыре класса защищенности ГИС, определяющие уровни защищенности, содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Согласно методическим рекомендациям степень возможного ущерба ГИС может быть:

ВЫСОКОЙ – если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в международной, политической, социальной, финансовой и экономической или иных областях деятельности, не могут выполнять возложенные на них функции.

СРЕДНЕЙ – нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в международной, политической, социальной, финансовой и экономической или иных областях деятельности, не могут выполнять хотя бы одну из возложенных на них функций.

НИЗКОЙ – если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в международной, политической, социальной, финансовой и экономической или иных областях деятельности, могут выполнять с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Уровень значимости информации (УЗ) формируются отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в ГИС, устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности конфиденциальности, и доступности информации каждого вида информации (табл.).

ТАБЛИЦА. Класс защищенности ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Согласно методическому документу «Меры защиты информации в государственных информационных системах» информационные системы подлежат классификации по степени защищенности. Установлены 4 класса защищенности информационной системы, а именно I класс, II класс, III класс, IV класс, определяющие уровень защищенности информации в ней. Самым высоким классом является I класс, низкий – IV класс [1].

Класс защищенности информационных систем определяется уровнем значимости информации, обрабатываемой в данной системе, и ее масштабом.

Класс защищенности (К) = [Уровень значимости информации; Масштаб системы]

Уровень значимости информации (УЗ) формируется степенью вероятного вреда для владельца информации и оператора от нарушения конфиденциальности, единства или доступности информации:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)]

Угрозы безопасности информации (УБИ) формируются по результатам оценки способностей (потенциала, оснащенности и мотивации) наружных и внутренних нарушителей, исследования вероятных уязвимостей информационной системы, вероятных способов осуществления угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности)

УБИ = [возможности нарушителя; уязвимости информационной системы; способ реализации угрозы; последствия от реализации угрозы] [2].

Таким образом, согласно трем этим характеристикам в информационной системе подлежат реализации следующие меры:

– идентификация и аутентификация субъектов доступа и объектов доступа;
– управление доступом субъектов доступа к объектам доступа;
– ограничение программной среды;
– защита машинных носителей информации;
– регистрация событий безопасности;

– антивирусная защита;
– обнаружение (предотвращение) вторжений;
– контроль (анализ) защищенности информации;
– обеспечение целостности информационной системы и информации;
– обеспечение доступности информации;
– защита среды виртуализации
– защита технических средств;
– защита информационной системы, ее средств и систем связи и передачи данных.

Меры по защите информации, выбираемые в информационной системе, должны гарантировать блокировку угроз безопасности информации, использующиеся в модель угроз безопасности информации.

Мероприятия по доступу субъектов и объектов обязаны гарантировать присвоение субъектам и объектам доступа оригинального признака (идентификатора), сопоставление предъявляемого субъектом (объектом) доступа идентификатора со списком присвоенных идентификаторов, а еще проверку субъекта (объекта) доступа на принадлежность показанного им идентификатора (подтверждение подлинности)

Меры по управлению доступом субъектов доступа к объектам доступа обязаны гарантировать управление правами и привилегиями субъектов доступа, разделение доступа субъектов доступа к объектам доступа на базе совокупности установленных в информационной системе законов разграничения доступа, а также обеспечивать контроль соблюдения этих законов.

Меры по ограничению программной среды обязаны гарантировать установку и (или) запуск лишь допустимого к использованию в информационной системе программного обеспечения либо исключать право установки и (или) запуска, запрещенного к применению в информационной системе программного обеспечения.

Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) обязаны исключать право несанкционированного доступа к машинным носителям и хранящейся на них информации, а также неразрешенное применение съемных машинных носителей информации.

Меры по регистрации событий безопасности обязаны гарантировать сбор, запись, хранение и защиту информации о действиях безопасности в информационной системе, а также право просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите обязаны гарантировать разоблачение в информационной системе компьютерных программ или иной компьютерной информации, предопределенной для неразрешенного уничтожения,

блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений обязаны гарантировать установление действий в информационной системе, нацеленных на предумышленный неразрешенный доступ к информации, специальные действия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности информации обязаны гарантировать контроль уровня защищенности информации, которая содержится в информационной системе, порядком проведения мероприятий по анализу защищенности информационной системы и испытанию ее системы защиты информации.

Меры по обеспечению доступности информации обязаны гарантировать авторизованный доступ пользователей, обладающих правом по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите информационной системы, ее средств, систем связи и передачи данных обязаны гарантировать защиту информации при взаимодействии информационной системы или ее единичных сегментов с иными информационными системами и информационно-телекоммуникационными сетями с помощью использования архитектуры информационной системы, проектных заключений по ее системе защиты информации, нацеленных на предоставление защиты информации.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также установление мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обязаны гарантировать управление преобразованиями конфигурации информационной системы и системы защиты персональных данных, обзор потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Выводы

Таким образом, первоочередной задачей является необходимость обеспечения безопасности информации в соответствии с ее значимостью, Обязательное построение модели нарушителя, модели угроз и ежегодное обновление документов по ИБ, в связи с быстрым темпом обновления спо-

собов и типов угроз для различных ИС. Разделение мероприятий позволит защитить ГИС от воздействия вируса шифровальщика, например. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе. Соблюдая требования информационной безопасности и разумно проводя экономическую политику, государство напрямую и опосредованно может добиться развития данной части информационного сектора рынка, в полном соответствии с принятой доктриной информационной безопасности.

Список используемых источников

1. Компьютерная преступность и информационная безопасность // Под ред. А. П. Леонова. Минск : АРИЛ, 2000. 552 с.

2. Мирошников Б. Н. Борьба с киберпреступлениями одна из составляющих информационной безопасности Российской Федерации [Электронный ресурс] / 30.07.2003. Источник: crime-research.ru. URL: http://www.crime-research.ru/articles/Mirosh1/2

УДК 519.688

ПРИМЕНЕНИЕ МУЛЬТИАГЕНТНОГО ПОДХОДА ДЛЯ ПОСТРОЕНИЯ СИСТЕМ АРОМОБЕЗОПАСНОСТИ

В. В. Антонов

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

В статье рассматривается построение системы аромобезопасности с использованием мультиагентов. Применение такого подхода позволит построить универсальную информационно-мониторинговую систему способную принимать решения и адаптироваться под изменяющиеся внешние условия.

аромобезопасность, мультиагентная система, интеллектуальные агенты.

В настоящее время активно разрабатываются и внедряются различные автоматизированные системы контроля безопасности техногенных объектов. Начало таких разработок было положено Распоряжением Правительства Российской Федерации о необходимости разработки единой базовой системы мониторинга критически важных объектов и потенциально опас-

ных объектов инфраструктуры [1]. Такие системы уже используются на особо опасных, технически сложных объектах, представляющих угрозу жизни и здоровья большому количеству людей или окружающей среде.

Достоинства подобных систем очевидны и обусловлены возможностью постоянного предоставления данных с датчиков, установленных на объектах, с заданной частотой и в любых погодных условиях.

Однако, как отмечается в докладе [2], значительное количество техногенных катастроф происходит из-за так называемого «человеческого фактора», который не поддаётся алгоритмическому описанию и обработке. Кроме того, уникальность каждого объекта, имеющего индивидуальные конструктивные особенности воздействие различных случайных внешних факторов, не позволяет применить унифицированные алгоритмы обработки данных. Исходя из этого могут быть сформулированы следующие задачи, решаемые системой в условиях неопределённости:

1. Принятие решения на основе имеющихся данных.
2. Адаптация к изменениям в окружающей среде.
3. Работа с большим объёмом данных разнородной структуры.
4. Самостоятельное принятие управленческих решений.

Для решения подобных задач используются мультиагентные технологии, реализуемые на взаимодействии между собой интеллектуальных агентов, способных к общению между собой и совместному принятию решений. Общая теория интеллектуальных агентов описана в фундаментальной работе Стюатра Рассела и Питера Норвига [3]. Условная схема простого рефлексивного агента для использования в системе аромобезопасности представлена на рис. 1.

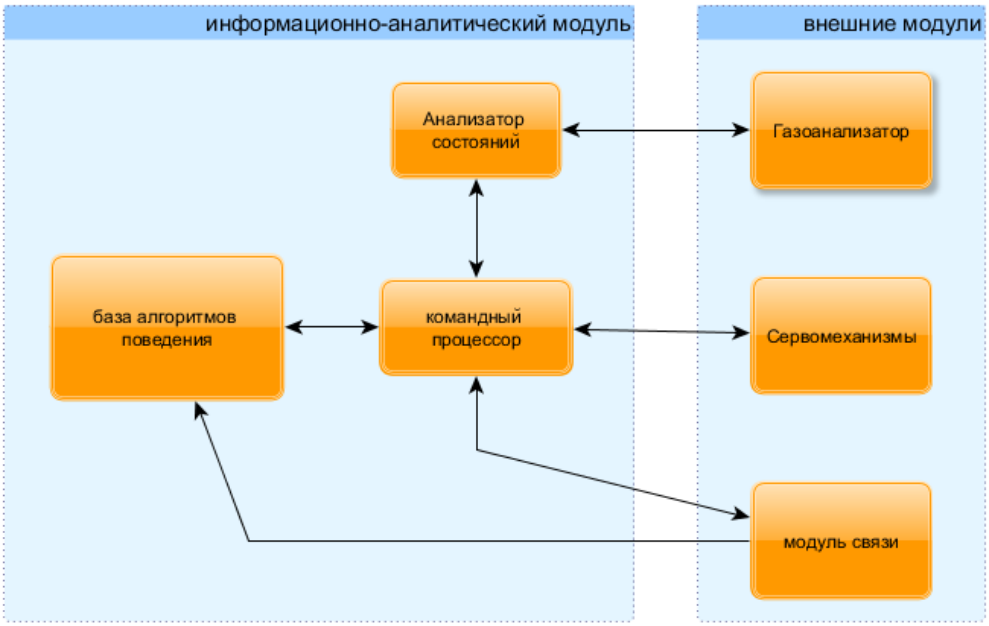


Рис. 1. Схема рефлексивного агента

Каждый агент включает в себя внешние элементы, состоящие из датчиков для сбора информации и исполнительные механизмы и информационно-аналитического модуля (ИАМ). Рефлексивные агенты действуют на основе знаний присутствующих в системе в текущий момент. Их поведение основывается на функции вида условие-действие.

Рассмотрим возможную реализацию такого агента для применения в системах аромобезопасности. Интеллектуальным ядром агента является «командный процессор» принимающий информацию от блока «анализатор состоянии» и реагирующий на эту информацию управлением механизмами сервоприводов. Реакция агента определяется алгоритмами поведения, хранящимися в базе. К блоку «анализатор состояний» подключены датчики газоанализаторы, сигнализирующие изменением уровня передаваемого сигнала при наличии в окружающей среде регистрируемого газа. Получив информацию об изменении состояния, командный процессор запрашивает у базы алгоритмов поведения алгоритм реагирования.

Возможные алгоритмы реагирования можно разделить на информационные и сервисные. Первые заключаются в передаче информации о изменении состояния по каналам связи на сервер событий [4] и возможной выдаче локального информационного сообщения по каналам громкой связи. Сервисные алгоритмы реагирования предполагают механические реакции системы, например, открытие заслонок, перекрытие вентелей, включение принудительной вентиляции.

Поведенческие особенности подобной системы можно описать графом состояний, представленным на рис. 2. Направление дуг графа соответствуют путям перехода системы из начального состояния в конечное. Дробь вида p_x/s_x представляет вероятность – p перехода по данной дуге графа, а s – условные единицы задействованных ресурсов.

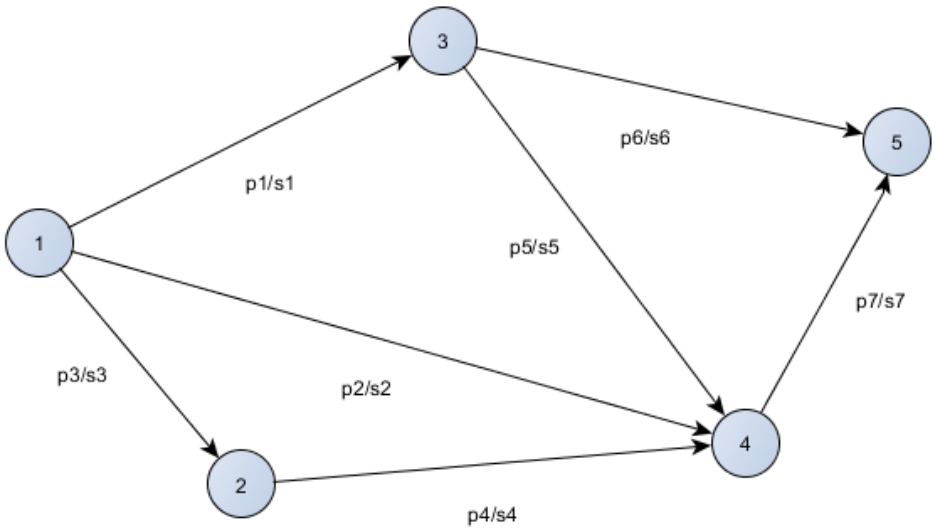


Рис. 2. Схема графа состояний

Выбор наилучшего пути в такой системе можно провести на основе минимизации задействованных ресурсов. Критерии выбора могут быть различны и существенно отличаться в зависимости от индивидуальных особенностей самой системы и окружающей её среды. Так, например, реакция информационной части системы на утечку газа может быть различной в зависимости от направления ветра и объёма газа.

Объединение агентов в систему позволяет существенно расширить возможности системы аромобезопасности:

1. Значительно расширится возможность информационной составляющей системы и её информационного обмена. В отсутствии прямой связи с сервером событий агенты могут использовать друг друга для передачи сообщений по цепочке.

2. Адаптация газоанализаторов системы под конкретный тип газа обнаруженного одним из агентов системы.

3. Включение в систему «спящих агентов» для обнаружения следов утечек газов облачного характера и анализа концентрации газов на различных расстояниях от эпицентра утечки.

Таким образом создание систем аромобезопасности, основанных на мультиагентном подходе повысит эффективность работы системы и даст гарантию её бесперебойной работы.

Список используемых источников

1. Концепция Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов (ФСМ КВО и ОГ). Распоряжение Правительства Российской Федерации от 27 августа 2005 г. № 1314-р. // Собрание законодательства РФ. 29.08.2005. № 35. Ст. 3660.

2. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2011 году». М. : МЧС России; ФГБУ ВНИИ ГОЧС (ФЦ), 2012. 315 с.

3. Рассел С., Норвиг П. Искусственный интеллект: современный подход; пер. с англ. М. : И. Д. Вильямс, 2015. 1408 с.

4. Антонов В. В. Построение информационно-мониторинговой системы аромобезопасности на аппаратно-программных средствах // Информационная безопасность регионов Росии-2017. Юбилейная X Санкт-Петербургская межрегиональная конференция: материалы конференции, СПОИСУ. СПб., 2017. С. 501–502.

Статья представлена заведующей кафедрой, доктором технических наук, профессором Л. К. Птицыной.

УДК 007.53

ПРОБЛЕМЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ И ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ В СРЕДЕ ИНТЕРНЕТ ВЕЩЕЙ

В. Д. Артемьева[1], А. Ю. Гришенцев[2], Д. И. Дикий[2], А. Г. Коробейников[2, 3]

[1]Балтийский федеральный университет им. И. Канта
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский филиал Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук

В работе рассмотрены проблемы информационной безопасности на уровне беспроводных сенсорных и исполнительных устройств среды Интернет вещей. Рассмотрены аспекты применения технологии радиочастотной идентификации и методы повышения уровня защищенности. Описаны проблемы безопасности сенсорных сетей.

Интернет вещей, безопасность, исполнительные и сенсорные устройства, RFID-технологии, беспроводные сенсорные сети.

Прогнозируется, что в третьем десятилетии XXI века число устройств, подключенных к среде Интернет вещей [1] превысит 18 млрд устройств. Наряду с большим распространением и внедрением этих технологий в повседневную жизнь людей, а также в промышленные процессы, немаловажным становится вопрос о безопасности. Здесь под безопасностью подразумевается не только физическая безопасность устройств от хищения или уничтожения, но и все другие аспекты информационной безопасности, свойственные автоматизированным системам, обрабатывающим информацию [2, 3, 4]. Под угрозой становятся процессы приема и передачи информации, ее обработки и хранения с учетом особенностей устройств, подключаемых к среде Интернет вещей [5].

Как правило, принято изначально рассматривать архитектуру среды Интернет вещей [6]. Здесь существует множество мнений о том, сколько всего можно выделить слоев в данной системе, также распределение их границ, взаимосвязей и другое. Например, в архитектуре ITU-T Y.2002 предлагается разделение на 3 слоя [7]. Однако, все они сходятся к тому, что основой среды Интернет вещей являются исполнительные и сенсорные устройства. Объединяя в сеть десятки и сотни таких устройств под управлением одним или несколькими вычислительными центрами [8, 9] (или в случае для самоопределяющихся ad-hoc сетей [10] – самими устройства-

ми) получается достигнуть поставленных перед средой Интернет вещей целей.

Таким образом, ключевое значение в среде Интернет вещей имеют исполнительные и сенсорные устройства, особенности которых будут рассмотрены далее.

Вопросы безопасности RFID технологий и решений RFID. Бесконтактная технология автоматической идентификации, которая может автоматически идентифицировать сигнал радиометки для получения соответствующих данных, не требует вмешательства пользователя и может работать в суровых метеорологических условиях. В то время как технология RFID широко используется, она также представляет много проблем безопасности.

В настоящее время нет единого международного стандарта кодирования для радиометок. Каждый производитель предлагает свой стандарт и программное обеспечение для кодирования информации в радиометках. Это может вызвать проблемы с получением доступа к информации.

Возможен конфликт, когда несколько радиометок могут одновременно передавать данные к считывателю, что приводит к ошибкам. Во избежание подобных ситуаций применяются определенные методы.

Внедрение защиты конфиденциальности в радиометках приводит к ограничению ресурсов. Конфиденциальность данных можно разделить на две категории: физические схемы и схемы, основанные на паролях. В дальнейшем стали применяться схемы, основанные на хэш функциях и множественном шифровании.

Внедрение радиометок может способствовать получению злоумышленником сведений о местоположении объекта. Например, при использовании радиометок на транспортных средствах.

Управление доверием также играет немаловажную роль. Здесь рассматривается не только связь между радиометкой и считывателем, но и связи между считывателями.

На данный момент криптографические алгоритмы и протоколы требуют больших вычислительных ресурсов, чем имеется у технологии радиоидентификации. Следовательно, создаваемые для этой технологии алгоритмы и протоколы должны не только учитывать условия безопасности и конфиденциальности, но также принимать во внимание вычислительные мощности [11, 12, 13, 14, 15, 16, 17].

Беспроводные сенсорные сети имеют широкое распространение. К сожалению, большинство устройств, входящих в такие сети также, как и в случае с RID метками, имеют множество ограничений. А именно, небольшое количество энергонезависимой и энергозависимой памяти, малые вычислительные мощности, малая энергоемкость. Эти устройства необходимы для сбора информации и данных. В процессе сбора данных, возмож-

ны утечки информации, появление вредоносной маршрутизации, подделка сообщений и другие.

Вопросы безопасности беспроводных сенсорных сетей можно обобщить в виде конфиденциальности данных, аутентичности данных, целостности данных и актуальности данных. Эти четыре вида проблем безопасности могут быть решены с помощью криптографических алгоритмов, управление ключевой информацией, защищенной маршрутизация и управлением доверия.

Криптографические алгоритмы в беспроводных сенсорных сетях применяются в случае обработки информации, где необходима конфиденциальность и целостность информации. Алгоритм шифрования для беспроводных сенсорных сетей можно разделить на симметричные и ассиметричные.

Ввиду малой вычислительной мощности и большого потребление энергии асимметричные алгоритмы шифрования трудно применимы в данном случае. Наоборот, алгоритм симметричного шифрования широко используется в беспроводных сенсорных сетях из-за его простоты.

Алгоритмы симметричного шифрования обладают недостатками, а именно уязвимы протоколы обмена ключами, алгоритм имеет плохую масштабируемость, в то время как алгоритмы с открытыми ключами не имеют этих недостатков. В настоящее время широко стали применимы алгоритмы на эллиптических кривых. Симметричное шифрование и асимметричное шифрование имеют свои преимущества, но по-прежнему не могут полностью решить все проблемы безопасности беспроводной сенсорной сети датчика.

Управление ключами – это один из важнейших вопросов. Он включает в себя процесс генерации, распространения, хранения, обновления и уничтожения секретных ключей, где распределение ключей является наиболее важной проблемой. Распределение ключей, включая распространение открытого ключа и секретного ключа, заключается в обеспечении безопасной транспортировки и распространения ключей среди законных пользователей. Подходы к управлению ключевой информацией можно разделить на: широковещательную передачу по всей сети, групповое распределение ключей, распределение главного ключа узла, распределение ключа, разделяемого между узлами.

Другим важным аспектом является протокол безопасной маршрутизации. Атаки на протокол маршрутизации приведут непосредственно к краху сети. В отличие от традиционной схемы проверки подлинности такие как SSH и SSL, в сенсорной сети требуется, чтобы проверка подлинности производилась между узлами. Исследования в этой области можно разделить на следующие две категории: протоколы безопасной маршрутизации, раз-

работанные специально для беспроводной сенсорной сети и анализ потенциальных уязвимостей протоколов маршрутизации [18].

Таким образом, можно сделать вывод о том, что для уровня исполнительных и сенсорных устройств среды Интернет вещей характерны проблемы безопасности, не только свойственные другим устройствам, имеющим выход в сеть интернет, но и также связанные с ограниченным количеством ресурсов: объем памяти, вычислительная и энергетическая мощность. Большинство из рассмотренных аспектов безопасности будут развиваться на ряду с внедрением технологий, развитием аппаратных платформ и технических возможностей.

Список используемых источников

1. По прогнозу Ericsson, к 2022 году в интернете будет 29 млрд устройств, включая 18 млрд устройств IoT // ixbt.com URL: https://www.ixbt.com/news/2016/11/15/ericsson-2022-29-18-iot.html (дата обращения 21.01.2018).

2. Коробейников А. Г., Кутузов И. М., Колесников П. Ю. Анализ методов обфускации // Кибернетика и программирование. 2012. № 1. С. 31–37.

3. Коробейников А. Г., Кутузов И. М. Алгоритм обфускации // Кибернетика и программирование. 2013. № 3. С. 1–8.

4. Коробейников А. Г, Гатчин Ю. А. Математические основы криптологии : учебное пособие. СПб. : СПбГУ ИТМО, 2004. 106 с, илл.

5. Md Anam Mahmud, Ahmed Abdelgawad, Kumar Yelamarthi Energy efficient routing for Internet of Things (IoT) applications // IEEE International Conference on Electro Information Technology. 2017. PP. 442–446.

6. Puthal, D., Ranjan, R., Nepal, S., Chen, J.d IoT and big data: An architecture with data flow and security issues // 2nd EAI International Conference on ICT Infrastructures and Services for Smart Cities. 2018. Vol. 189. PP. 243–252.

7. Стандарт ITU-T Y.2002 SERIES Y: Global information infrastructure, internet protocol aspects and next-generation networks, 22 с.

8. Гришенцев А. Ю., Коробейников А. Г. Средства интероперабельности в распределенных геоинформационных системах // Журнал радиоэлектроники. 2015, № 3. С. 19.

9. Гришенцев А. Ю., Коробейников А. Г., Дукельский К. В. Метод численной оценки технической интероперабельности // Кибернетика и программирование. 2017. № 3. С. 23–38.

10. Ahmed W, Elhadef M. Securing intelligent vehicular ad hoc networks: A survey. Lect Notes Electr Eng 2018; Vol. 474. PP. 6–14.

11. Гришенцев А. Ю., Коробейников А. Г. Понижение размерности пространства при корреляции и свертке цифровых сигналов // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 3. С. 211–218.

12. Коробейников А. Г. Разработка и анализ математических моделей с использованием MATLAB и Maple : учебное пособие. СПб. : СПбГУ ИТМО, 2010. 144 с.

13. Коробейников А. Г. Проектирование и исследование математических моделей в средах MATLAB и Maple. СПб. : СПбГУ ИТМО, 2012. 160 с.

14. Коробейников А. Г., Гришенцев А. Ю. Разработка и исследование многомерных математических моделей с использованием систем компьютерной алгебры. СПб. : НИУ ИТМО, 2014. 100 с.

15. Гришенцев А. Ю., Гурьянов А. В., Тушканов Е. В., Шукалов А. В., Коробейников А. Г. Виртуализация и программное обеспечение в системах автоматизированного проектирования : учебное пособие. СПб. : Университет ИТМО, 2017. 60 с.

16. Гришенцев А. Ю., Гурьянов А. В., Кузнецова О. В., Шукалов А. В., Коробейников А. Г. Математическое обеспечение в системах автоматизированного проектирования. СПб. : Университет ИТМО, 2017. 88 с.

17. Гришенцев А. Ю., Коробейников А. Г., Гурьянов А. В., Шукалов А. В. Автоматизация проектирования распределенных геоинформационных систем: учебное пособие. СПб. : Университет ИТМО, 2017, 96 с.

18. Jing Q., Vasilakos A. V., Wan J., Lu J., Qiu D. Security of the internet of things: Perspectives and challenges. Wireless Networks, 20(8), 2014, pp. 2481–2501.

УДК 004.023

ОБЪЕКТИВНЫЕ МЕТРИКИ КАЧЕСТВА СТЕРЕОСКОПИЧЕСКИХ ИЗОБРАЖЕНИЙ

Н. М. Ахмедов, В. И. Курносов

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

Методы оценки качества восприятия изображений и совершенства телевизионных систем начали развиваться практически одновременно с появлением телевидения. Без разработки этих методов невозможна стандартизация систем, которая является основой промышленного производства товаров, к которым относятся и устройства, и контент. Оценка качества – ключевой критерий в проектировании и оптимизации систем для передачи объемного видео контента.

Рядом промышленных компаний и научных организаций предложены метрики для оценки перцепционного качества двумерных изображений. Однако гораздо меньшее внимание до последнего времени уделялось качественной оценке пространственных изображений. Между тем 3D отображение – широкая исследовательская область, в которой заинтересованы как индустрия развлечений, так и многочисленные научные приложения.

ТВ, 3D, качество.

Объективные оценки качества стереоскопических изображений основываются на измерениях качества двумерных изображений [1].

Объективные метрики оценки качества изображения и видео могут быть классифицированы по наличию искажений независимых сигналов изображения или видео, которые могут быть использованы для сравнения полученных искаженных сигналов изображения и видео и искаженных сигналов, имеющихся в распоряжении [2].

Метрики, которые принимают, что оригинальные данные доступны, определяются как метрики изображений и видео полной ссылки (*full-reference,* FR) [3]. Когда ссылочные изображения и видео последовательности не доступны, говорят о не ссылочных измерениях качества (*no-reference,* NR) [3]. Встречаются такие случаи, когда сигнал оригинального изображения полностью не доступен, но доступны некоторые его части. Они могут быть использованы для помощи в процессе вычисления качества. Такие вычисления называют сокращенно ссылочными (*reduced-reference,* RR) [3].

Для объективной оценки качества двумерных изображений и применимых также к оценке объемных изображений используется множество метрик. Ниже представлены некоторые из них.

Самая популярная метрик это PSNR, она использовалась для множества сравнений кодеков. Peak Signal to Noise Ratio (PSNR) – инженерный термин, являющийся отношением максимально возможной мощности сигнала к мощности портящего шума, действующего на качество сигнала. В связи с широким диапазоном PSNR обычно выражается в логарифмической шкале (dB) [4, 5]. Эта метрика применяется для оценки качества компрессии изображения. Mean Square Error (MSE) вычисляется для двух изображений, одно обычно компрессированное изображение другого. Вычисление происходит по следующему равенству:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{x=0}^{m-n}\sum_{y=0}^{n-1}\left\| I(x,y) - I'(x,y)\right\|^2,$$

где $I(x,y)$ – значение пикселя оригинала; $I'(x,y)$ – компрессированной версии; m, n – размеры изображений.

PSNR определяется следующим выражением:

$$PSNR = 10\cdot\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\cdot\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right),$$

где MAX_I – максимальное значение пикселя изображения. Низкое MSE показывает меньшую ошибку, и так как PSNR имеет обратное отношение с MSE, высокое значение PSNR показывает наличие меньшей ошибки. Наибольшее значение PSNR схемы компрессии считается лучшим.

Метрика MSAD [6]. Значением данной метрики является усреднённая абсолютная разность значений цветовых компонент в соответствующих точках сравниваемых изображений. Используется, например, для отладки кодеков или фильтров.

$$d(X,Y) = \frac{\sum_{i=1,j=1}^{m,n}|X_{i,j}-Y_{i,j}|}{mn}.$$

Одними из оценок, чаще встречающихся в литературе для оценки качества объемного изображения являются краткое подытоживание структурного подобия briefly summarize the Structural SIMilarity (SSIM) и C4.

SSIM (*Structural SIMilarity*) основывается на замере трёх компонент (сходности по яркости, по контрасту и структурного сходства) и объединения их значений в итоговый результат [4].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y\, c_1)(2cov_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)\,(\sigma_x^2+\sigma_y^2+c_2)},$$

где μ_x – усреднение x; μ_y – усреднение y; σ_x^2 – изменение x; σ_y^2 – изменение y; cov_{xy} ковариация y; $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ две переменных для стабилизации деления со слабым знаменателем; L – динамический диапазон значений пикселя (~~обычно~~ $2^{\#bits\ per\ pixel} - 1$); $k_1 = 0{,}01$ и $k_2 = 0{,}03$ по умолчанию.

Основная идея SSIM заключается в работе с предположением, что визуальное восприятие человека хорошо адаптируется для выделения структурной информации из сцены. Оценка качества основана на деградации воспринимаемой структурной информации, которую ошибочная видимость не должна приравнивать к потере качества, так же как некоторые искажения могут быть видимы, но не раздражать. SSIM на прямую измеряет структурные изменения между двумя совокупно-структурными сигналами (complex-structured signals) [4].

C4 – измерения, основанные на сравнении структурной информации искаженного изображения и оригинала. Этот метод использует реализацию детально разработанной модели зрительной системы человека. Весь процесс может быть представлен двумя этапами. Во время первого воспринимаемое изображение создается в оригинальном и искаженном виде, а затем, на втором этапе, изображения сравниваются по определенной шкале качества [4].

Оба этих метода могут оценивать параметры для каждой стереопары отдельно. Зависимость между DMOS и каждой из объективных метрик для каждого из рассматриваемых искажений вычисляются после «вычерчивания карты» в соответствии с вычислениями для каждого метода. Более детально «вычерчивание карты» (“*mapping*”) происходит при применении нелинейных функций по рекомендации VQEG [6], в соответствии с картой оценок измерений в области субъективной оценки. Для каждого случая параметры оптимизируются. Как предварительные результаты, среднее значение измерений для левого и правого глаз дает лучший результат среди остальных методов.

Основным недостатком данных измерении является, неучтенность восприятие объема изображения, а недостаток информации о глубине может привести к несоответствию между измерениями качества 2D и 3D изо-

бражений. Например, в некоторых случаях ухудшение одного изображения стереопары (фильтр размытия *blurring filter*) может помочь получить лучшее впечатление объема у зрителя, несмотря на то, что изменение качества двумерного изображения стереопары несвязно с улучшением восприятия стерео.

В статье «Quality Assessment of Stereoscopic Images» авторы Alexander Benoit, Patrick Le Callet, Patrizio Campisi и Romain Cousseau. Представили улучшения для исследования по множеству дополнительной информации о глубине изображения, влияющей на процесс измерения качества, в основе которой положена понятия диспарности, так как это напрямую связано с восприятием объема. Рассматривая две соответствующие точки для левого и правого изображений, вектор между этими точками будем называть диспаратностью. Диспаратность может быть использована для создания одного изображения стереопары по-другому. Два различных алгоритма вычисления диспаратности были выбраны для этой цели: один под названием “bpVision”, и второй “kz1”. Эти два алгоритма создают диспаратность по значениям MRF (*Markov random field*). Алгоритм bpVision использует доверительное распространения (*uses belief propagation*) для выводов, а kz1 алгоритм использует графические нарезки (*graph cuts*), следовательно, представление значений MRF будут различны. Метод графической нарезки дает более сглаженные результаты. А метод доверительного распространения включает в себя некоторые структуры, которые упущены в методе графической нарезки. С вычислительной точки зрения, метод графической нарезки эффективнее. Когда диспаратность появляется вследствие передачи по каналу связи или операций обработки сигнала, карта диспаратности стереопары изменяется, это представлено на рисунке, где показаны карты диспаратности оригинального изображения и после JPEG2000 кодера [5].

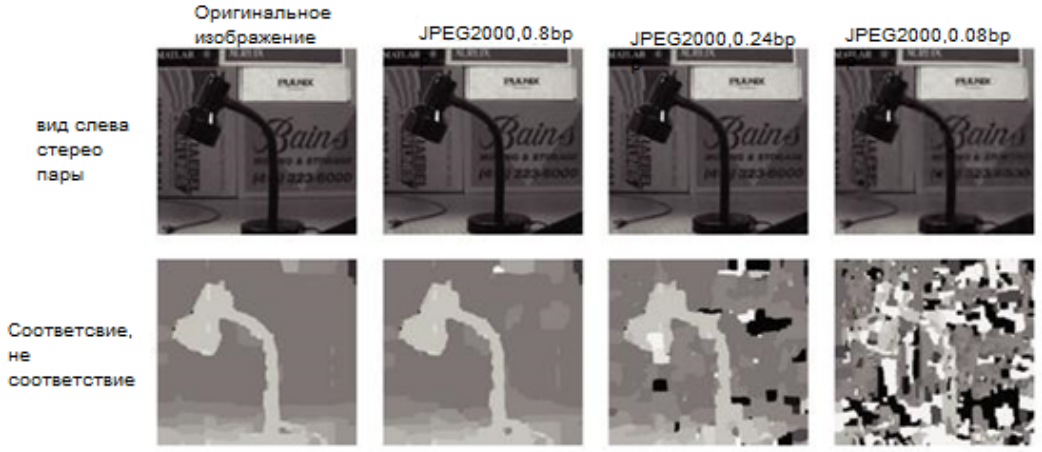


Рисунок. Карта диспаратности оригинального изображения и после кодирования, применялся алгоритм bp Vision

Телевизионное объемное изображение, которое наблюдается на экране (воспринимаемое изображение) должно максимально соответствовать исходному, т. е. восприятие передаваемого образа должно максимально соответствовать восприятию реального образа. Это соответствие и должно определять визуальное качество телевизионного объемного изображения.

Качество последнего может рассматриваться на различных уровнях и в различных аспектах – содержательных, эмоциональных, идеологических, творческих, технических и других. Для каждого из аспектов определяются свои параметры изображения, а также характеристики и оценки качества, которые зависят, в том числе и от назначения системы.

Параметры технического аспекта соответствия реального и воспроизводимого телевизионного изображения должны быть выбраны так, чтобы подробно воспроизвести в сознании зрителя все характеристики образа.

Основными качественными характеристиками зрительного образа являются:

- геометрические формы и относительные размеры;
- различимость деталей;
- распределение яркости;
- цветность;
- расположение предметов по глубине;
- восприятие относительного движения предметов.

В данной статье для оценки качества объемного изображения были использованы объективные методы, однако, когда речь идет о визуальном качестве, наиболее предпочтительны субъективные.

Список используемых источников

1. Лукин М. И., Черный В. Я. Измерение расхождения во времени сигналов яркости и цветности // Электросвязь. 1982. № 9. С. 34–35.

2. Миненко Ю. Г. А.с. 146367. Устройство для измерения отношения сигнал/помеха. Опубл.1962. Бюл. № 8.

3. ANSI T1.801.03-1996. "American National Standard for Telecommunications – Digital Transport of One-Way Video Telephony Signals – Parameters for Objective Performance Assessment," Alliance for Telecommunications Industry Solutions, 1200 G Street, N. W., Suite 500, Washington DC 20005.

4. Кривошеев М. И., Мкртумов А. С., Федунин В. Г. Методы оценки качества изображения в цифровом телевидении // Прогресс технологий телерадиовещания. Материалы международного конгресса. НАТ, Москва, 1–3 ноября 1999 г. (TRBE-99). Тезисы докладов. М., 1999. С. 189–190.

5. Lauterjung, J. Picture quality measurement. In: International Broadcasting Convention, Amsterdam, 11–15 September 1998. IEE, London, 1998. pp. 413–417.

6. Stephen Wolf. Features for Automatic Quality Assessment of Digitally Transmitted ITU Study Group VQEG (Visual Quality Experts' Group). See http://www.itu.int and ftp://ftp.its.bldrdoc.gov/dist/ituvidq.

УДК 004.054

РАЗРАБОТКА МЕТОДОВ ПРОВЕРКИ СООТВЕТСТВИЯ СЕРВЕРОВ ВИРТУАЛИЗАЦИИ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ СОГЛАСНО СТАНДАРТУ ГОСТ Р 56938-2016

А. Р. Багомедова, И. А. Ушаков, А. Ю. Цветков

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

В статье рассматриваются основные требования, предъявляемые к виртуальной инфраструктуре: методы защиты, и способы реализации данных методов на основе ГОСТ Р 56938-2016, которые будут способствовать улучшению уровня безопасности информационной системы. Так же будет разобран прототип алгоритма разрабатываемого автоматизированного решения для проверки предъявляемых требований к серверам виртуализации согласно ГОСТ Р 56938-2016.

виртуализация, гипервизор, ГОСТ.

Как в государственных, так и в негосударственных системах виртуализации, есть перечень объектов, подлежащих защите от несанкционированного доступа, изменения, блокировки и хищения информации ограниченного доступа, содержащей как конфиденциальные сведения, так и сведения составляющие государственную тайну, находящиеся в данной системе. В приказах ФСТЭК России регламентировано выполнение определенных мер защиты среды виртуализации, используемой при обработке информации в автоматизированных системах, государственных информационных системах и системах персональных данных. В связи с этим все организации, являющиеся операторами данных информационных систем и применяющие технологии виртуализации, обязаны выполнить необходимые меры защиты и привести свою вычислительную инфраструктуру в соответствие требованиям регулирующих органов. Для защиты информации, обрабатываемой с использованием технологий виртуализации, были разработаны соответствующие требования, одним таким перечнем требований является национальный стандарт Российской Федерации ГОСТ Р 56938-2016. В нем представлены угрозы безопасности и меры защиты информации, обрабатываемой с помощью технологий виртуализации. При использовании технологий виртуализации создаются (виртуальные и виртуализованные) объекты доступа, подлежащие защите наравне с другими объектами информационных систем, в том числе аппаратные средст-

ва информационных систем, используемые для реализации технологий виртуализации. Для защиты таких объектов используются специальные средства защиты информации. Сейчас на рынке виртуализации можно приобрести различные системы защиты, внедряемые в имеющуюся (или разрабатываемую) виртуальную инфраструктуру, способствующие полному или частичному улучшению уровня безопасности, которые строятся на выполнении соответствующих требований российских регуляторов в области информационной безопасности.

Перед рассмотрением главной темы статьи, определимся с определениями, которыми будем оперировать [1]:

− виртуализация – группа технологий, основанных на преобразовании формата или параметров программных, или сетевых запросов компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

− гипервизор I типа – гипервизор, устанавливаемый непосредственно на аппаратное обеспечение в качестве системного программного обеспечения.

− гипервизор II типа – гипервизор. устанавливаемый вереде хостовой операционной системы в качестве прикладного программного обеспечения.

− виртуальная инфраструктура – композиция иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств

− виртуальная машина – виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать программное обеспечение и пользовательские данные.

− гостевая операционная система – операционная система, установленная в виртуальной машине.

В национальном стандарте Российской Федерации по Защите информации при использовании технологий виртуализации (ГОСТ Р 56938-2016) приведен перечень особенностей защиты информации, которые разделены на несколько групп в зависимости от объекта защиты и различных предъявляемых к ним требований, которые варьируются по уровню и глубине от класса защищенности информационной системы. К основным требованиям, предъявляемые к объектам защиты, не зависящие от типа серверов виртуализации, относится:

− блокировка возможности включения репликации виртуальных машин;

− блокировка возможности миграции виртуальных машин;

− блокировка возможности экспорта виртуальных машин;

− блокировка возможности создания и удаления контрольных точек виртуальных машин;

− политика затирания файлов жестких дисков при удалении виртуальных машин;

− запрет хранения дисков виртуальных машин и конфигураций в корневом разделе;

− запрет хранения дисков виртуальных машин и конфигураций на системном разделе;

− политика проверка имени учетной записи локального администратора заданным требованиям безопасности;

− политика проверка имени гостевой учетной записи заданным требованиям безопасности;

− запрет смены MAC – адресов;

− политика проверки состояния сервисов, позволяющих предотвратить обмен данных между виртуальной машиной и серверов;

− политика проверки состояния служб, отвечающих за синхронизацию времени между сервером и виртуальной машиной;

− запрет удаленного доступа к менеджеру служб на сервере

− и пр.

Для осуществления проверки серверов виртуализации заданным выше требованиям, будем предполагать, что система виртуализации построена следующим образом: имеются сервера виртуализации, на которых расположено несколько виртуальных машин, доступ к которым разграничен [2]. Попытки получения доступа к конфиденциальным и защищённым данным будем осуществлять с хоста, находящемся в отличной подсети от серверов виртуализации. Реализуем два варианта попытки получения доступа: при первом – пользователь не аутентифицирован в системе, предназначенной для разграничения доступа, и его действия будут является несанкционированными, при втором – пользователь аутентифицирован в системе и пытается осуществить ряд действий, противоречащих требованиям безопасности. Защита информационной системы настроена заданным образом, зависящим от выбранного решения, предлагаемого на рынке. В нашем случаем, тестирование разрабатываемого автоматизированного решения для проверки соответствия серверов виртуализации заданным требованиям выполняется с использованием сертифицированного средства защиты информации, предназначенного для обеспечения безопасности виртуальной инфраструктуры на базе систем VMware vSphere и Microsoft Hyper-v – vGate 4.0 (рис. 1).

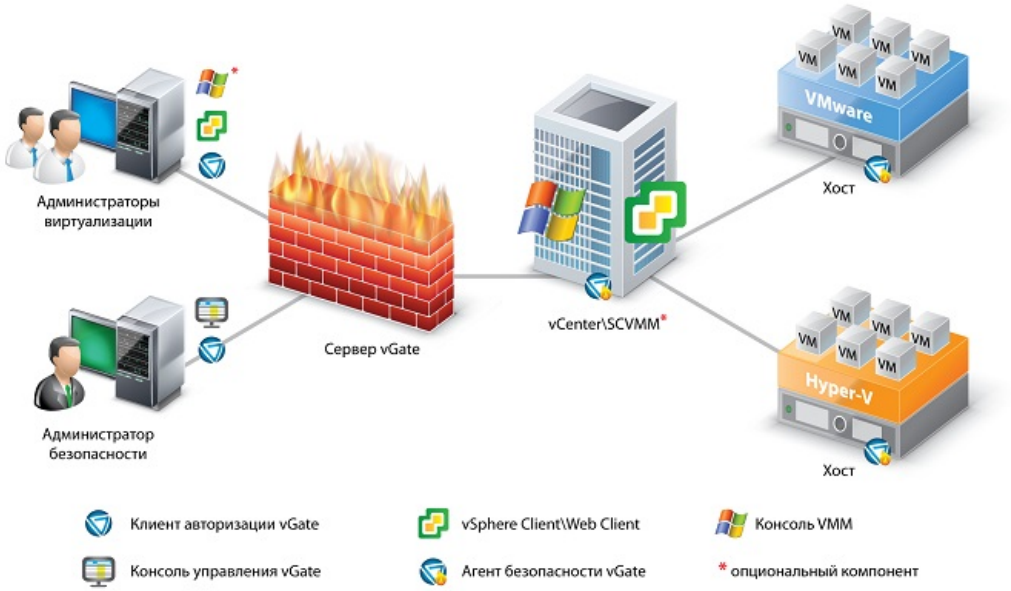


Рис. 1. Архитектура развертывания инфраструктуры с использованием vGate

Разрабатываемое решение предназначено для оценки настроенной инфраструктуры и политик безопасности в среде виртуализации, которое после окончания своего выполнения выводит отчет (рис. 2), соответствия данных серверов указанным требованиям в ГОСТ Р 56938-2016 и с перечнем необходимых мер по улучшению уровня безопасности.

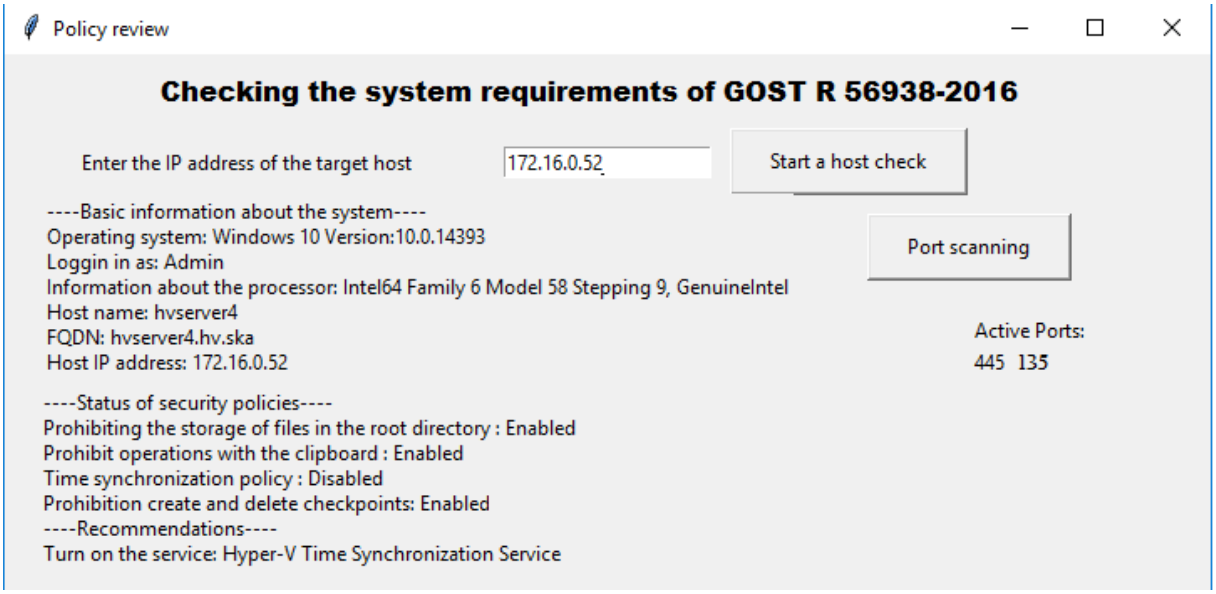


Рис. 2. Пример отчета после проведенной проверки сервера

Рассмотрим более подробно само разрабатываемое автоматизированное решение и его алгоритм работы и механизм осуществления проверок, и критерии принятия решений. Для написания данного решения, основным

языком программирования выбран Python, так как он отлично подходит для написания сценариев для автоматизации задач, и анализа данных [3]. Так же он позволяет использовать мощный инструмент, как Scapy для работы с сетью и проведения исследований в области информационной безопасности. При запуске данного решения, и указания сервера виртуализации, для которого будет осуществлена проверка, выполнится анализ самой системы гипервизора. Исходя из собранных данных о системе, при различных видах осуществления манипуляция для проверки требований, будет использоваться тот или иной механизм работы с объектами инфраструктуры (*PowerShell* / *PowerCLI*). При запуске данного решения на хосте, с которого будет осуществляться проверка требований, выполняется сбор сведений о системе, и дальнейшие операции, связанные с обычной работой в среде виртуализации, но доступ, к которым ограничен или невозможен. На основе успеха или неудачи выполнения данных манипуляции, строится отчет об проведенных операциях и мерах улучшения уровня безопасности системы, а так же делается вывод о том, удовлетворяет ли наша система тем или иным требованиям, которые будут рассматриваться как политики безопасности системы и иметь два состоянии: политика будет считаться влечёной в случае если выполнение действий, направленных на преодоление данной политики не увенчалось успехом; и политика будет считаться выключенной, когда действия, направленные на ее преодоление, увенчалось успехом.

Однако, нужно уточнить, что не все решения о состояниях тех или иных политик являются одноэтапными. Для некоторых политик будет применяться многоэтапное принятие решений. Многоэтапность приводит к тому, что схема принятия решения может быть представлена в виде дерева, в каждой вершине которого осуществляется либо: 1) Выбор между двумя состояниями; 2) Обработка события при исключениях.

Выбор между двумя состояниями ничем не отличается от одноэтапного принятия решения, за исключением того, что один этап принятия решения может накладываться на другой, образуя древовидную системы с единственным результатом на выходе (рис. 3). А обработка событий при исключениях необходим в многоэтапности для того чтобы избежать случаев, когда система будет не в состоянии обработать запрос.

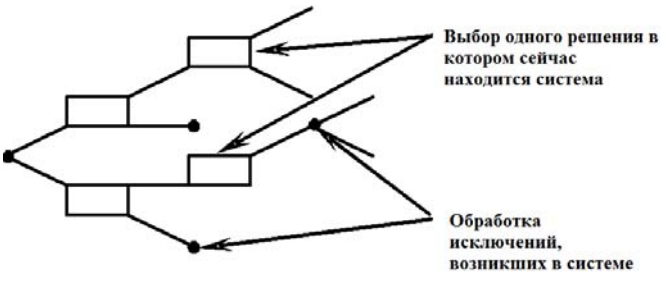


Рис. 3. Многоэтапное принятие решений

Из всего выше сказанного можно заключить, что данное решение актуально для администраторов информационной безопасности и для ад-

министраторов виртуальной инфраструктуры при проведении плановых и внеплановых проверок соответствия собственной инфраструктуры требованиям безопасности согласно стандарту ГОСТ Р 56938-2016. Так же оно пригодится для тестирования системы и определения используемых политик, при невозможности доступа к серверу авторизации (управляющему серверу), который осуществлял настройку политик безопасности и разграничение доступа к объектам инфраструктуры.

Список используемых источников

1. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общее положение. М. : Стандартинформ, 2016. 30 с.

2. ООО «Код Безопасности». vGate R2 Hyper-V. Руководство администратора. Установка, настройка и эксплуатация [Электронный ресурс] // Руководство администратора. Установка, настройка, эксплуатация: техническая документация 2017. URL:https://www.securitycode.ru/upload/documentation/vgate/vGate_R2_Hyper_V_Руководство_администратора_Установка_настройка_эксплуатация.pdf С. 15–20 (дата обращения 05.02.2018).

3. Мэтиз Э. Изучаем Python. Программирование игр, визуализация данных, веб-приложения. СПб. : Питер, 2017. 496 с.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 681.518 + 004.35 + 004.42

РАЗРАБОТКА ИНФОРМАЦИОННОЙ ПАНЕЛИ НА БАЗЕ СВЕТОДИОДНЫХ МАТРИЦ

К. В. Белоус, В. А. Вачугова

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

Разработано техническое устройство, которое визуализирует в виде «бегущей строки» различную учебно-организационную информацию, а также информацию о параметрах внешней среды. Техническое устройство реализовано на программируемой плате Node MCU со встроенным Wi-Fi модулем. В качестве устройства визуализации использовался светодиодный модуль, построенный на базе микросхем MAX7219.

информационная панель, светодиодная матрица, программируемая плата, Arduino.

В настоящее время жизнь большинства людей связана с обработкой и анализом информации, представленной в различных видах. Среди боль-

ших массивов информации встречается как полезная и необходимая, так и информационный шум, представленный, прежде всего, рекламной информацией. В условиях мощного информационного потока особо актуальным является вопрос о простых и эффективных способах донесения важной информации до непосредственного получателя [1]. В виду того, что до 80 % информации человек воспринимает через органы зрения – глаза, поэтому в статье рассматривается прототип технического устройства, позволяющего визуализировать необходимую информацию в виде «бегущей строки». Особую важность обладание актуальной информацией имеет для сферы образования – для информирования студентов и преподавателей об изменениях в расписании занятий, о проведении мероприятий развлекательного и научного плана, а также для предоставлять срочную, безотлагательную информацию в случаях чрезвычайных ситуации; кроме того, система может выводить информацию о дате и времени, и о параметрах внешней среды, в частности о температуре, влажности и давлении.

Для разработки информационной панели было решено использовать программируемую плату Node MCU, которая имеет встроенный Wi-Fi модуль, что позволяет ей стать полноценным объектом локальной или глобальной сети. Плата имеет небольшие размеры, относительно низкую стоимость, низкое энергопотребление, большое количество выводов для подключения других периферийных устройств и датчиков, а также обладает возможностью беспроводного обновления [2]. Данная плата представлена на рис. 1.

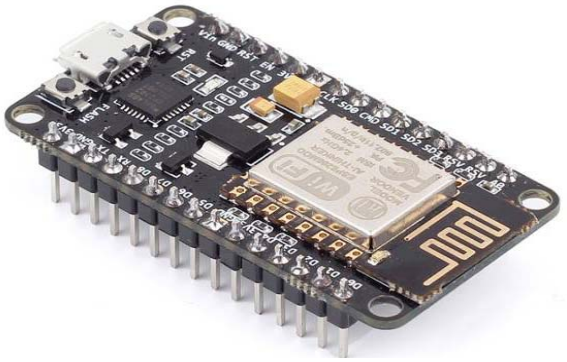


Рис. 1. Плата Node MCU

В качестве устройства визуализации выбран светодиодный модуль, построенный на базе микросхем MAX7219 (рис. 2). Данный вариант позволяет объединять несколько модулей в единую систему, что делает возможным построение светодиодных панелей больших размеров, оптимальных для восприятия информации человеческим глазом. Существует возможность выбора цвета, используемого для индикации выводимого сообщения. Доступны красный, синий, зелёный и жёлтые цвета. В данном случае использовался модуль с синей индикацией.

Для реализации вывода информации о параметрах внешней среды были использованы: датчик давления HX711 и датчик влажности и температуры DHT11. Датчики представлены на рис. 3.

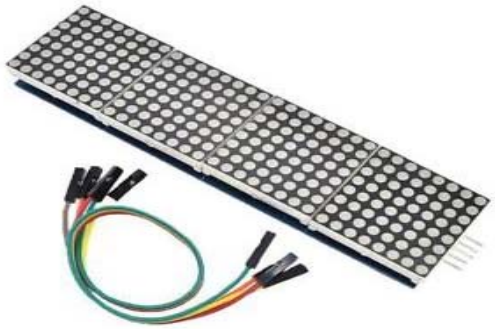


Рис. 2. Светодиодный модуль MAX7219

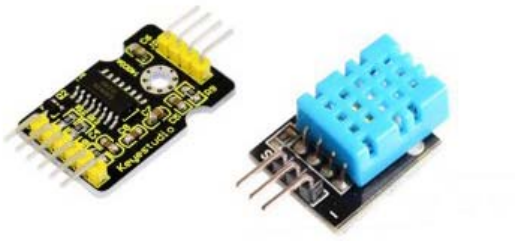


Рис. 3. Датчик HX711 и DHT11

Обобщенный алгоритм функционирования информационной панели представлен на рис. 4.

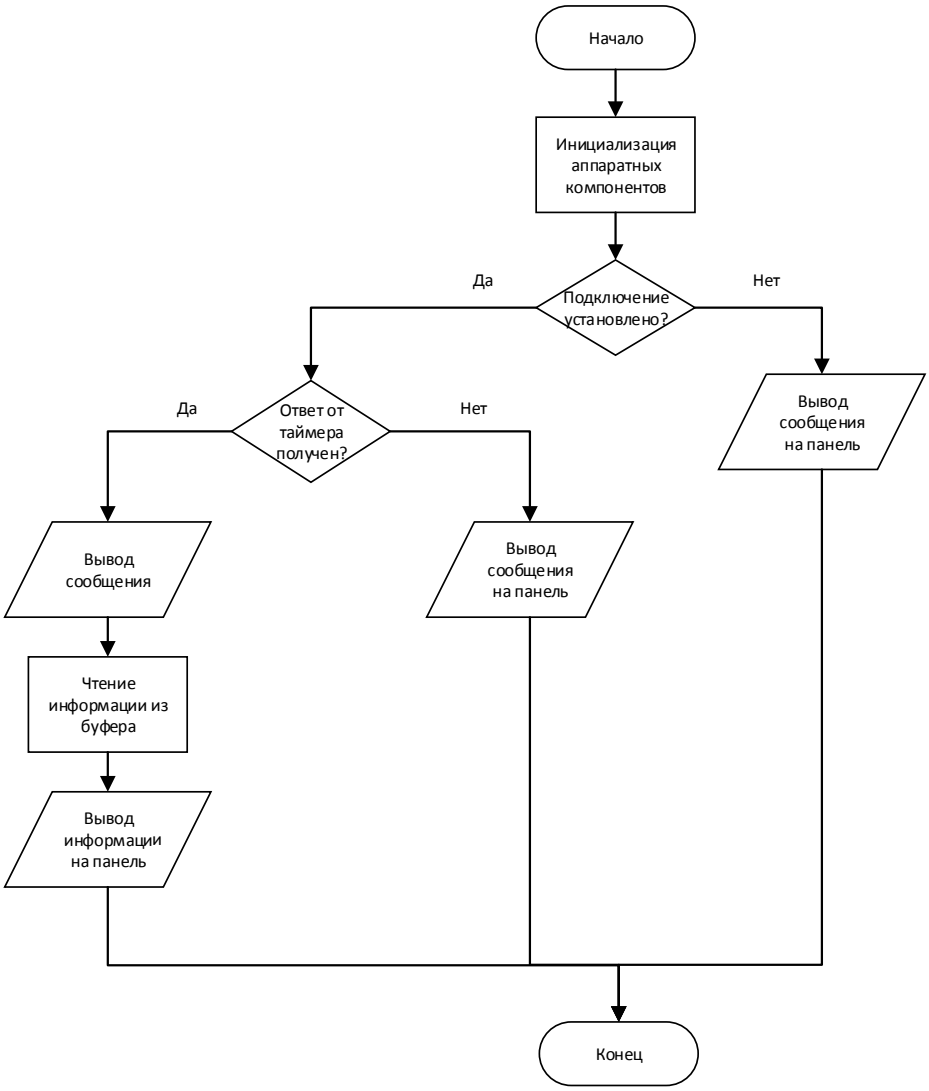


Рис.4. Блок-схема функционирования информационной панели

Прототип технического устройства представлен на рис. 5.

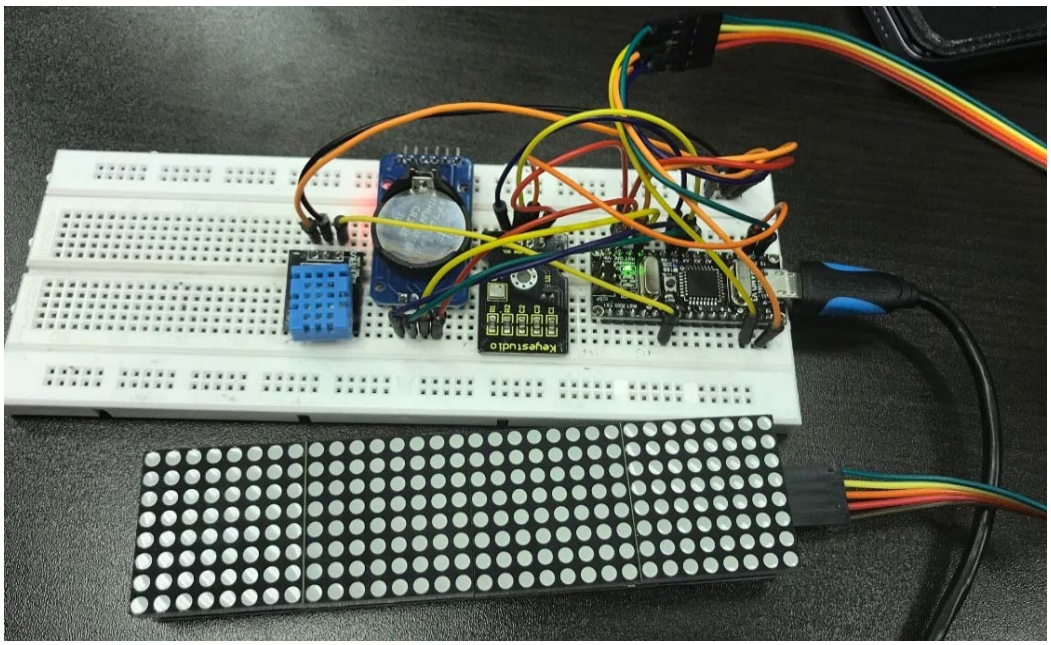


Рис. 5. Прототип технического устройства

Архитектура системы построена на основе клиент-серверной технологии (рис. 6). Для реализации серверной части была использована технология Microsoft ASP.Net [3]. В системе предусмотрена парольная защита, что позволяет снизить вероятность несанкционированного доступа, и вывода на панель нежелательной информации. Существует возможность вывода стандартных сообщений, либо ввода пользовательского текста. Вся информация о попытках входа, добавлении сообщений, а также технические данные сохраняются в БД, работающей под управлением СУБД MS SQL Server. При необходимости количество информационных модулей может быть расширено.

Интерфейс серверной части представлен на рис. 7.

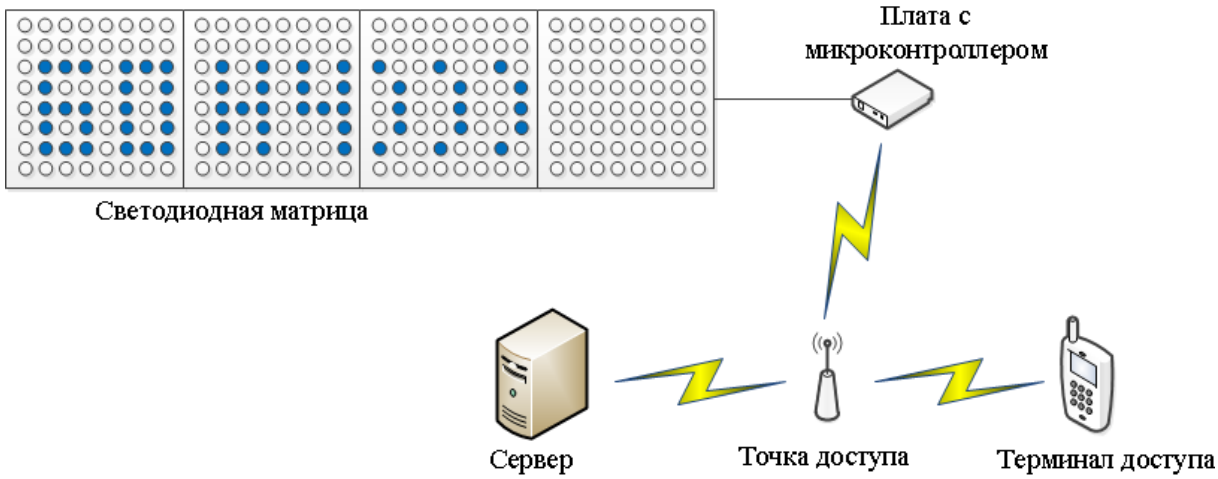


Рис. 6. Архитектура системы

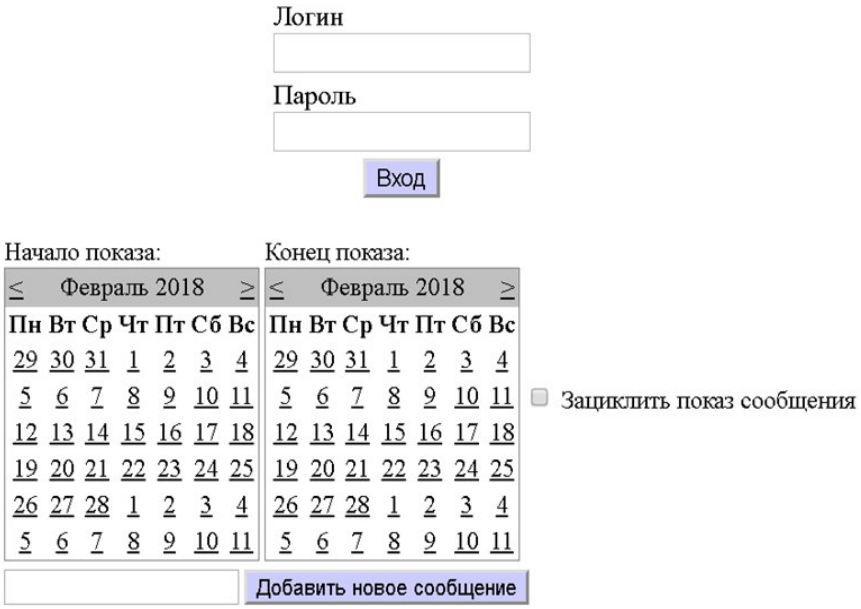


Рис. 7. Авторизация и ввод пользовательского сообщения

В дальнейшем предполагается усовершенствование данной системы путем добавления нескольких светодиодных модулей, что позволит существенно расширить возможности выведения визуальной информации.

Список используемых источников

1. Крапивенко А. В. Технологии мультимедиа и восприятие ощущений : учебное пособие. М. : БИНОМ. Лаборатория знаний, 2009. 271 с. : ил.

2. Петин В. Проекты с использованием контроллера Arduino. Серия Электроника. СПб. : БХВ-Петербург, 2015. 400 с. : ил.

3. Фримен А., Сандерсон С. ASP.NET MVC 3 Framework с примерами на C# для профессионалов М. : Вильямс, 2011. 672 с. ил.

УДК 004.031.42

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС УЧЁТА МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ

К. В. Белоус, А. А. Григорьева

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

Рассмотрен прототип клиент-серверного приложения предназначенного для учёта сведений о материальных ценностях, находящихся на балансе учреждения, предприятия или организации. Проведён анализ предметной области, на основе кото-

рого спроектирована объектная модель. В качестве языка программирования использован язык C#. Базовой технологией разработки явилась технология ASP.Net. Хранение данных осуществляется в реляционной СУБД MS SQL Server. Реализована базовая поддержка устройств чтения штрихкодовых идентификаторов, смарт-карт и меток RFID.

материальные ценности, база данных, учёт, СУБД, радиочастотная идентификация.

Функционированию практически любого предприятия предполагает наличие на её балансе некоторого количества материальных ценностей, которые должны быть учтены, что напрямую влияет на ее бесперебойную работу. Процесс учёта материальных ценностей предполагает проведение ряда процедур, таких как постановка на учёт, эксплуатация, снятие с учёта, списание, а также составление различной отчетной документации. Проведение процедуры учёта помогает избегать нерационального использования материальных ценностей, а также проводить своевременную утилизацию материальных запасов. Автоматизированный учёт материальных ценностей упрощается проведение инвентаризации и различных проверок [1].

Внедрение автоматизированной системы учёта материальных ценностей позволяет сократить время, затрачиваемое на ведения учета материальных ценностей, уменьшить количество ошибок, вызванных человеческим фактором, повысить достоверность информации о материальных запасах, а также своевременно актуализировать информацию об их передвижении и местонахождении, уменьшить трудозатраты на ведение учета, обеспечить достоверной и эффективной информацией о проведении технического обслуживания, ремонтных работ и утилизации материальных объектов.

Одной из наиболее востребованной сферой применение подобных систем является сфера образования, так как в образовательном процессе используется большое количество различных материальных ценностей, как непосредственно в образовательном процессе, так и во вспомогательных процессах. Внедрение автоматизированной системы учета материальных ценностей в образовательном учреждении позволит решить следующие проблемы:

– повысить эффективность и достоверности процедуры учета материальных ценностей;

– снизить вероятность ошибок, вызванных «человеческим фактором»;

– сократить трудозатраты и временны*е* издержки по учету материальных средств;

– снизить вероятность воровства и несанкционированного использования материальных средств;

– улучшить контроль местонахождения, перемещения и использования материальных ценностей;

– обеспечить достоверную информацию о проведении технического обслуживания и сроках утилизации материальных ценностей;

– оперативную фиксацию материальных ценностей за материально ответственным лицом;

Исходя из вышеизложенного, можно сделать вывод о том, что внедрение автоматизированной системы учёта материальных ценностей является достаточно актуальной задачей, особенно в свете формирования единого информационного пространства предприятия. В настоящей статье рассматривается автоматизированная система учета материальных ценностей университета в рамках одной учебной кафедры. Основными требованиями к разрабатываемой информационной системе являются следующие:

– возможность внесения, редактирования и удаления информации о материальных ценностях;

– авторизованное подтверждение корректности введенного в систему информации о материальных ценностях (анализируются корректность заполнения различных полей в системе);

– контроль выполнения обязательств по ценностям и изменения статуса ценностей (необходимо техническое обслуживание, утилизация);

– возможность проведения интересующей выборки;

– возможность сортировки и поиска материальных ценностей;

Важной функцией системы является манипулирование данными о материальных ценностях. Основная задача заключается в разработке простого и понятного для пользователя, не имеющего специальной подготовки, веб-интерфейса. Система должна выполнять ряд необходимых функций, таких как создание новой записи об объекте, ее редактирование и удаление [2].

При работе с основными функциями внесения, редактирования и удаления данных должна быть выполнена их проверка на корректность введенной информации. Следует включить в систему проведение проверки на корректность заполнения полей в записи о материальных ценностях [3].

Также необходимо учесть привязку объектов к месту (кабинетам). Важно чтобы материальные ценности были закреплены за определенным местом, в данном случае рассматриваются кабинеты кафедры, ответственным лицом. Каждый объект должен иметь уникальный идентификатор, под которым он будет значиться в базе данных автоматизированной системы.

Каждый из объектов должен иметь дату поступления в эксплуатацию, дату окончания реализации, дату проведения необходимого технического обслуживания. Следует учесть в системе оповещение пользователя о наступлении времени проведения определенных действий с материаль-

ными объектами, например, о необходимости вывода материальной ценности из эксплуатации.

С точки зрения контроля за надлежащим исполнением ролей в системе необходимым условием является организация многоуровневого доступа к автоматизированной системе учета материальных ценностей. Важно соблюдение разграничений в отношении доступа к материальным ценностям. Администратор в автоматизированной системе учета материальных ценностей должен иметь доступ ко всей информации, хранящейся в базе данных, а также ко все возможностям самой системы. Материально ответственные лицам должен быть предоставлен доступ лишь к тому имуществу, над которым они несут ответственность. Также важно учитывать срок действия полномочий лиц, имеющих доступ к системе, по истечении которого необходимо ограничивать их права доступа [4].

Для удобства пользования автоматизированной системой учета материальных ценностей пользователю должна быть предоставлена возможность поиска и сортировки доступных объектов. Также должно быть реализовано проведение интересующей пользователя выборки, для упрощения работы с системой.

Список используемых источников

1. Баронов В. В. Автоматизация управления предприятия. М.: Инфо-М, 2010. 239с.

2. Буч Г. Объектно-ориентированное проектирование с примерами применения. М. : Радио и связь, 2012. 149 с.

3. Гагарина Л. Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. М. : ИД «ФОРУМ»: ИНФРА-М, 2013. 384 с.: ил.

4. Фридлянд А. Я. Информатика: процессы, системы, ресурсы. М. : Бином. Лаборатория знаний, 2003. 232 с., илл.

УДК 336.717

ПЕРСПЕКТИВЫ РАЗВИТИЯ ПС «МИР»

К. В. Белоус, В. А. Иванова, Т. Д. Куликова, Е. А. Пиликина

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

В настоящей статье рассмотрена первая российская национальная платежная система «Мир», предоставляющая различные услуги по переводу денежных средств. Приведены понятие, структура, основные характеристики и определены причины соз-

дания данной платежной системы. Выделены преимущества и недостатки, отображены перспективы ее развития.

платежная система, карта «Мир», НСПК.

Идея создать отечественную платежную систему появилась после того, как международные сервисы Visa и MasterCard перестали обслуживать ряд российских банков, таких как «Россия», «СМП Банк», «Собинбанк», «Инвесткапиталбанк», попавших под санкции, которые США ввело в ответ на ратификацию ГосДумой соглашения по присоединению Крыма [1].

23 июля 2014 г. было основано акционерное общество «Национальная система платёжных карт» (АО «НСПК») [2], основными задачами которого являлись:

1) Организация операционного и платежного клирингового центра для банковского обслуживания карт международных платежных систем внутри России (С 1 апреля 2015 г. платежи внутри России по всем пластиковым картам, включая Visa и MasterCard, проходят через НСПК – оператора платёжной системы «Мир»).

2) Выпуск и обеспечение развития платежной карты «Мир» (В июне 2017 г. эмиссия карты «Мир» перешагнула порог в 10 млн штук) [3].

После создания НСПК в 2015 г. черный список Visa и Mastercard пополнили еще ряд банков: «Генбанк», банк «Верхневолжский», «Севастопольский морской банк», которые работают в Крыму, а также «Инресбанк» и «Мособлбанк». Некоторые операции по картам Visa и Mastercard были приостановлены. Следуя из этого можно сказать, что организация отечественной платежной системы было верным выходом из сложившейся ситуации [4].

Нормативный документ о принятии платежной системы «Положение о платежной системе Банка России» (утв. Банком России 06.07.2017 N 595-П) с внесенными изменениями вступит в силу 02.07.2018.

Учредителем АО «НСПК» является Банк России (ему принадлежат 100 % акций).

Правилами платежной системы предусматривается прямое и косвенное участие (рис. 1).

В федеральном законе от 27.06.2011 №161-ФЗ «О национальной платежной системе» определен список участников платежной системы, представленный на рис. 2.

В марте 2014 г. было принято решение о создании национальной платежной системы, оператором которой выступило АО «НСПК» [2].

Платежная система «Мир» предусматривает широкий набор услуг, в рамках которого каждый клиент может оформить карту нужного типа, представленную в таблице.

Рис. 1. Участие в платежной системе

Рис. 2. Участники платежной системы

ТАБЛИЦА. Виды карт платежной системы «Мир»

Вид карты	Предоставляемые услуги
Дебетовая карта	позволяют осуществлять операции в режиме онлайн, а также возможен выпуск обезличенных карт
Классическая карта	предоставляет полный набор услуг в торговых точках и в интернете
Премиальная карта	включает разные виды бонусов, оказание персональной поддержки, кешбэк и бесплатное СМС-информирование

Например, Связь-банк начал выпускать следующие виды карт, представленные на рис. 3.

– Дебетовые карты «МИР»;
– Классические дебетовые карты «МИР»;
– Премиальные дебетовые карты «МИР».

Рис. 3. Карты «Мир» от Связь-банка

Для осуществления платежей за границей были разработаны кобейджинговые программы в сотрудничестве с международными платежными системами, позволяющие в России использовать как карту ПС «Мир», а в других странах как карту ПС Maestro, JCB или UnionPay (рис. 4).

Рис. 4. Пример кобейджинговых карт

На данный момент выпускаются карты «Мир»-Maestro, «Мир»-JCB и «Мир»-UnionPay. Достигнута договоренность с платежной системой AmericanExpress по выпуску кобейджинговых карт «Мир»-AMEX

и cArmenianCard – «Мир»-ArCa, а также подписан меморандум между АО «НСПК» и вьетнамской платежной системой BanknetVN. Первая кобейджинговая карта «Мир»-Maestro была выпущена в декабре 2015 г. [2].

Первыми банками, присоединившимися к платежной системе «Мир», являются Газпромбанк, МДМ Банк, Московский Индустриальный банк, РНКБ, Банк «Россия», Связь-Банк и СМП Банк [2]. По официальным данным на февраль 2018 г. выпускают карту 147 банков, а обслуживают 367 [5].

Карта «Мир» содержит фирменные элементы, обеспечивающие безопасность использования, такие как:

– чип золотого или серебряного цвета;

– символ рубля, видимый в ультрафиолетовом свете;

– голограмма «Мир» с изображением глобуса;

– в первых восьми цифрах номера карты содержится информация о платежной системе и о банке-участнике, выпустившем карту.

К преимуществам карты «Мир» можно отнести:

– увеличенный лимит на снятие денежных средств. В сутки со счета можно снять до 150 тыс. рублей без комиссии (с комиссией – до 1,5 млн рублей) [6, 7];

– независимость от политической обстановки и других внешних факторов;

– высокая система защиты при онлайн расчетах обеспечивающаяся системой MirAccept, основанной на базе технологии 3-D Secure.

К недостаткам системы можно отнести:

– для реализации национального проекта по созданию и развитию национальной системы платежных карт на территории Российской Федерации, на карты «Мир» будут перечисляться зарплаты работников бюджетной сферы, пенсии, пособия и прочие социальные выплат;

– ограниченное количество пунктов приема платежных карт;

– отсутствие бесконтактной технологии оплаты карт у ведущих банков России;

– меньшее количество предлагаемых услуг по сравнению с международными картами при одинаковой стоимости годового обслуживания;

– для держателей премиальных карт отсутствуют услуги консьержа и страхование.

На первый взгляд может показаться, что у ПС «Мир» недостатков больше, чем преимуществ. Однако в настоящее время вводятся корректировки по работе системы, внедряются новые сервисы:

1. Количество пунктов приема и обслуживания карт на территории РФ постоянно растет.

2. Планируется выпуск кобейджинговых карт с платежными системами American Express, ArmenianCard, BanknetVN [2].

3. Осуществляется бесплатный выпуск и обслуживание карт «Мир», предназначенных для начисления социальных выплат.

4. Запущена пилотная версия программы лояльности, которая позволяет получать кэшбек (возврат части стоимости покупки) обратно на карту [8].

5. Ведутся работы над приложением, с помощью которого держатели карт «Мир» смогут получить электронный доступ к медицинским услугам, например, записаться к врачу или совершить покупку лекарственных препаратов [9].

В заключении необходимо отметить, что создание и развитие эффективно функционирующей национальной платежной системы, с помощью которой национальная валюта используется как средство платежа, обеспечивает при этом реализацию независимой денежно-кредитной политики России.

Список используемых источников

1. MasterCard приостановила обслуживание карт банка «Россия», Собинбанка, «СМП банка» и Инвесткапиталбанка. – 2014 [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/news/2014/04/29/mastercard-priostanovila-obsluzhivanie-kart-banka-rossiya (дата обращения 08.01.2018).

2. О платежной системе «Мир». – 2017 [Электронный ресурс]. Режим доступа: http://mironline.ru/history/ (дата обращения 08.01.2018).

3. О компании. – 2018 [Электронный ресурс]. Режим доступа: http://www.nspk.ru/about/ (дата обращения 12.01.2018).

4. Еремина А. Visa и MasterCard отключили очередную порцию российских банков. – 2015 [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/articles/2015/12/24/622355-otklyuchili-obsluzhivaniya-bankov (дата обращения 24.01.2018).

5. Выпускают и обслуживают карту. – 2017 [Электронный ресурс]. Режим доступа: http://mironline.ru/partners/#allbanks (дата обращения 21.01.2018).

6. 10 преимуществ карты «Мир». – 2017 [Электронный ресурс]. Режим доступа: http://www.nspk.ru/about/press/about_us/10-preimushchestv-karty-mir/ (дата обращения 21.01.2018).

7. 10 преимуществ карты «Мир». – 2017 [Электронный ресурс]. Режим доступа: https://cityreporter.ru/author/cityreporter/ (дата обращения 21.01.2018).

8. Алексеевских А., Тегин М. Граждане смогут записаться к врачу по картам «Мир». – 2018 [Электронный ресурс]. Режим доступа: https://iz.ru/706067/anastasiia-alekseevskikh-mikhail-tegin/grazhdane-smogut-zapisatsia-k-vrachu-po-kartam-mir (дата обращения 12.02.2018).

9. Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения 08.01.2018).

УДК 004.434

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ СРЕД ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

П. В. Белошеева, В. Л. Литвинов

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

Имитационное моделирование позволяет получать наглядную картину поведения системы, рассматривать различные варианты модели, отвечающие различным сторонам функционирования системы и возможным структурным преобразованиям, получать значения необходимых количественных характеристик. Поэтому имитационное моделирование в настоящее время получает все большее распространение в исследовании сложных технических систем и технологических процессов, в том числе и инфокоммуникационных сетей.

имитационное моделирование, GPSS, AnyLogic.

Во многих задачах практики непосредственное изучение объектов (технических систем или технологических процессов) затруднено из-за сложности объекта, высокой стоимости или длительности исследования, отсутствия объекта (на этапе разработки объект еще отсутствует в природе), сложности задания необходимых условий функционирования объекта (например, определение характеристик процессов перевозок в чрезвычайных ситуациях) и других причин. В таких случаях для изучения объектов используется моделирование – метод научного исследования, заключающийся в замене исходного объекта его моделью, изучением модели и обобщением полученных при анализе характеристик на сам объект [1].

В случае, когда процессы в изучаемой системе столь сложны и многообразны, что аналитические модели становятся слишком грубым приближением к действительности, возможным выходом является имитационное моделирование.

Имитационный подход применяют, когда параметров много, зависимости нелинейны, система имеет качественно различные состояния (непрерывные процессы прерываются дискретными переходами), траекторию во времени (объект эволюционирует), обладает вероятностным поведением и обратными связями. Имитационный подход незаменим, когда нужно сопроводить модель анимационной презентацией (симуляцией).

Имитационное моделирование (ИМ) на ЭВМ позволяет получать наглядную картину поведения системы, рассматривать различные варианты

модели, отвечающие различным сторонам функционирования системы и возможным структурным преобразованиям, получать значения необходимых количественных характеристик. Поэтому имитационное моделирование в настоящее время получает все большее распространение в исследовании сложных технических систем и технологических процессов, в том числе и инфокоммуникационных сетей.

Целесообразность применения имитационного моделирования становится очевидной при наличии следующих условий:

– не существует законченной математической постановки задачи либо еще не разработаны аналитические методы решения сформулированной задачи;

– аналитические методы имеются, но математические процедуры столь сложны и трудоемки, а имитационное моделирование дает более простой способ решения задачи;

– кроме оценки определенных параметров, требуется осуществить наблюдение за ходом процесса функционирования системы в течение некоторого времени. При этом имитационное моделирование дает возможность полностью контролировать время изучения системы, поскольку явление может быть замедлено или ускорено по желанию;

– необходимо использование ИМ в качестве тренажера при подготовке специалистов. При этом ИМ может применяться для приобретения новых навыков в управлении системой и освоения правил принятия решений.

Несмотря на широту понятия «имитационное моделирование», существует определенная специализация его задач. В связи с этим выделяют следующие направления этого метода и наиболее соответствующее им программное обеспечение:

– моделирование динамических систем (MATLAB, Vis-Sim, Lab View, Easy5);

– дискретно-событийное моделирование (GPSS, SYMULA, Arena, AutoMod, Enterprise Dynamics, FlexSim);

– агентное моделирование (Net Logo, Swarm, Repast, ASCAPE);

– системная динамика (VenSim, PowerSim, iSink).

Перечисленные программные пакеты обладают как несомненными достоинствами, так и имеют свои недостатки, к которым относятся – узкая направленность, нелокализованный интерфейс, привязка моделей к среде разработки (не автономность) и дороговизна (MATLAB). Следствие этого – формирование непредставительных сообществ разработчиков.

При ИМ дискретных процессов в современной практике в качестве инструментального средства получила широкое распространение система общецелевого назначения GPSS World, являющаяся последним современным представителем семейства языков моделирования GPSS.

В последние годы наряду с ней применяется система моделирования AnyLogic которая обладает рядом преимуществ, главное из которых – возможность реализации всех направлений имитационного моделирования в одной модели. Это комплексный инструмент, охватывающий в одной модели основные в настоящее время направления моделирования: дискретно-событийное, системной динамики, агентное. Многоподходность не характерна для существующих систем моделирования. Агентные модели не позволяет создавать ни одна из известных систем моделирования, в том числе и GPSS World.

Пакет AnyLogic – отечественный профессиональный инструмент нового поколения, который предназначен для разработки и исследования имитационных моделей [2, 3].

AnyLogic был разработан на основе новых идей в области информационных технологий, теории параллельных взаимодействующих процессов и теории гибридных систем. Благодаря этим идеям чрезвычайно упрощается построение сложных имитационных моделей, имеется возможность использования одного инструмента при изучении различных стилей моделирования. Программный инструмент AnyLogic основан на объектно-ориентированной концепции. Другой базовой концепцией является представление модели как набора взаимодействующих, параллельно функционирующих активностей. Активный объект в AnyLogic – это объект со своим собственным функционированием, взаимодействующий с окружением. Он может включать в себя любое количество экземпляров других активных объектов. Графическая среда моделирования поддерживает проектирование, разработку, документирование модели, выполнение компьютерных экспериментов, оптимизацию параметров относительно некоторого критерия. При разработке модели можно использовать элементы визуальной графики: диаграммы состояний (стейтчарты), сигналы, события (таймеры), порты и т. д.; синхронное и асинхронное планирование событий; библиотеки активных объектов.

При разработке модели на AnyLogic можно использовать концепции и средства из нескольких классических областей имитационного моделирования: динамических систем, дискретно-событийного моделирования, системной динамики, агентного моделирования. Кроме того, AnyLogic позволяет интегрировать различные подходы с целью получить более полную картину взаимодействия сложных процессов различной природы.

AnyLogic используется для разработки имитационных исполняемых моделей и последующего их прогона для анализа. Разработка модели выполняется в графическом редакторе AnyLogic (см. рис. ниже) с использованием многочисленных средств поддержки, упрощающих работу.

Построенная модель затем компилируется встроенным компилятором AnyLogic и запускается на выполнение. В процессе выполнения модели

пользователь может наблюдать ее поведение, изменять параметры модели, выводить результаты моделирования в различных формах и выполнять разного рода компьютерные эксперименты с моделью. Для реализации специальных вычислений и описания логики поведения объектов AnyLogic позволяет использовать мощный современный язык Java.

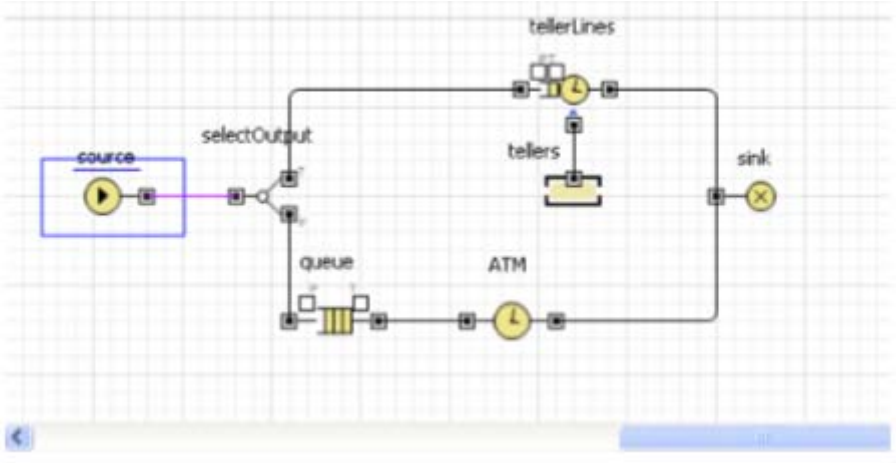


Рисунок. Модель системы в AnyLogic

Важными ограничениями имитационного моделирования является то, что:

– оно не предоставляет непосредственного решения математических задач, что характерно для аналитических методов. Оно служит в качестве средства для анализа поведения системы в условиях, которые определяются экспериментатором;

– разработка хорошей ИМ часто обходится дороже создания аналитической модели и требует наличия квалифицированных специалистов и больших затрат времени;

– при использовании ИМ применяются многочисленные методы статистического анализа данных, что усложняет исследование.

Преодоление перечисленных выше ограничений лежит на пути создания программно-технологического инструментария, позволяющего автоматизировать этапы построения инфокоммуникационных систем и тем самым ускорить сроки их исследования.

Список используемых источников

1. Куприяшкин А. Г. Основы моделирования систем : учеб. пособие; Норильский индустр. ин-т. Норильск: НИИ, 2015. 135 с.

2. Карпов Ю. Имитационное моделирование систем. Введение в моделирование AnyLogic 5. СПб. : БХВ–Петербург, 2005. 400 с.

3. Официальный сайт компании AnyLogic [Электронный ресурс]. Режим доступа: www.anylogic.ru.

УДК 004.5

АНАЛИЗ БИБЛИОТЕК ЭЛЕМЕНТОВ ИНТЕРФЕЙСА ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX

Г. С. Боголепов, В. И. Краснов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В данной работе рассмотрены причины, требующие обсуждения данной темы, дана краткая справка о двух широко используемых библиотеках элементов интерфейса, дано их сравнительное описание и рекомендации по использованию их в разработке для операционной системы Astra Linux.

astra linux, графический интерфейс пользователя, GTK+, Qt, фреймворк, анализ.

В январе 2018 г. Министерство обороны Российской Федерации сообщило о принципиальном решении о переводе всех компьютеров военного ведомства на российское программное обеспечение. Для реализации данного решения Министерство обороны с 2018 г. получит первые пакеты Astra Linux для тестирования в войсках [1].

Данная операционная система является полностью отечественным решением на базе ядра Linux, создана она была московской компанией «РусБИТех» и имеет две версии: Astra Linux Common Edition – операционная система, разработанная для обычных пользователей – и Astra Linux Special Edition – дистрибутив, предназначенный для использования в автоматизированных системах в защищенном исполнении, обрабатывающих информацию ограниченного распространения, включая государственную тайну до степени секретности «совершенно секретно». В данный момент на компьютерах военного ведомства установлены лицензионные продукты Microsoft. Ранее Astra Linux стала единой операционной системой для военных автоматизированных систем управления. Для рабочих компьютеров Минобороны выбрало расширенный ее вариант – Astra Linux Special Edition со встроенным офисным пакетом. На следующем этапе новая ОС будет загружена на специальные служебные смартфоны и планшеты [2].

В связи с данным решением стоит вопрос о портировании (переносе) специфичного для военных программного обеспечения, разработанного для ОС Windows под ОС AstraLinux. Большинство из них написано с использованием графического интерфейса пользователя, а это предполагает использования различных библиотек пользовательских элементов.

В операционных системах Linux используются следующие библиотеки пользовательских элементов. В их число входит: GTK+, Qt, EFL, SDL,

wxWidgets. В настоящее время также используются платформы, позволяющие разрабатывать программное обеспечение на основе web-технологии. Они предоставляют большую гибкость при разработке, но используют больше ресурсов операционной системы. К технологиям данного вида можно отнести платформу Electron.

Исходя из рейтингов операционных систем и непосредственно графической составляющей Astra Linux, которая используется в ней, было решено рассмотреть две графических библиотеки для реализации графического интерфейса пользователя: GTK+ и Qt и проанализировать их.

GTK+ (сокращение от GIMP ToolKit) – кроссплатформенная библиотека элементов интерфейса (фреймворк), имеет простой в использовании API, является одной на сегодняшний день библиотек для X Window System [3].

Будучи изначально частью графического редактора GIMP, она развилась в отдельный проект и приобрела заметную популярность. GTK+ является официальной библиотекой для создания графического интерфейса проекта GNU. Текущая актуальная версия данной библиотеки – 3.22 (рис. 1).

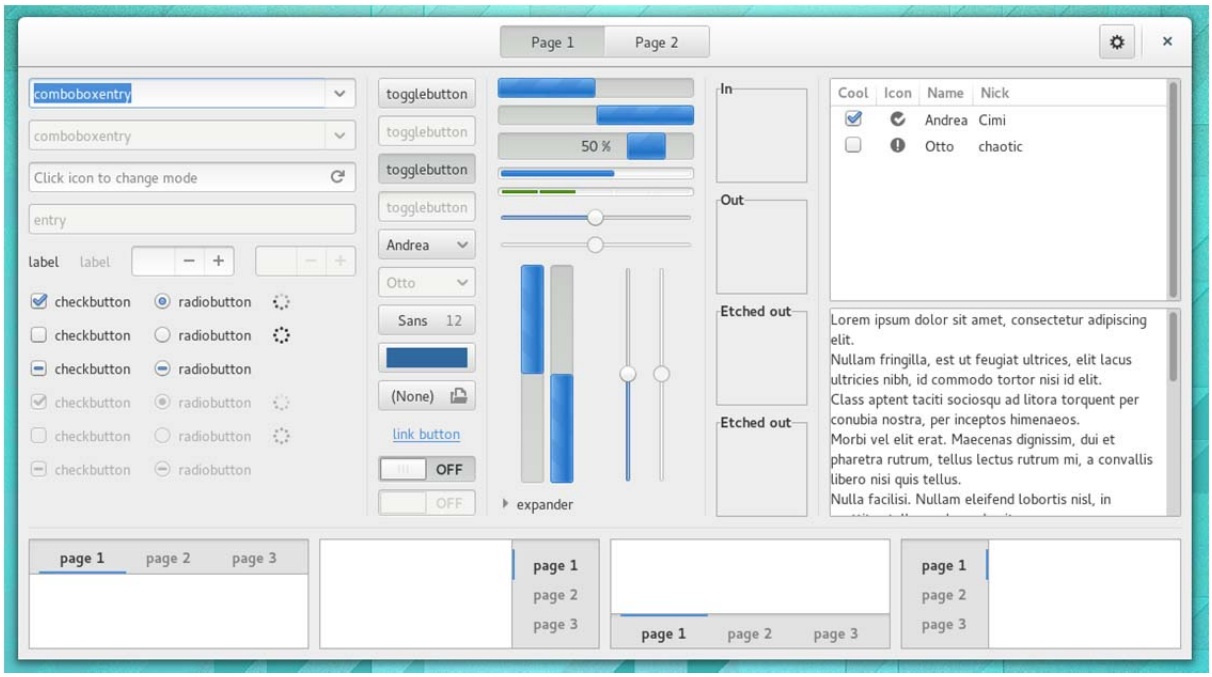


Рис. 1. Элементы библиотеки GTK+

Qt (произносится [ˈkjuːt] (кьют) как “*cute*” или неофициально Q-T (кью-ти)) – кроссплатформенный фреймворк для разработки программного обеспечения на языке программирования C++. Текущая версия – 5.10 [4].

Перейдем к непосредственному анализу данных библиотек. GTK+ написана на языке C, а Qt написана на C++, поэтому GTK+ быстрее работает, но читать код проще у Qt. К тому же у Qt имеется отдельный препроцессор для исходного кода (*meta object compilator*), поэтому на нем можно писать и внедрять более высокоуровневый код с использованием абстракций, не свойственных чистым языкам, на которых они написаны.

Обе библиотеки имеют оболочки (так называемые биндинги) под различные языки программирования – это позволяет разрабатывать программное обеспечение без привязки к какому-либо языку. Данное свойство библиотек осуществлять быстрое прототипирование на интерпретируемых языках и реализовывать сами продукты на компилируемых языках.

Обе библиотеки имеют редактирование интерфейса с использованием CSS подобных стилей. Но у Qt имеется Qt Quick – технология создания UI, особенностью которой является разделение декларативного описания дизайна интерфейса и императивной логики программирования (рис. 2). Данная технология позволяет описывать графический интерфейс на CSS-подобном языке, что является стандартом де-факто в web-программировании. Это позволяет реализовывать графическую часть на более понятном языке (QML), который исключает код на C++ и позволяет избежать нагромождения кода.

Рис. 2. Реализация интерфейса «умного дома» на базе библиотеки Qt

У GTK+ слишком разрозненная система. Его стек состоит из порядка 40 библиотек. У Qt всё объединено в единое монолитное ядро, к которому

подключаются требуемые модули (JSON, XML и т. д.). Поэтому инфраструктура Qt выглядит единообразной и интуитивной.

Главным преимуществом Qt является наличие среды разработки, работающий по принципу wysiwyg (*what you see is what you get* – что видишь, то и получишь). Это дает возможность проектировать интерфейс пользовательского приложения непосредственно в интегрированной среде разработки, и видеть уже готовый интерфейс пользователя. Также экономится время разработки программного обеспечения за счёт генерации верстки форм программы в формате XML и последующей их генерацией в код C++. В GTK+ такая программа отсутствует, поэтому положение всех элементов необходимо просчитывать, потом реализовать схему интерфейса в коде, что занимает достаточное количество времени.

Исходя из вышеперечисленных особенностей, рекомендуется в качестве библиотеки графического интерфейса пользователя выбирать Qt, потому что:

– написан на C++, что делает код на нем гибким, лаконичным и легкочитаемым;

– имеет прослойки для множества популярных языков, таких как Python, Java, Ruby, PHP;

– удобный инструментарий и возможности раздельного редактирования логики приложений и графического интерфейса пользователя;

Список использованных источников

1. Круглов А., Рамм А. Военные сказали Windows «прощай» [Электронный ресурс] // Известия. 09.01.2018. URL: https://iz.ru/688478/aleksandr-kruglov-alekseiramm/voennye-skazali-windows-proshchai (дата обращения 12.01.2018).

2. URL: http://astra-linux.ru/products/alse.html (дата обращения 12.01.2018).

3. Qt [Электронный ресурс] // Википедия. URL: https://ru.wikipedia.org/wiki/Qt (дата обращения 13.01.2018).

4. GTK+ Qt [Электронный ресурс] // Википедия. URL: https://ru.wikipedia.org/wiki/GTK%2B (дата обращения 13.01.2018).

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Саенко.

УДК 65.011.56

ИСПОЛЬЗОВАНИЕ ПРОСТРАНСТВЕННЫХ ДАННЫХ ОБ ОСНОВНЫХ СРЕДСТВАХ ПРЕДПРИЯТИЯ СВЯЗИ В АВТОМАТИЗИРОВАННОМ УЧЕТЕ ДРАГОЦЕННЫХ МЕТАЛЛОВ

В. В. Ботяков, А. В. Шестаков

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

Рассматриваются вопросы существующего порядка и организации регламентированного автоматизированного учета драгоценных металлов в основных средствах предприятия, организации связи. Применительно к сложившимся объективным условиям перехода к цифровой экономике страны выработаны организационные и организационно-технические предложения по вводу, обработке и поддержанию в актуальном состоянии пространственных данных об основных средствах предприятия, содержащих драгоценные металлы, а также по их практической реализуемости при незначительном изменении задействованного в настоящее время ресурса и средств предприятия.

оператор связи, основные средства, драгоценные металлы, радиочастотная метка, радиочастотная идентификация, пространственные данные, автоматизация учета пространственно-временных данных.

Реализация программы «Цифровая экономика Российской Федерации» [1] базируется на информационной инфраструктуре, которая определяется ресурсами предприятий, организаций операторов связи единой сети электросвязи России (далее – Предприятие связи) [2].

Ресурсы Предприятия связи, то есть средства и сооружения связи согласно определениям в [2], либо непосредственно связаны с процессом передачи сообщений (как оборудование и передаточные устройства – в терминах [3]), либо обеспечивают необходимые материальные условия (здания, сооружения, инструменты) для осуществления этого процесса или управления Предприятием и относятся к основным средствам, которые подлежат бухгалтерскому учету.

Порядок и организация бухгалтерского учета основных средств Предприятий связи в Российской Федерации регламентированы правовыми и нормативными документами [3, 4, 5, 6, 7].

Как правило, объемы этих средств значительны, а эксплуатация достаточно длительная. Это подтверждается данными об объемах и установленной к начислению амортизации основных средств, например,

в ПАО «Ростелеком» [8, 9, 10] (табл. 1 и 2), которые не противоречат данным Общероссийского классификатора основных фондов (ОКОФ, в частности ОК 013-2014, СНС 2008) [11].

ТАБЛИЦА 1. Объемы основных средств ПАО «Ростелеком»

По состоянию на 31 декабря	Объем основных средств, млн рублей
2016 года	320,615
2015 года	318,353
2014 года	313,635
2013 года	311,654

ТАБЛИЦА 2.Предполагаемый срок полезного использования основных средств в ПАО «Ростелеком» [10]

Перечень основных средств	Срок полезного использования, лет
Здания и сооружения	10–50
Кабели и передающие устройства:	
Кабель	10–40
Оборудование для радиопередачи и передачи по фиксированным каналам связи	8–20
Телефонные станции	15
Прочее	5–10

Особенностью основных средств Предприятия связи (например, по кодам ОКОФ 330.28.23.23; 320.26.30.11.110; 320.26.30.11.150; 320.26.30.11.190) является наличие в их составе компонент, содержащих драгоценные металлы, таких как золото, платина, серебро и другие. Вместе с тем, законодательно определено, что любое предприятие (организация) обязано документально оформлять поступление, движение, инвентаризацию и выбытие драгоценных металлов, содержащихся в составных частях различных видов техники. Согласно нормам Федерального Закона «О драгоценных металлах и драгоценных камнях» (п. 2 ст. 20) [12] драгоценные металлы и драгоценные камни подлежат обязательному учету по массе и качеству при добыче, производстве, использовании и обращении. Порядок такого учета и отчетности установлен Правительством Российской Федерации, федеральными органами исполнительной власти, регулирующими отчетность (например [13, 14]), а также ведомственными и внутрипроизводственными документами, которые учитывают специфику выпол-

няемых предприятием операций с драгоценными металлами и разработаны на основании положений Инструкции № 231н [14].

Организация учета обусловлена необходимостью получения своевременных и точных сведений о количестве и местонахождении драгметаллов; документальным подтверждением движения драгоценных металлов относительно материально ответственных лиц, структурных подразделений и предприятия в целом; подтверждением достоверности данных в представляемой отчетности.

В настоящее время системы автоматизированного учёта драгметаллов имеют ряд недостатков: низкую информативность и недостаточную актуальность данных о нахождении объектов учёта; ручной способ ввода, изменения и удаления данных об объектах учёта; отсутствие интеграции с другими автоматизированными системами предприятия, которые функционально также ведут учет электронных данных об изделиях.

В ходе проведенного исследования возможных направлений снижения выявленных недостатков рассмотрены существующие подходы и решения по использованию радиочастотных меток и радиочастотной идентификации (RFID) основных средств предприятия связи.

Для упорядочивания информационных потоков из различных источников информации, систематизации и анализа вариантов организационных и технических решений разработана и предложена оригинальная классификация маркировки и радиочастотных меток, которая учитывает частные аспекты классификации объектов в действующих стандартах и нормативно-технических документах (рис. 1 и 2).

Рис. 1. Классификация маркировки

Рис. 2. Классификация радиочастотных меток

Эффективный IT контроль оборота основных средств может стать за счет обязательной маркировки средств при помощи RFID-метки с записью уникального номера и последующим отслеживанием ее перемещения [15].

Системотехнические решения по построению системы IT контроля оборота основных средств, содержащих драгметаллы, включают:

оснащение основных средств RFID-метками;

доразвертывание инфраструктуры Предприятия связи техническими средствами съема информации;

развертывание подсистемы RFID-терминалов;

интеграцию пространственных данных и атрибутов с учетными данными основных средств, содержащих драгметаллы.

Проработанный вариант системотехнических решений представлен на рис. 3.

Внедрение предлагаемых системотехнических решений обеспечит:

учёт основных средств Предприятия связи, содержащих драгметаллы, с пространственным позиционированием их местонахождения;

автоматизацию ввода и выгрузки данных, включая пространственные;

автоматизацию процесса инвентаризации основных средств, содержащих драгметаллы;

ведение и поддержание в актуальном состоянии информационной базы данных об основных средствах, содержащих драгметаллы, с атрибутами их пространственных данных.

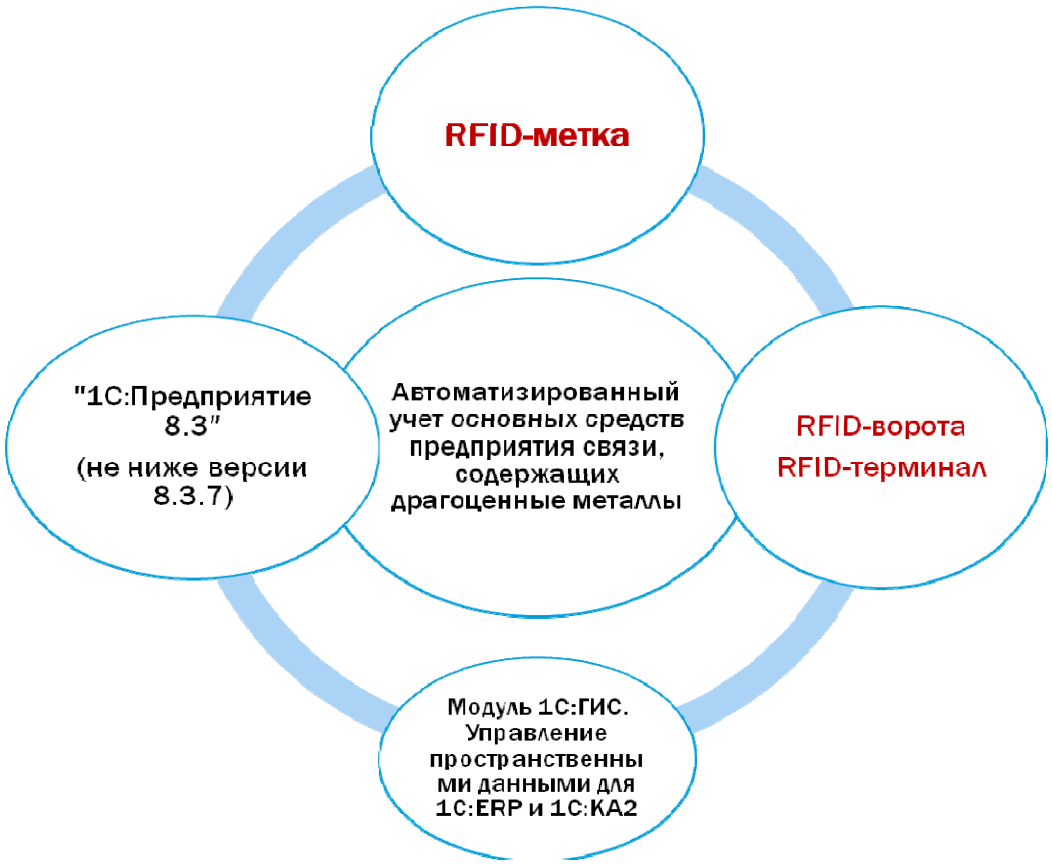


Рис. 3. Системотехнические решения обеспечения учета основных средств

Список используемых источников

1. Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. Режим доступа: http://government.ru/rugovclassifier/ 614/events/ (дата обращения 01.03.2018).

2. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения 01.03.2018).

3. Налоговый кодекс Российской Федерации от 05.08.2000 № 117-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/ document/cons_doc_LAW_28165/ (дата обращения 01.03.2018).

4. Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/ 902360261 (дата обращения 01.03.2018).

5. Приказ Минфина России «Об утверждении Положения по бухгалтерскому учету «Учет основных средств» ПБУ 6/01 от 30.03.2001 № 26н [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/901784528 (дата обращения 01.03.2018).

6. Приказ Минфина РФ «Об утверждении Методических указаний по бухгалтерскому учету основных средств» от 13.10.2003 № 91н [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/901877931 (дата обращения 01.03.2018).

7. Классификация основных средств, включаемых в амортизационные группы [Электронный ресурс] Режим доступа. URL: https://normativ.kontur.ru/document?moduleId= 1&documentId=276705 (дата обращения 01.03.2018).

8. Бухгалтерская (финансовая) отчетность ПАО «Ростелеком» за 2016 год. [Электронный ресурс]. Режим доступа: https://e-ecolog.ru/buh/2016/ 7707049388 (дата обращения 01.03.2018).

9. Бухгалтерская (финансовая) отчетность ПАО «Ростелеком» за 2014 год [Электронный ресурс]. Режим доступа: https://e-ecolog.ru/buh/2014/ 7707049388 (дата обращения 01.03.2018).

10. Пояснения к Консолидированной финансовой отчетности ОАО «Ростелеком» [Электронный ресурс]. Режим доступа: http://www.intercon-intellect.ru/upload/distant/msfo/rostelecom-ias16.pdf (дата обращения 01.03.2018).

11. ОК 013-2014 Общероссийский классификатор основных фондов (ОКОФ). М. : Стандартинформ, 2015.

12. Федеральный Закон «О драгоценных металлах и драгоценных камнях» от 26.03.1998 № 41-ФЗ [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/901704628 (дата обращения 01.03.2018).

13. Правила учета и хранения драгоценных металлов, драгоценных камней и продукции из них, а также ведения соответствующей отчетности, утверждены Постановлением Правительства РФ от 28.09.2000 № 731 [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/901771424 (дата обращения 01.03.2018).

14. Инструкция о порядке учета и хранения драгоценных металлов, драгоценных камней, продукции из них и ведения отчетности при их производстве, использовании и обращении, утверждена Приказом Минфина России от 09.12.2016г. № 231н [Электронный ресурс]. Режим доступа: http://www.garant.ru/ products/ipo/prime/doc/71482774/ (дата обращения 01.03.2018).

15. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

УДК 004.056.57

ЗАЩИТА ОТ КИБЕРАТАК НА ОСНОВЕ НЕСТАЦИОНАРНОСТИ СЕТИ СВЯЗИ

А. А. Бречко

Военная академия связи им. Маршала Советского Союза С. М. Будённого

В статье рассматриваются типовые этапы компьютерных атак на элементы сети связи, в особенности уклон сделан на анализ временных показателей атак, а также динамики изменения сети связи, её состояния и состояния её элементов,

на основе чего предложена база для обоснования критериев защищенности сети связи и её элементов – среднее время квазистационарного состояния сети.

компьютерная атака, защищенность сети связи, критерии защищенности.

Сети связи, её элементы характеризуются значительным числом признаков. Ниже рассматриваются хронологические признаки. Суть их заключается в изменении и динамике изменения состояния сети и её элементов с течением времени под воздействием различных факторов.

Современные сети связи являются ресурсом, который используют множество пользователей, преследующих свои цели, которые могут быть антагонистичными. Этот факт обуславливает существование компьютерных атак [1].

Как правило, любая компьютерная атака состоит из типовых этапов. Это сбор информации, сканирование, реализация атаки (эксплуатация уязвимости) и закрепление в системе [2].

Представленные этапы, как правило, реализуются в отношении отдельного элемента сети. Атака в отношении сети в целом состоит из последовательных атак на её элементы.

Следует отметить, что этапы реализуются последовательно, выполнение следующего этапа невозможно без данных, полученных на предыдущих этапах.

Первый этап – сбор информации об объекте атаки, и он может проводится различными методами. Это самый важный этап. От объема, своевременности и достоверности сведений, собранных на этом этапе, зависит успешность проведения атаки в целом.

На этом этапе производится сбор информации об оборудовании, установленном на объекте, используемых программах и их версиях. Определяется топология сети, используемые в ней протоколы и технологии. Формируется список целевых IP адресов [3].

Следующий этап – сканирование объекта атаки. Он включает в себя сканирование портов и сканирование системы на уязвимости.

Сканирование портов, как правило, проводится автоматизированными средствами. Типовое сканирование портов заключается в попытке установления соединения на сканируемом порте. Причем сканирование только общеизвестных номеров портов может не принести результата, тогда для повышения вероятности успешной атаки сканируются все порты, что занимает определенное время.

Далее, когда найдены открытые порты и определены запущенные на них службы, проводится поиск уязвимостей. Существуют автоматизированные средства поиска уязвимостей, позволяющие найти в системе известные уязвимости. Однако система может не иметь известных уязвимо-

стей, тогда проводится анализ программного кода (поиск ошибок в коде), установленных на объекте атаки программ и служб. Это сложная и нетривиальная задача, которая занимает много времени. Но решив ее, вероятность успешной атаки сильно повышается, поскольку новая уязвимость будет известна только атакующему.

После того, когда найдены уязвимости происходит реализация атаки (эксплуатация уязвимости). Уязвимость позволяет загрузить и выполнить вредоносный код на атакуемой системе. Этот этап также может быть выполнен дистанционно автоматизированными средствами. Такие средства позволяют выбрать вредоносный код, доставить на объект и выполнить его.

Написание оригинального вредоносного кода повышает вероятность успешного проведения атаки в силу того, что системам защиты, основанным на сигнатурном методе детектирования, еще не известен такой код. Это также нетривиальная задача, решение которой может занять много времени.

Общей целью компьютерных атак является получение полного контроля над объектом в привилегированном режиме. Как только это случается, происходит развитие атаки. Полный нелегитимный контроль над элементом сети, или еще хуже над всей сетью, может привести не только к нарушению конфиденциальности, доступности и целостности важной информации, но и нарушить работу объектов, управление которыми, осуществляется с помощью ресурсов этой сети. Страшно представить последствия атаки, например, на сеть управления атомной электростанцией.

Следующий типовой этап – закрепление в системе. Основной целью этого этапа является создание возможности повторно и с меньшими временными затратами получить доступ к системе в случае обнаружения атаки и блокирования действий злоумышленника. На этом этапе искусственно создаются уязвимости, например, открываются новые порты, запускаются службы, меняются конфигурации на небезопасные.

Исходя из вышеописанного следует вывод, что каждый из этапов компьютерной атаки занимает определенное время. Время реализации атаки в отношении сети, помимо всего прочего, характеризуется её топологией и связностью. Поскольку сначала атакуется граничный элемент, а потом связанные с ним, тогда время вскрытия сети, состоящей только из последовательно соединенных элементов, будет складываться из времен вскрытия каждого элемента. Но если сеть полносвязная, то время её вскрытия сложится из времени вскрытия первого элемента и максимального времени вскрытия остальных элементов.

Общеизвестно, что сложные системы, которыми являются сети связи, элементы сетей связи с течением времени изменяются. Изменение местоположения элементов сети в пространстве называется мобильностью.

Это классическое определение и его недостатком является учет лишь местоположения объекта и его перемещение. Сети связи и её элементы имеют множество показателей, которые меняются во времени и это не только географические координаты. Меняется топология, связность, конфигурация оборудования, настройки, устанавливаются обновления безопасности, меняются пароли, ключи и т. д. Такое изменение состояние сети, элементов сети можно назвать мобильностью в широком смысле.

Состояние объекта, когда он похож сам на себя с заданным коэффициентом сходства называется квазистационарным.

Классические критерии защищенности, основанные на мобильности объекта, имеют следующее обоснование: пусть существует некий объект, который изменяет свое местоположение и существует некий субъект, который имеет целью оказать негативное воздействие на объект, причем субъект не знает, месторасположение объекта. Тогда, если время поиска объекта больше периода смены его местоположения, то субъект воздействия оказать не сможет.

По аналогии с вышеописанным, при компьютерной атаке объект атаки будет защищен, в случае, когда злоумышленник на атаку тратит больше времени, чем объект находится в квазистационарном состоянии. Это означает, что реализация атаки, основанная на данных, полученных на предыдущих этапах, будет неэффективна в силу изменения объекта с момента получения сведений о нём, до момента реализации атаки.

Подводя общий итог, среднее время квазистационарного состояния сети или её элементов может быть использовано в качестве признаков или критериев защищенности от компьютерных атак.

Список используемых источников

1. Стародубцев Ю. И., Бегаев А. Н., Давлятова М. А. Управление качеством информационных услуг / Под общ. ред. Ю. И. Стародубцева. СПб. : Изд-во Политехн. ун-та, 2017. 454 с.

2. Коцыняк М. А., Иванов Д. А., Лаута О. С. Модель таргетированной кибернетической атаки // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 90–98.

3. Иванов В. А., Белов А. С., Гречишников Е. В., Стародубцев Ю. И., Ерышов В.Г., Алашеев В. В., Иванов И. В. Способ контроля демаскирующих признаков системы связи. Патент № 2419153 от 30.06.2009 г.

Статья представлена научным руководителем, доктором военных наук, профессором Ю. И. Стародубцевым.

УДК 004.031.42

МНОГОПОТОЧНОСТЬ И ПАРАЛЛЕЛИЗМ В UNIX ПОДОБНЫХ ОС НА ПЛАТФОРМЕ X86

Г. А. Булыгин, Л. П. Козлова

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

В статье рассматривается одна из самых фундаментальных абстракций в UNIX-подобных системах после файла – процесс (главные составляющие процесса, способы параллельного исполнения программ как в рамках одного, так и множества процессов). Именно здесь, в управлении процессами, ярче всего проявляют дальновидность и долговечность первоначальной концепции Unix. В концепции Unix создание нового процесса отделяется от загрузки нового двоичного образа, в большинстве случаев эти действия выполняются совместно, разделение позволяет экспериментировать и открывает широкие возможности для развития каждой задачи. Сделаны выводы о параллелизме на уровне команд процессора, основанного на архитектуре x86.

процесс, поток, x86, UNIX, CISC, RISC, системный вызов, параллелизм.

Разработчики вычислительной техники стремятся к повышению производительности, достижение которой реализуется либо повышением тактовой частоты, который имеет технологические ограничения, либо используют параллелизм (исполнение двух и более операций одновременно).

Компьютеры, поддерживающие параллелизм, возникли как средство для высокопроизводительных научных вычислений и получили широкое распространение. Их можно встретить практически везде: от высоконагруженных серверов до домашних станций пользователей.

Параллелизм существует в виде двух форм: на уровне команд и на уровне процессоров. В первом случае он реализуется за счет выполнения сразу нескольких команд (или их частей) на одном процессоре одновременно. Во втором случае над одним заданием работает одновременно несколько процессоров.

Процессы являются одной из самых фундаментальных абстракций в системах UNIX после файлов. Они больше чем просто код, написанный на ассемблере, владеют данными, ресурсами, имеют состояния и виртуальный процессор.

В UNIX создание нового процесса отделяется от загрузки нового двоичного образа. В то время как большинство операционных систем предлагают один системный вызов для запуска одной программы, в UNIX требуются два: fork и exec. Каждый процесс в любой конкретный момент

времени обозначается уникальным идентификатором (*processID*, *pid*) и, если выполняется ядром в отсутствие всех других процессов, имеет pid равный 0. Первый процесс, который ядро выполняет во время запуска системы, называется процессом инициализации и имеет pid равный 1. Обычно initprocess в Linux является программой инициализации [1].

Процесс, запускающий другой процесс, называется родительским, порождаемый процесс является дочерним. Эти взаимоотношения записаны в каждом идентификаторе родительского процесса (*ppid*), значение которого для дочернего процесса равно значению pid родительского процесса.

Каждый процесс принадлежит определенному пользователю и группе. Эти принадлежности используются для управления правами доступа к ресурсам. С точки зрения ядра пользователь и группа – это просто некие целочисленные величины. Они хранятся в файлах /etc/passwd и /etc/group, с помощью которых сопоставляются с привычными глазу пользователя UNIX именами и тесно связана с понятием задания (*task*).

В UNIX действие загрузки в память и запуска образа программы выполняется отдельно от операции по созданию нового процесса [2]. Один системный вызов загружает бинарную программу в память, замещая текущее содержание адресного пространства, и начинает выполнение новой программы. Это называется выполнением новой программы, а функциональность обеспечивается семейством вызовов exec.

Системный вызов используется для создания нового процесса, который изначально является практически копией своего родительского – fork(). Часто новый процесс немедленно приступает к выполнению новой программы. Акт создания нового процесса называется ветвлением и обеспечивается системным вызовом fork(). Два действия – сначала ветвление для создания нового процесса, а затем exec для открытия нового выполнения этого процесса – требуются для запуска новой программы в новом процессе.

В современных системах UNIX вместо копирования всего объема родительского адресного пространства используются страницы копирования при записи (*copy on write*, COW) [3], откладывающая стратегия оптимизации, разработанная для уменьшения нагрузки из-за дублирования процессов. Принцип прост: если запрашивается доступ для чтения нескольких копий ресурса, нет смысла их дублировать. Вместо этого каждый потребитель может получить указатель к одному и тому же ресурсу. При этом сохраняется иллюзия эксклюзивного доступа к нему, пока пользователи не пытаются изменить свою «копию», и затрат на копирование не требуется. При редактировании копии, ресурс прозрачно дублируется, и она отправляется редактирующему пользователю, который не видя происходящего, может изменять свою копию ресурса, пока другие продолжают просматривать оригинальную, неизмененную версию.

Классический способ прекратить работу программы – не использование явного системного вызова, а простое «достижение конечной точки» программы. Процесс также может завершиться, если ему отправлен сигнал, действие которого по умолчанию – окончание процесса.

При завершении процесса, ядро посылает сигнал SIGCHLD родительскому процессу. По умолчанию этот сигнал игнорируется и родительский процесс не предпринимает каких-либо действий. Однако при необходимости процессы могут обработать данный сигнал с помощью системных вызовов signal() или sigaction(). Сигнал SIGCHLD может быть сгенерирован и отправлен в любое время, так как завершение дочернего процесса не синхронно родительскому. Однако часто предку требуются сведения о завершении его потомка или даже некоторое время для ожидания события.

Когда дочерний процесс завершается прежде родительского, ядро должно поместить потомка в особый процессный статус. Процесс в этом состоянии называется зомби. В данном состоянии существует лишь образ процесса – основные структуры данных, содержащие потенциально нужные сведения. Процесс в таком состоянии ожидает запроса о своем статусе от предка (процедура ожидание процесса-зомби). Только после того как предок получит всю необходимую информацию о завершенном дочернем процессе, последний формально удаляется и перестает существовать даже в статусе зомби.

Ядро LINUX предоставляет несколько интерфейсов для получения информации о завершенном дочернем процессе:

– *pid_t wait* (*int *status*) – возвращает pid завершенного дочернего процесса или -1 в случае ошибки.;

– *pid_t waitpid* (*pid_t pid*, *int *status*, *int options*) – ожидание определенного процесса дополнительные параметры позволяют настроить его более тонко;

– *int waitid* (*idtype_tid type*, *id_t id*, *siginfo_t *infop*, *int options*) – как и wait() и waitpid(), системный вызов waitid() используется для ожидания и получения информации об измененном статусе (завершение, остановка, продолжение) дочернего процесса.

Процессы принадлежат определенным пользователям и группам. Идентификаторы группы и процесса – численные величины, представленные типами C uid_t и gid_t соответственно.

В системе LINUX идентификаторы пользователя и группы какого-либо процесса определяют операции, доступные для выполнения данным процессом, которые исполняются от имени определенных пользователей и групп. Много процессов может быть запущено только от имени пользователя root. Однако при разработке программного обеспечения лучше все-

го следовать доктрине наименьших прав, что означает: процесс должен работать с минимальным из возможных уровней прав.

Идентификаторы пользователя или группы устанавливаются с помощью двух системных вызовов:

– *int setuid* (*uid_t uid*) – устанавливает действительный идентификатор пользователя текущего процесса;

– *int setgid* (*gid_t gid*) – устанавливает действительный идентификатор группы текущего процесса.

Каждый процесс является членом группы процессов, которая представляет собой коллекцию из одного или нескольких процессов, связанных друг с другом с целью управления заданиями.

При первичном входе в систему, процесс авторизации создает новую сессию, которая содержит единственный процесс – оболочку авторизации пользователя.

Основная сложность при проектировании программ, работающих с использованием распараллеленных алгоритмов – обеспечить правильную последовательность взаимодействий между различными вычислительными процессами, а также координацию ресурсов, разделяемых между процессами.

Многопоточность имеет большие преимущества: увеличение скорости использование общих ресурсов – общую память и файлы, экономия памяти, времени; повышение производительности процесса

Многопоточность и параллелизм – современные направления программирования, особенно актуальные в настоящее время, в период широкого использования многоядерных гибридных и многопроцессорных систем. Именно многопоточность и параллелизм программ, основанные на многоядерности процессора, дают возможность почувствовать реальные преимущества параллельного выполнения.

Список используемых источников

1. Лав Р. Linux. Системное программирование. СПб. : Питер, 2008. 416 с.

2. Дунаев С. Б. UNIX System V. Release 4.2: общ. руководство. М. : Диалог-МИФИ, 1995. 287 с

3. Дунаев С. Б. UNIX-сервер. Настройка, конфигурирование, работа в операционной среде, Internet-возможности. В 2 т. Т. 2. Системное администрирование UNIX и настройка основных сетевых служб. М. : Диалог-МИФИ, 1999. 304 с.

4. Немет, Эви, Снайдер, Гарт, Хейн, Трент, Уэйли, Бэн. Unix и Linux: руководство системного администратора, 4-е изд. : пер. с англ. М. : Вильямс, 2012. 1312 с

УДК 621.37

МЕТОД ПРОЕКТИРОВАНИЯ ТРАКТА ПЕРВИЧНОЙ ОБРАБОТКИ СИГНАЛА НА ОСНОВЕ ЛИНЕЙНЫХ ИМПУЛЬСНЫХ СИСТЕМ

А. В. Ваганов, Н. Н. Кочмарик

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

В данной статье рассматривается метод проектирования тракта первичной обработки сигнала от измерительных преобразователей в АСУ на основе интегральных линейных импульсных систем. Предложена математическая модель тракта при условии соотношения частот тактирования ЛИС и верхней границы полезного сигнала не менее ста. Произведено моделирование фрагмента тракта первичной обработки сигнала в специализированном САПР.

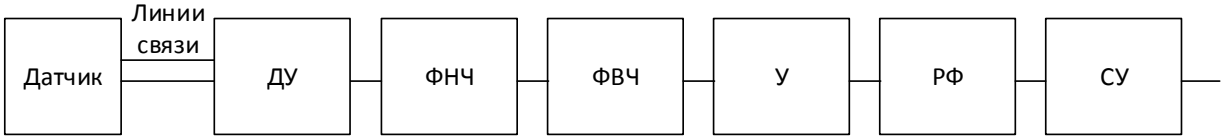
обработка сигнала, тракт, линейные импульсные системы, помеха.

Автоматизация системы управления производством призвана повысить эффективность и расширить функциональные возможности производства, сократить затраты и время выпуска различной продукции и товаров.

Автоматизированные системы управления технологическим процессом (АСУ ТП) способствуют повышению производительности и качества труда сотрудников, улучшению контроля за ходом процесса производства, повышению эффективности учёта и отчётности, оперативности и обоснованности принятия решений по управлению различными процессами.

Неотъемлемой частью любой АСУ ТП является тракт первичной (предварительной) обработки сигнала (ТПОС). В его задачи входит передача информации от различных измерительных преобразователей (датчиков) по линиям связи, коммутация этих линий, выделение полезного сигнала на фоне различных помех, его усиление, а также согласование данного тракта по уровню выходного сигнала с аналого-цифровым преобразователем (АЦП) АСУ. Современные АСУ используют большое количество различных видов датчиков. Наиболее современными из них являются интегральные датчики с цифровым выходом. Такие преобразователи позволяют упростить процесс их стыковки с остальной частью АСУ. Однако наряду с цифровыми измерительными преобразователями в некоторых случаях применяют аналоговые датчики.

Типовая структурная схема тракта для работы с аналоговыми измерительными преобразователями представлена на рис. 1.



ДУ-дифференциальный усилитель
ФНЧ-фильтр низких частот
ФВЧ-фильтр высоких частот
У- усилитель
РФ-режекторный фильтр
СУ-согласующий усилитель

Рис. 1. Структурная схема ТПОС

Как было сказано ранее, в АСУ ТП датчик может находится на значительном расстоянии от системы обработки сигнала, поэтому для передачи сигнала используют двухпроводную линию связи, предполагающую передачу парафазного (сдвинутого на 180^0) сигнала от датчика. Такое решение минимизирует влияние различных электрических помех. Кроме случайных помех полезный сигнал, предаваемый по данной линии, может содержать постоянную составляющую, являющуюся статической помехой.

Таким образом входной тракт ТПОС должен обеспечивать подавление синфазной помехи, то есть иметь дифференциальный вход. А последующие его блоки должны обеспечивать необходимую фильтрацию помех, выделяя рабочую полосу частот. Для подавления наиболее интенсивной составляющей помехи, например, электрической сети, используют режекторный фильтр с частотой среза 50 Гц. Для согласования уровней сигнала ТПОС и АЦП АСУ необходимо применение усилителей.

Тракт предварительной обработки сигнала возможно реализовать с применением как аналоговой, так и на цифровой элементной базы. В данной статье рассматривается возможность реализации ТПОС на базе импульсной схемотехнике, т. к. она сочетает плюсы аналоговой схемотехники и лишена недостатков цифровой. Её использование не требует сложных алгоритмов и минимизирует затраты ресурсов на обработку сигнала.

Если частота тактирования линейных импульсных систем (ЛИС) превышает верхнюю границу частоты полезного сигнала, то описание процесса преобразования этого сигнала в ТПОС удобно проводить на основе математического аппарата для линейных систем. В этом случае математическая модель ТПОС может быть записана в виде произведения комплексных передаточных функций его компонентов [1]:

$$G_{\text{тпос}}(s) = G_{\text{лс}}(s) \cdot G_{\text{ду}}(s) \cdot G_{\text{у}} \cdot G_{\text{фнч}}(s) \cdot G_{\text{фвч}}(s) \cdot G_{\text{рф}}(s) \cdot G_{\text{су}},$$

где $G(s)_i$ – передаточные функции входящих в ТПОС компонентов.

В основе программируемых аналоговых интегральных схем (ПАИС) лежит схемотехника на переключаемых конденсаторах. Внутренняя структура чипа ПАИС представлена на рис. 2 (см. ниже).

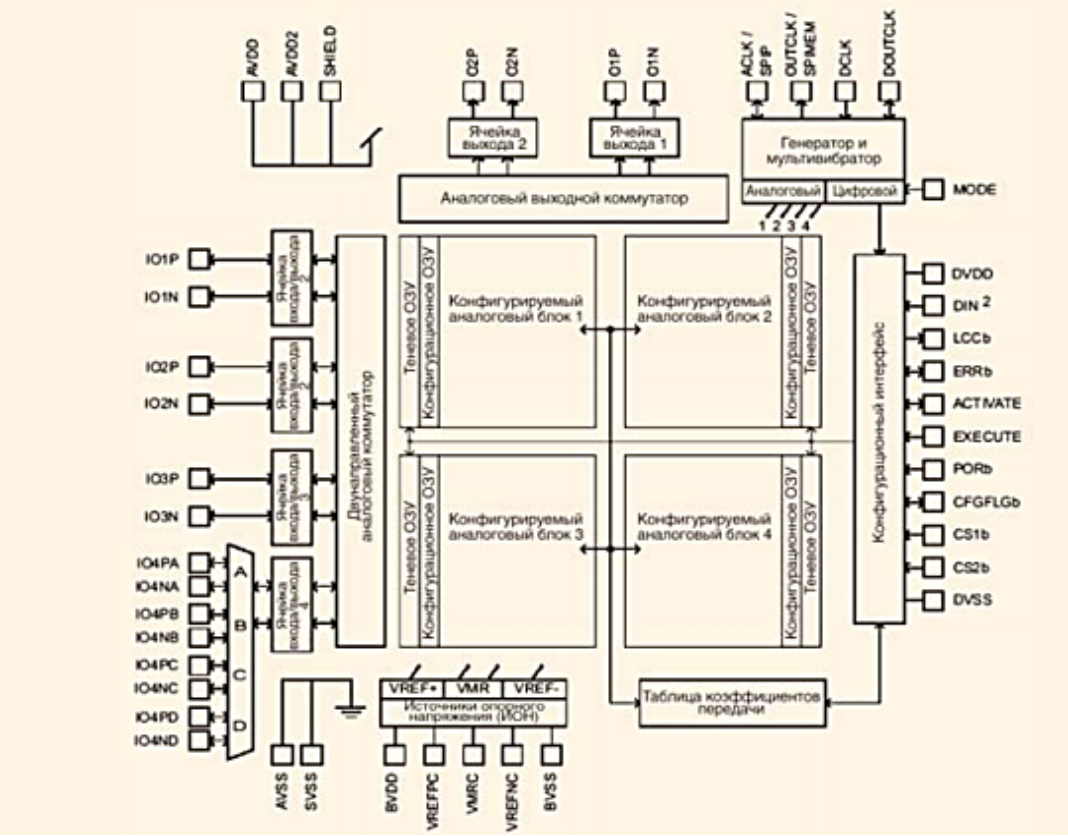


Рис. 2. Структура ПАИС

Её основу составляют конфигурируемые аналоговые блоки (CAB), которые содержат наборы элементов для реализации стандартных устройств – операционных усилителей, компараторов – конфигурируемых аналоговых модулей (CAM), а также конфигурационную память (*Look Up Table*) и специальный интерфейс. Входные аналоговые сигналы подаются в CAB через конфигурируемые двунаправленные I/O ячейки. Синхронизация в ПАИС может осуществляться при помощи внешнего источника или от встроенного тактового генератора с внешним кварцевым резонатором. Режимы работы CAB, значения тактовых частот, направления передачи сигналов, назначения и конфигурация ячеек входа/выхода хранятся в так называемой конфигурационной памяти (*Configuration* SRAM). Копия содержимого конфигурационной памяти хранится в теневом ОЗУ (*Shadow* SRAM), которое может перезаписываться без нарушения процесса обработки сигнала. Это позволяет динамически изменять конфигурацию ПАИС в работающем устройстве во время работы предыдущей версии. После загрузки в теневое ОЗУ новых данных конфигурация устройства изменяется

за один цикл тактовой синхронизации. Все САВ имеют доступ к общей конфигурационной памяти (*Look Up Table*), в которой хранится информация о передаточных характеристиках устройств, необходимых для реализации таких функций, как сжатие динамического диапазона, линеаризация сигналов датчиков, формирование сигналов произвольной формы, управляемая фильтрация [2].

Для моделирования тракта предварительной обработки сигнала используем систему автоматизированного проектирования программируемых аналоговых интегральных схем Anadigm Designer 2, которая позволяет создавать новые или вносить изменения в уже имеющиеся схемотехнические решения на основе ПАИС [3].

На рис. 3 показана структура, моделирующая работу нескольких элементов, входящих в состав ТПОС: инвертирующего суммирующего усилителя и фильтра низких частот.

Для исследования данной схемы подадим на ее вход два синусоидального сигнала: полезный сигнал с амплитудой 50 мВ и частотой 10 кГц, а также высокочастотную помеху с аналогичными параметрами 50 мВ и 1000 кГц соответственно.

Результаты моделирования можно наблюдать на имитаторе осциллографа (рис. 4).

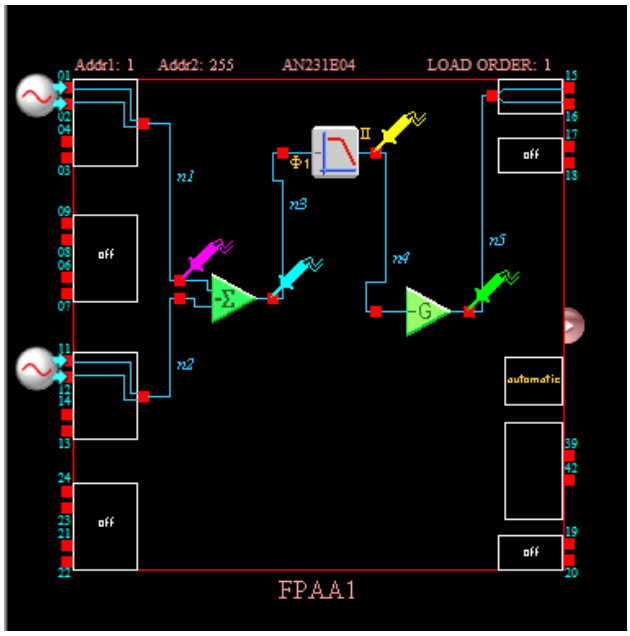


Рис. 3. Фрагмент ТПОС в Anadigm Designer 2

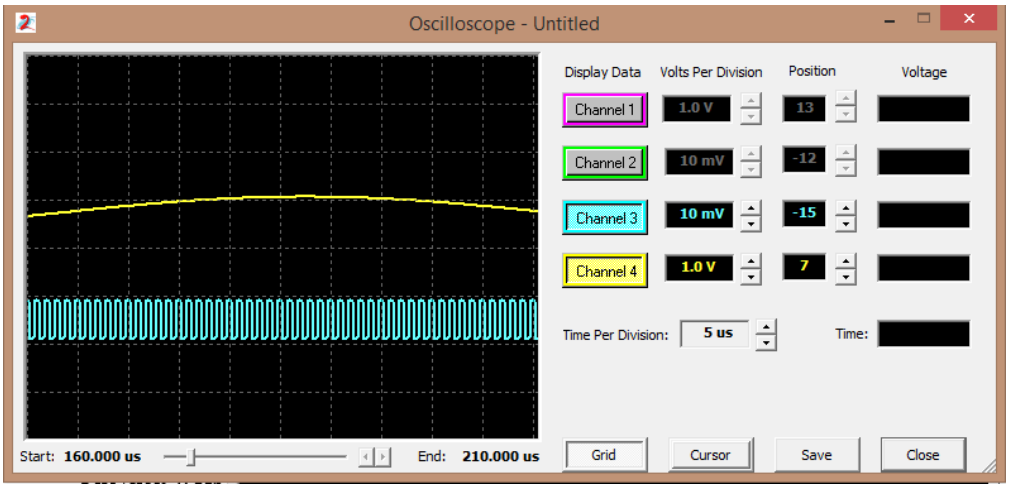


Рис. 4. Прохождение двух сигналов через САМ ФНЧ

Из графика видно, что помеха после прохождения САМ фильтра низких частот полезный сигнал, не меняет своей амплитуды (желтая линия, рис. 4), а помеха заметно ослабляется (синяя линия, рис. 4).

С целью увеличения амплитуды полезного сигнала на выходе ФНЧ до необходимого значения (1–1,5 В) использован САМ инвертирующего усилителя с коэффициентом усиления около 3 (рис. 5).

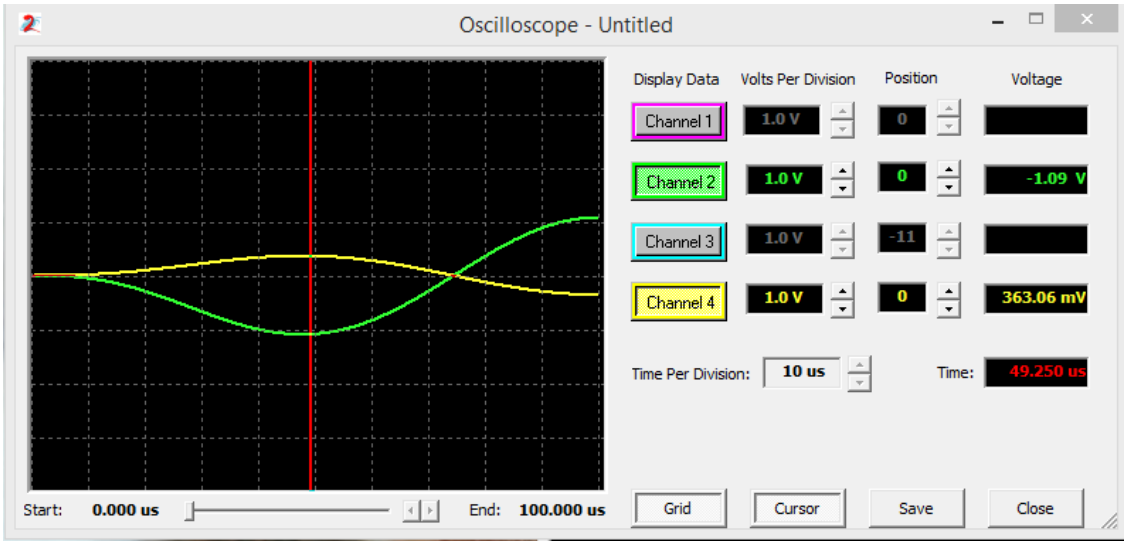


Рис. 5. Сигнал на входе (желтая линия) и выходе (зеленая линия) САМ инвертирующего усилителя

Сигнал на выходе аналогового цифрового преобразователя (АЦП) (зеленая линия) имеет значение амплитуды 1,09 В, что достаточно для обеспечения входного динамического диапазона АЦП (1,5 В).

В заключении статьи хочется отметить, что использование ПАИС при разработке ТПОС имеет ряд преимуществ по сравнению с использованием для аналогичных целей только дискретных систем. А САПР Anadigm Designer 2 позволяет производить не только моделирования разрабатываемой схемы, но и ее программирование в чип ПАИС.

Список используемых источников

1. Волович Г. И. Схемотехника аналоговых и аналого-цифровых электронных устройств. М. : Издательский дом «Додека–XXI», 2005. 258 с.

2. Полищук А. Программируемые аналоговые ИС Anadigm: весь спектр аналоговой электроники на одном кристалле. Первое знакомство // Современная электроника, 2004. № 12. С. 8.

3. Полищук А., Полищук А. Система автоматизированного проектирования программируемых аналоговых интегральных схем Anadigm Designer 2. Часть 1. Первый шаг: знакомство с интерфейсом // Компоненты и технологии, 2005. № 8. С. 62–66.

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

УДК 621.37

РАСПОЗНАВАНИЕ АПЕРИОДИЧЕСКОЙ ИМПУЛЬСНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НЕЙРОННОЙ СЕТЬЮ ВИДА NARX

А. В. Ваганов, А. С. Чистяков

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

В статье описывается нейронная сеть вида NARX, предназначенная для обнаружения импульсной апериодической последовательности, имитирующей сигнал от измерительного преобразователя АСУ, на фоне помех. Рассматривается процесс формирования наборов тестовых данных, на основе которых происходит обучение сети. Обосновывается архитектура NARX-сети, обеспечивающая возможность надежного обнаружения импульсного сигнала на фоне белого шума, синусоидальной помехи и одновременного воздействия обоих видов помех. Рассмотрен вопрос определения минимальной ширины импульса, при которой он может быть обнаружен зашумленном сигнале. Формируются рекомендации для выбора параметров нейронной сети, обладающей минимальными ресурсозатратами с целью ее реализации на базе программируемых аналоговых интегральных схем.

искусственные нейронные сети, распознавание сигнала, импульсная последовательность, помеха.

Искусственные нейронные сети (ИНС) являются перспективным направлением развития в различных областях науки и техники. В настоящее время существует множество разновидностей нейронных сетей, для решения широкого спектра задач, связанных с обработкой и распознаванием сигналов.

В статье ставится задача распознавания полезного сигнала на фоне случайной и постоянной помех, а также сочетания данных видов помех. Для решения задачи использовалась нелинейная авторегрессионная сеть прямого распространения NARX (*Nonlinear Autoregressive Network*) [106]. Выбор был обусловлен тем, что NARX является реккурентной и имеет достаточно простую структуру.

Выбор структуры сети производился экспериментальным методом. Для каждого вида помех, воздействующих на полезный сигнал, был составлен обучающий набор входных данных и целевых выходных данных, на основе которых происходило обучение нейронной сети с различной конфигурацией параметров. Структура, с которой нейронная сеть показывала наименьшее расхождение между целевыми и входными данными,

принималась в качестве наилучшей для решения задачи распознавания сигнала на фоне исследуемого вида помехи.

Для обучения ИНС использовался метод обратного распространения ошибки основанный на алгоритме Левенберга-Маркуардта [2]. Вектор входов (IW) и вектор обратных связей (LW) ограничены 5 значениями (max IW, max LW). Размер скрытого слоя (H) ограничен 10 нейронами (max H). В качестве целевых данных использовалась последовательность прямоугольных импульсов одинаковой ширины, случайно сдвинутых по фазе. Эта последовательность сравнивается выходной с последовательностью нейронной сети на этапе обучения для редактирования весовых коэффициентов. Случайное расположение импульсов выбрано для того, чтобы исключить зависимость параметров нейронной сети от периода следования сигнала.

В качестве случайной помехи был выбран белый шум, поскольку он является идеальным образцом случайных шумов, возникающих в АСУ, например, теплового шума [3]. Тренировочная последовательность делилась на 5 частей, на которых отношение сигнала к шуму равнялось -1 дБ, -5 дБ, -10 дБ, -15 дБ, -20 дБ соответственно. На рис. 1 представлены наложенные друг на друга графики входной и целевой последовательностей. Красным цветом изображена целевая последовательность, синим цветом – входная последовательность.

Экспериментально установлено, что наилучший показатель результатов обучения имеет структура сети с IW равном 2, LW равном 5, H равном 7. В таблице 1 представлена корреляция целевой последовательности (ЦП) и выходной последовательности (ВП) данных.

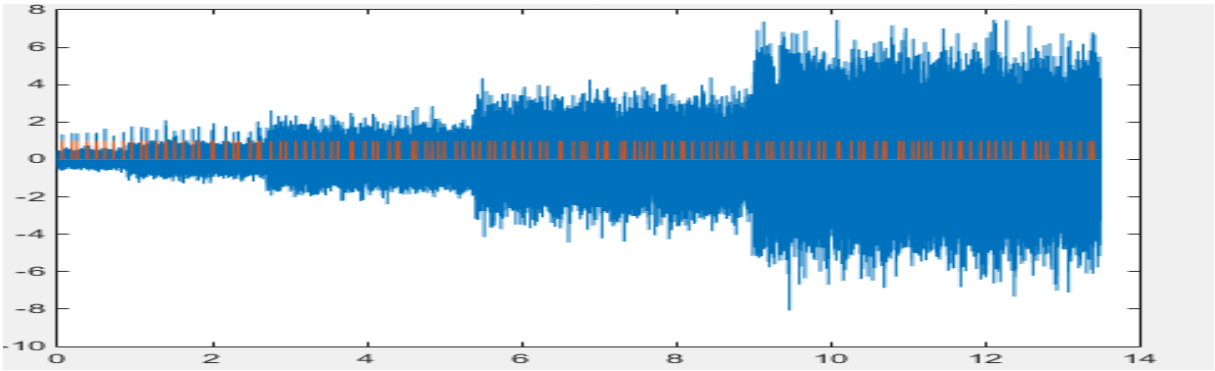


Рис. 1. Сигнал с помехой в виде белого шума. Тренировочный набор данных

ТАБЛИЦА 1. Корреляция ЦП и ВП для случайной помехи

Отношение сигнал/шум, дБ	–1	–5	–10	–15	–20
Корреляция	0,588	0,600	0,454	0,291	0,017

В качестве постоянной помехи была выбрана синусоидальная помеха, поскольку такая помеха часто имеет место на практике в виде наводок от сети переменного тока. Входная последовательность была разделена на 5 частей, на которых отношение сигнал/шум равнялось 0 дБ, а частота синусоидальной помехи устанавливалась 1 кГц, 10 кГц, 20 кГц, 30 кГц, 40 кГц, 50 кГц соответственно. На рис. 2 представлены наложенные друг на друга графики входной и целевой последовательностей. Красным цветом изображена целевая последовательность, синим – входная последовательность.

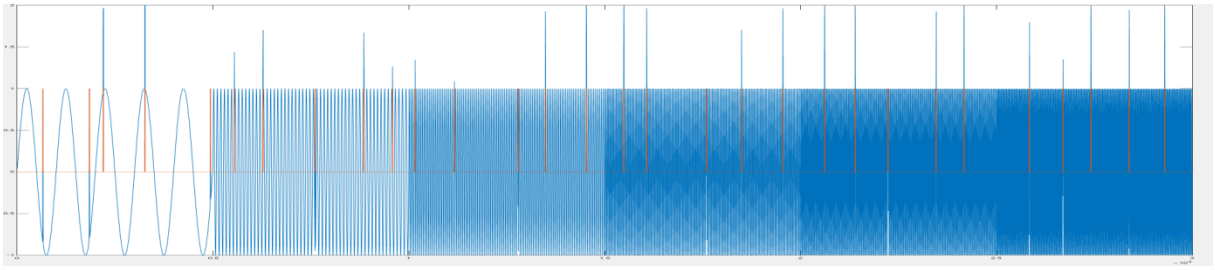


Рис. 2. Сигнал с синусоидальной помехой. Тренировочный набор данных

Установлено, что наилучший показатель результатов обучения имеет структура сети с IW равном 4, LW равном 4, H равном 5. В таблице 2 представлена корреляция целевой последовательности и выходной последовательности данных [4].

ТАБЛИЦА 2. Корреляция ЦП и ВП для постоянной помехи

Частота, кГц	0,05	1	10	50	75
Корреляция	0,945	0,945	0,944	0,942	0,773

Проведено исследование работы ИНС по распознаванию полезного сигнала при воздействии на него синусоидальной помехи и белого шума одновременно. В качестве тренировочного набора входных данных бралась последовательность целевых данных, на которую накладывалась помеха в виде всех возможных сочетаний синусоидальных помех и белого шума. На рис. 3 представлены наложенные друг на друга графики входной и целевой последовательностей. Красным цветом изображена целевая последовательность, синим – входная последовательность.

Установлено, что наилучший показатель результатов обучения имеет структура сети с IW равном 5, LW равном 5, H равном 5. В таблице 3 представлена корреляция целевой последовательности (ЦП) и выходной последовательности (ВП) данных.

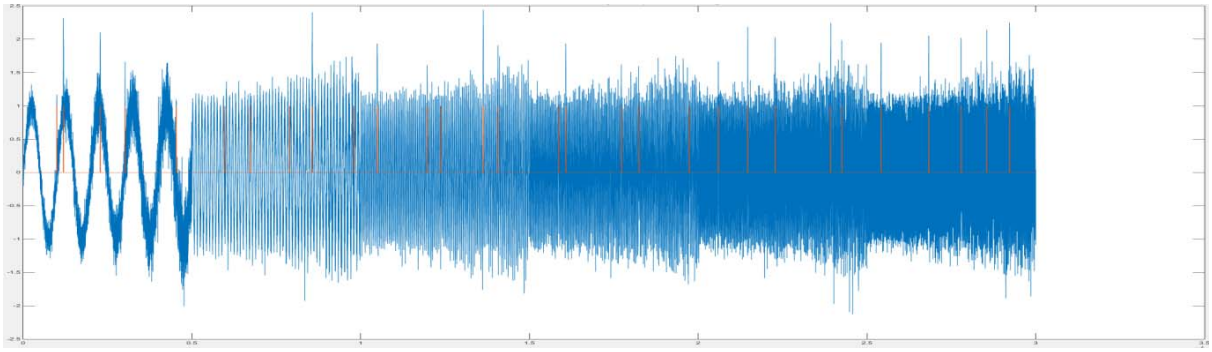


Рис. 3. Сигнал с двумя видами помех. Тренировочный набор данных

ТАБЛИЦА 3. Корреляция ЦП и ВП для постоянной помехи

Частота, кГц	0,05			1			50		
Отношение сигнал/шум, дБ	–1	–7,5	–15	–1	–7,5	–15	–1	–7,5	–15
Корреляция	0,655	0,684	0,387	0,542	0,484	0,317	0,450	0,102	0,360

Выявлено, что амплитуда импульсов выходной последовательности будет зависеть от положения импульса входной последовательности относительно фазы синусоидальной помехи.

Для определения допустимой ширины импульса при распознавании полезного сигнала на фоне помехи, ширина импульса входной последовательности бралась равной $k * t$, где $t = 0{,}01$ сек. – ширина импульса в целевой последовательности, k – коэффициент изменения ширины, который принимался от 0,1 до 1 с шагом 0,1 и от 1 до 10 с шагом 1. На рис. 4 представлены графики работы сети при уровне шума -5 дБ и $k = 10$. Можно сделать вывод, что нейронная сеть выделяет помеху, сложенную с импульсом полезного сигнала. В таблице 4 представлена корреляция целевой последовательности (ЦП) и выходной последовательности (ВП) данных при соотношении сигнал/шум равном -5 дБ.

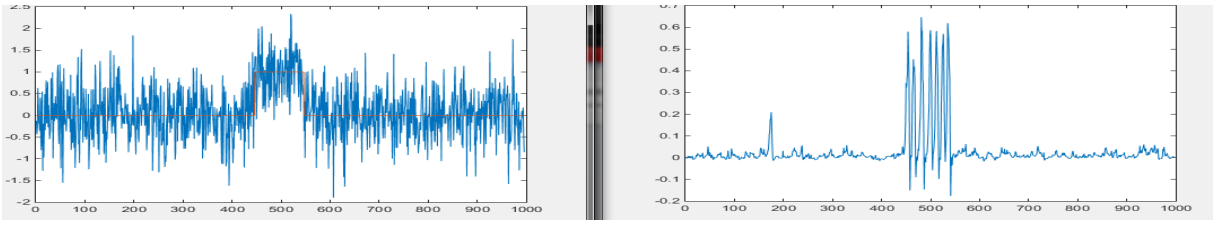


Рис. 4. Распознавание полезного сигнала с увеличенной шириной импульса

ТАБЛИЦА 4. Корреляция ЦП и ВП для различной ширины импульса.

Ширина импульса, с.	0,001	0,005	0,010	0,050	0,100
Корреляция	–0,001	0,32	0,751	0,592	0,575

Можно заключить, что полезный сигнал, ширина которого меньше ширины полезного сигнала в тренировочной последовательности распознается значительно хуже сигнала, ширина которого больше ширины полезного сигнала в тренировочной последовательности.

Изучение ИНС вида NARX в качестве системы для распознавания сигнала показало, что сеть достаточно хорошо распознает полезные сигналы на фоне помехи определенного вида. Сигнал с постоянной помехой распознается лучше сигнала со случайной помехой. При совместном воздействии рассмотренных видов помех качество распознавания снижается пропорционально увеличению частоты. Дальнейшие исследования проблемы могут быть направлены в сторону улучшения качества организации тренировочных наборов данных для случаев сочетания различных видов помех.

Список используемых источников

1. Ефименко Г. А., Синица А. М. Нейронные сети в MatLab [Электронный ресурс] // Digiratory. 2017. URL: https://digiratory.ru/508 (дата обращения 09.01.2018).

2. Гилл Ф., Мюррей У., Райт М. Практическая оптимизация. М. : Мир, 1985. 509 с.

3. Понятие о помехах и методы борьбы с ними [Электронный ресурс] // Wikibooks. 2017. URL: https://ru.wikibooks.org/wiki/Понятие_о_помехах_и_методы_борьбы_с_ними (дата обращения 09.01.2018).

4. Corrcoef [Электронный ресурс] // MathWorks. 2018. URL: https://www.mathworks.com/help/matlab/ref/corrcoef.html (дата обращения 09.01.2018).

Статья представлена заведующим кафедрой, доктором технических наук, профессором Г. В. Верховой.

УДК 514.88;004.925.8

МЕТОДЫ СКАНИРОВАНИЯ ОКРУЖАЮЩЕГО ПРОСТРАНСТВА СПОСОБАМИ ТРИАНГУЛЯЦИОННОГО ЛАЗЕРНОГО ДАЛЬНОМЕРА С ПРИМЕНЕНИЕМ ДИФРАКЦИОННОЙ РЕШЁТКИ

И. А. Васильев, М. А. Трифанов, В. С. Усс

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

В статье рассматривается новый способ измерения расстояния с помощью лазерных дальномеров и на его основе разрабатываются методы построения карты ме-

стности и определения положения. Новизна заключается в совместном применении триангуляционного лазера и дифракционной решётки для сбора информации о форме и расположении объектов в пространстве. За счёт дифракционной решетки данный метод позволяет производить сканирование и построение карты сразу в нескольких плоскостях; выстраивание плоских контуров по оси Z позволяет создавать модель поверхностей объектов в окружающем трехмерном пространстве.

дифракционная решётка, триангуляционный лазер, сканирование, пространство, форма, карта местности.

Современные технологии трёхмерного сканирования основаны на применении достаточно дорогостоящих устройств, требующих тонкой настройки и калибровки, и зачастую не обеспечивают получения исчерпывающей информации о геометрических свойствах сканируемого объекта [1]. Кроме того, размеры сканируемых объектов могут быть столь велики, что обычная сканирующая техника становится практически неэффективной. В особенности, эти проблемы становятся актуальными, когда получаемая информация должна быть использована для восстановления частично разрушенных объектов, реконструкции событий дорожно-транспортных происшествий, в разметке местности и геолокации, а также для создания модели виртуальной среды с целью оценки событий и для управления их развитием [2]. Для получения виртуальной модели среды важно также получить информацию не только о форме, но и о свойствах материала.

Данное исследование проводится с целью решения задач трёхмерного сканирования триангуляционным методом [2, 3] с помощью дифракционной решётки и получения воксельной модели [4], чем обеспечивается получение информации и о материале, и форме объекта. Модель пригодна также для осуществления вычислительных симуляций в созданной виртуальной среде.

Концепция устройства основана на технологии лазерного проецирования по принципу работы триангуляционного лазера. На рис. 1 два лазера синего и красного света с помощью расщепляющих линз, которые развёрнуты относительно друг друга на 90 градусов, освещают дифракционную решётку. С помощью системы зеркал лучи соединяются в призме и формируют картину трёхцветной решётки, где в пересечении линий образуют фиолетовые точки. Далее изображение попадает в объектив с переменным фокусным расстоянием (рис. 2). Камера, которая стоит под определённым углом α к системе построения проекции дифракционной решётки, считывает полученные точки и на основе этой информации программа рассчитывает воксель.

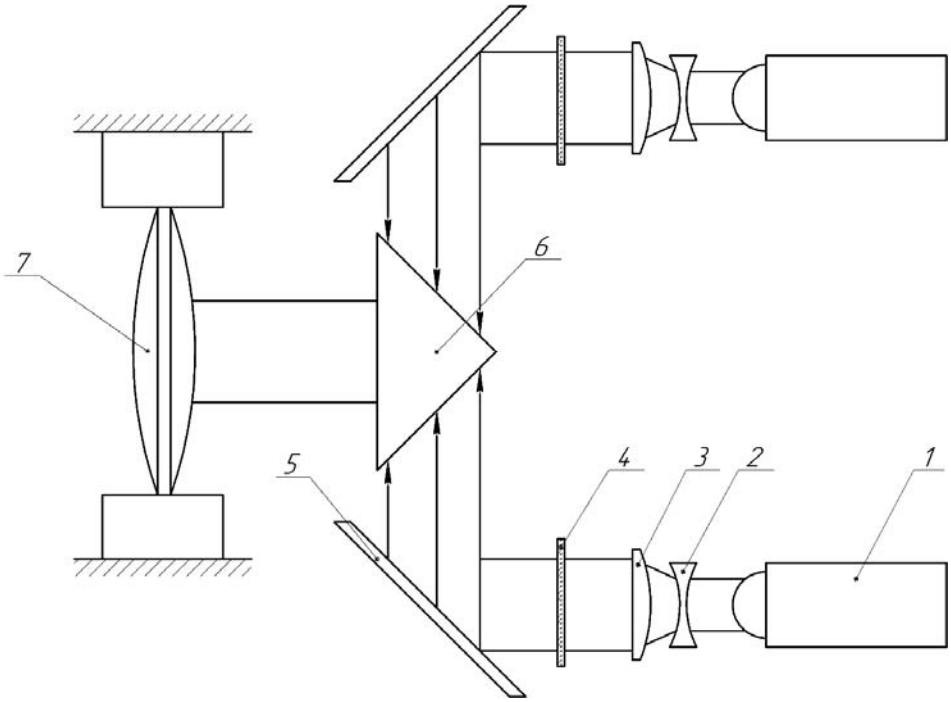


Рис. 1. Устройство лазерного проецирования дифракционной решётки (1 – лазер, 2 – расщепляющая линза, 3 – собирающая линза, 4 – дифракционная решётка, 5 – зеркало, 6 – призма, 7 – объектив)

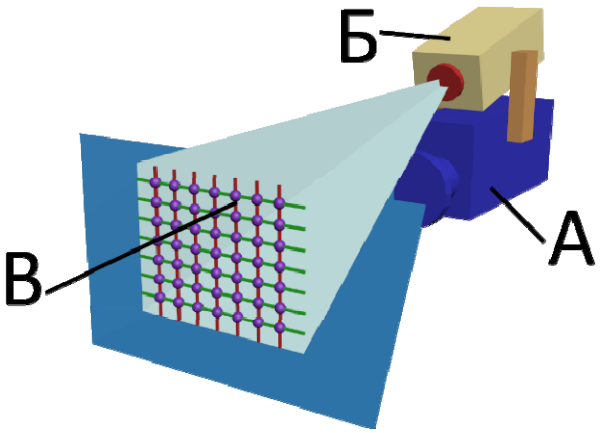


Рис. 2. Метод триангуляционного сканирования (А – камера, Б – система генерации дифракционной решётки, В – дифракционная решётка)

В каждой точке, полученной при пересечении линий, получается воксель и определяется его положение в пространстве. При изменении фокусного расстояния или расстояния до проецируемой дифракционной решётки производится детальное сканирование отдельных элементов объекта или среды. В итоге, удается получить гибридную воксельную трёхмерную модель, представленную в виде разреженного воксельного дерева, что обеспечивает сокращение объема полученных данных, передаваемых для обработки в нейросеть. Результатом преобразования информации в нейросети является геометрическая модель сканируемого объекта. В зависимости от постановки задачи, в которой предполагается использование данной модели, возможно получение модели либо полигонального, либо твердотельного представления

Изначально объект анализируется с помощью дифракционной решётки с относительно крупным шагом между узлами, чем обеспечивается по-

лучение предварительных данных о геометрической форме трёхмерного объекта. Для получения более детализированной информации об объекте следует сфокусировать изображение, созданное дифракционной решеткой, на интересующих исследователя областях и, тем самым, обеспечить дополнение первичной воксельной модели новыми данными о поверхности (рис. 3).

Рис. 3. Сканируемый объект

Рис. 4. Воксельная модель

Используя алгоритм voxel octree [5], на выходе преобразования можно получить воксельную модель с регулируемым количеством вокселей (рис. 4). За счёт этого можно менять тип модели, получая из базового воксельного представления твердотельную модель с возможностью геометрического редактирования и с дополнением информацией о материале, что в перспективе даёт возможность оценки физических параметров и проведения симуляции в виртуальной среде для оценки качества модели.

Помимо этого, предлагаемый метод позволяет осуществить преобразование воксельного представления формы в модель полигонального вида, обеспечивая значительное сокращение занимаемого моделью объёма вычислительной памяти, что крайне важно при решении задач симуляции событий [6].

Для получения более полной информации об объекте по базовой воксельной модели с помощью использования технологий нейросети можно определить его тип. Это позволяет решать задачи автоматизированной реконструкции объектов и реконструкции событий с использованием карты местности.

В результате сканирования с использованием триангуляционного лазерного метода и получением воксельной модели разряженного дерева на основе обработки информации в нейросети удается относительно быстро и точно получить данные о геометрической форме объекта, его материале и иных расчетных физических характеристиках. Получаемая таким образом модель может быть легко адаптирована для конвертации в полигональные модели объектов в программах твердотельного моделирования.

Список используемых источников

1. Грузман И. С., Киричук В. С., Косых В. П., Перетягин Г. И., Спектор А. А. Цифровая обработка изображений в информационных системах: учебное пособие. Новосибирск : Изд-во НГТУ, 2000. 168 с

2. Гужов В. И. Методы измерения 3D-Профиля объектов контактные, триангуляционные системы и методы структурированного освещения. Новосибирск : Изд-во НГТУ, 2015. 82 с.

3. Скворцов А. В. Триангуляция Делоне и ее применение. Томск : Изд-во Том. ун-та, 2002.

4. Григорьев С. Н., Локтев М. А., Толок А. В. Построение воксельных моделей геометрических объектов // Прикладная информатика 2013. № 4 (46). С. 50–55.

5. Толок А. В. Функционально-воксельный метод в компьютерном моделировании / под. ред. академика РАН С. Н. Васильева. М. : ФИЗМАТЛИТ, 2016. 112 с. ISBN 978-5-9221-1680-0.

6. Силантьев Д. А., Лоторевич Е. А., Пушкарёв С. А., Толок А. В. Воксельно-математическое моделирование при решении задач определения площади для поверхностей деталей // Информационные технологии в проектировании и производстве. 2013. № 3. С 29–33.

УДК 004.7

ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ КОМПЛЕКСОВ

Е. М. Вашурина, Ю. Ю. Гагарин, О. С. Лаута, Д. В. Соловьев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье разработан робототехнический комплекс и система, позволяющая управлять этим комплексом по надежному криптографически стойкому соединению. Основным элементом данной системы является криптографический чип stm32f415. Он позволяет уменьшить нагрузку на центральный процессор для выполнения алгоритмов управления, освободив его от криптографических операций, тем самым, гарантируя выигрыш во времени.

канал управления, киберфизические системы, роботизированные системы, криптографические алгоритмы.

Кибернетическое противоборство знаменует собой новый уровень вооружённого противостояния. Насущным требованием времени, с учётом роботизация вооружения и военной техники, становится пересмотр принципов построения автоматизированных систем управления, информацион-

ных систем и сетей связи с позиций обеспечения кибербезопасности на основе построения интеллектуальных сервисов защиты информации.

В системе кибербезопасности должны быть предусмотрены возможности проведения упреждающих аппаратно-программных воздействий (упреждающих ударов) и активных атак на выявленные источники кибератак, информационные системы и ресурсы противоборствующей стороны, а также способность к дезинформации противоборствующей стороны об истинных свойствах и параметрах информационных систем и сетей связи.

На систему мониторинга и разведки киберпространства должна возлагаться функция обеспечения формирования и ведения базы данных по вскрытым (обнаруженным) различным видам и источникам киберугроз (кибератак), что предусматривает создание и ведение каталога потенциальных угроз кибербезопасности и признаков кибервоздействий на информационные ресурсы, определение номенклатуры потенциальных угроз кибербезопасности, создание и ведение банка критериев обнаружения кибератак на информационные системы, выявление и противодействие внедряемым боевым программным агентам и противодействия им [1].

С целью решения вышеуказанной проблемы предлагаются аппаратно-программные решения, путем разработки роботизированной системы, предназначенной для аудита (киберразведки) устойчивости сетевой инфраструктуры и приложений к существующим и перспективным киберугрозам (стрессовой нагрузке, различным DDoS-атакам, вредоносному коду в общем трафике, спаму, червям, атакам типа ”*zero day*”, атакам с применением технологии *fuzzing*, и т. д.), программно-математического воздействия на информационно-управляющие системы, физического уничтожения (или выводу из строя) объектов информационной инфраструктуры противника.

Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях – космос, автомобильные, химическая технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт, и потребительские устройства. Такой класс систем часто рассматривается как киберфизические системы.

С одной стороны, киберфизические системы за счет распределенной сети датчиков и блоков управления позволяют решить многие практические задачи, позволяющие как сэкономить время, так и уменьшить человеческие потери, за счет выполнения наиболее опасных заданий роботизированными системами.

С другой стороны, за счет использования открытых радиоканалов и известных протоколов киберфизические системы подвержены воздейст-

вию компьютерных атак, которые в наилучшем случае могут привести к нарушению работоспособности сети, а в худшем к перехвату управления.

К наиболее распространенным компьютерным атакам на киберфизические системы относятся:

Активные виды компьютерных атак – компьютерные вирусы, модифицированные драйвера, целенаправленные (таргетированные) атаки.

Пассивные виды компьютерных атак – подслушивание, парольные атаки, имитация удостоверения, атаки на уровне приложений [2, 3].

Учитывая вышеизложенное, в настоящее время остро стоит вопрос о защите киберфизических систем и каналов управления ими. С этой целью предлагается использовать криптографические протоколы и алгоритмы. Выделяют следующие виды криптографических преобразований:

1. Симметричное шифрование – TDES, DES, AES, ГОСТ 28147-89.
2. Ассиметричное шифрование – RSA, DSA, Эль-Гамаль.
3. Электронная цифровая подпись–FDH, ESDSA, ГОСТ Р 34.10-2012.
4. Хеш-функция – MD 2/4/5/6, SHA, ГОСТ Р 34.11-94.

Из перечисленных выше криптографических алгоритмов, для реализации защиты канала управления киберфизической системы, рациональным является симметричный алгоритмAES, который отличается криптостойкостью и быстродействием.

В настоящее время криптография решает следующие основные задачи:

1. Обеспечение конфиденциальности сообщений – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права к ней.
2. Обеспечение целостности данных – гарантированная невозможность несанкционированного изменения информации.
3. Аутентификация – подтверждение подлинности сторон и самой информации в процессе обмена данными.
4. Невозможность отказаться от авторства – предотвращение отказа абонента от совершенных им действий.

Эти задачи защиты данных реализованы в специальном аппаратном блоке, который называют криптографическим ускорителем (криптографическим блоком). Криптографические ускорители работают отдельно от основного ядра процессора, что позволяет ему сохранять свои ресурсы для выполнения следующих задач [4, 5, 6]:

– обслуживание для организации обмена с периферийными устройствами;
– обработку данных;
– осуществление беспроводного соединения с другими устройствами;
– управляющие и другие алгоритмы;

– ускорители позволяют шифровать данные по алгоритмам DES/TDES/AES, вычислять хеш-функции SHA-1/MD5/HMAC и генерировать случайные числа.

С целью проверки работы криптографического ускорителя была разработана роботизированная система, состоящая из следующих частей:

– BeagleBoneBlack (главный процессор роботизированной системы);
– Mini Maestro 18-Channel USB Servo Controller (драйвер–двигатель);
– MG996R (сервоприводы);
– STM32F415 (криптографический чип);
– Блок питания;
– Wifi-адаптер [7].

Корпус представляет собой металлический скелет, который связывает и объединяет необходимую периферию в единое целое, при этом, обеспечивая защиту и целостность компонентов. Все детали, из которых он состоит, были спроектированы в программе КОМПАС-3D V16 и вырезаны на фрезерном станке. Управление роботизированной системой осуществляется использованием wi-fi адаптера в качестве передатчика радиосигнала.

Для обеспечения криптографически стойкого протокола управления в роботизированной системе используется микроконтроллер с 32-разрядным ядром ARM Cortex-M4F с криптографическим ускорителем stm32f415rgt производства компании «STMicroelectronics».

Используя техническую документацию, был проведен анализ выводов криптографического чипа с выводами микроконтроллера stmf0, после которого было принято решение внедрить чип в плату stm32f0discovery, заземлив несколько контактов.

Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования использовался AES с длиной ключа 128 бит.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи–Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

В качестве центрального процессора и электронного мозга для робота был выбран одноплатный компьютер BeagleBoneBlack (BBB) [6, 7].

С целью подключения драйвера-двигатель (*MiniMaestro* 18-*ChannelUSBServoController*) к главному процессору (*BeagleBoneBlack*) по UART-интерфейсу был взят конвертор ADuM1201, который предназначен для преобразования электроэнергии одних параметров или показателей качества в электроэнергию с другими значениями параметров или показателей качества.

Для того чтобы провести исследования реализованной криптографической системы на предмет обнаружения проблем и ошибок, был осуществлен перехват и анализ передаваемых пакетов с помощью программы Wireshark.

Анализ пакетов реализованной криптографической системы на предмет обнаружения проблем и ошибок с помощью программы Wireshark показал, что команда, передаваемая роботизированной системе, является зашифрованной на шифрование wi-fi сети (WPA2), в отличие от технологии Bluetooth, является дополнительным препятствием к расшифрованию секретной команды злоумышленником. Кроме этого, организована постоянная смена крипто-ключей, тем самым исключена возможность их подбора [8].

Таким образом, в настоящей статье представлен пример создания роботизированного комплекса, как элемента КБС, с защищенной системой управления им на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кром того, для защиты от атаки «грубого перебора» криптографического ключа в системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

Список используемых источников

1. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сборник научных сетей : сб. науч. ст. в 4 т. 2017. С. 420–425.

2. Reference manual STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced ARM®–based 32–bit MCUs [Электронный ресурс] // STMicroelectronics, 2016. 1744 с.

3. Коцыняк М. А., Лаута О. С., Осадчий С. А. Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика» // Информация и космос. 2013. № 3–4. С. 25–27.

4. Схема обмена ключами Диффи-Хеллмана [Электронный ресурс]. URL: http://kaf403.rloc.ru/POVS/Crypto/DiffieHellman.html

5. Васюков Д. Ю., Коцыняк М. А., Коцыняк М. М., Лаута О. С., Лаута А. С. Устройство обнаружения удаленных компьютерных атак. Патент на изобретение RUS 2540838. 03.03.2014.

6. Елисеев А. И., Долгов А. А., Хорохорин М. А., Лаута О. С., Набатов К. А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Вестник Воронежского института ФСИН России. 2013. № 1. С. 91–94.

7. Баранов В. В., Иванов Д. А., Коцыняк М. А., Московченко В. М., Нечепуренко А. П. Применение метода топологического преобразования стохастической сети

для моделирования системы воздействия // Актуальные проблемы обеспечения информационной безопасности труда. Межвузовской научно-практической конференции. 2017. С. 38–43.

8. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях, ВАС. СПб., 2013.

УДК 004.491

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ ИНФОРМАЦИОННОМУ ВОЗДЕЙСТВИЮ НА САМООГРАНИЗУЮЩУЮСЯ ГРУППУ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А. М. Великанов[1], И. И. Викснин[1], И. И. Комаров[2], Е. Д. Мариненков[1], С. А. Ткаченко[1]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Важнейшим направлением преодоления технологических барьеров, определенных в рамках Национальной техн0логической инициативы, связанных с использованием мультиагентных самоорганизующихся беспилотных систем, является проблема обеспечения безопасного информационного взаимодействия между агентами. В работе предлагается метод обеспечения информационной безопасности информационного взаимодействия самоорганизующейся группа БПЛА, находящейся под деструктивным информационным воздействием.

беспилотный летательный аппарат, мультиагентная система, робототехническая система, информационное взаимодействие, деструктивное информационное воздействие, информационная безопасность.

В настоящее время расширяются сферы применения беспилотных летательных аппаратов: они отлично подходят для воздушного мониторинга, создания карт местности, поисковых работ. Вместе с тем, практическое применение этой технологии сдерживается наличием Технологического барьера «Большие данные № 1» системы AeroNet в рамках «Национальной технологической инициативы» [1].

Важнейшей задачей по преодолению этого барьера является обеспечение информационная безопасность, и, прежде всего, целостности и доступности информации в процессе информационного взаимодействия (ИВ)

элементов группировки БПЛА. Эта задача тем более актуальна, что классические методы обеспечения информационной безопасности (ИБ) слабо применимы для мультигентной системы с децентрализованным управлением. Практически применимые результаты в этой области опубликованы в работах [2, 3].

В работе рассматривается группировка БПЛА как система, обладающая эффектом эмерджентности, то есть, способной решать задачи, нехарактерные для любого участника данной структуры.

Классические временные ограничения стратегий группового управления [4], предопределили наиболее перспективную децентрализованную коллективную стратегию на основании следующих аргументов: время принятия решения линейно зависит от количества объектов в группе; в связи с отсутствием центрального управляющего устройства повышается отказоустойчивость системы; наличие общего канала информации позволяет реализовать взаимодействие между объектами коллаборации, что обеспечивает нахождение оптимального алгоритма для реализации поставленной авторами цели. Поскольку децентрализованные методы коллективного управления базируются на мультиагентном подходе, возможна адаптация и применение их в контексте групп БПЛА.

Постановка задачи обеспечения ИБ кибер-физической системы (КФС) аналогична, представленной в [5], и предполагает, что наибольшую опасность для группировки представляет именно деструктивное информационное воздействие (возможно скрытое). Особенностью скрытого деструктивного информационного воздействия (ДИВ) является то, что все подсистемы агента и группировки в целом функционируют в штатном режиме, а деструктивное воздействие формируется за счет нарушения семантической целостности информации.

В случае группировки БПЛА, межагентный обмен содержит информацию о: основной задаче группировки; их местоположениях; топологии среды; техническом состоянии и плане действий взаимодействующих агентов.

Рассмотрим случай нарушения семантической целостности информационного сообщения при сохранении синтаксической корректности сообщений. Показано [6], что это может привести к нарушению функционирования как подмножества агентов, так и группировки в целом.

На основе анализа обобщённого протокола взаимодействия (рис. 1) следует заключение о возможности нарушения семантической целостности любого из направлений ИВ при компрометации хотя бы единственного БПЛА, причем существующими средствами обнаружить факт компрометации невозможно.

Рис. 1. Уязвимые информационные сообщения и процессы в обобщенной модели ИВ элементов группы БПЛА

Особенностью ИВ в группировке является то, что информация, получаемая *i*-м БПЛА от других агентов, а также информация, передаваемая между этими агентами, уязвима для ДИВ, причем скомпрометированные сообщения передаются другим агентам без возможности проверки их корректности, что определяется ограниченностью области непосредственного «восприятия» сенсоров агента и ограниченностью вычислительных ресурсов. В данном случае первая информация передается напрямую от агентов, в то время как вторая – передается и обрабатывается всеми агентами группы, после чего обработанная информация, определяющая оптимальный алгоритм действий, передается всем агентам группы.

Предотвращение возникновения ДИВ предполагает разработку модели функционирования самоорганизующейся коллаборации на основе безопасного ИВ. Для разработки и внедрения контрмер были рассмотрены следующие методы обеспечения ИБ, применимые к КФС, организованным при помощи мультиагентного подхода: классификация информации, мобильная криптография, «товарищеская» модель, Police Office Model (POM), криптосистемы с открытым ключом.

Для обеспечения ИБ ИВ элементов группировки БПЛА предлагается усовершенствованная модель безопасного ИВ агентов в рамках группировки БПЛА (рис. 2). Применимость в области AeroNet определяется: возможностью индивидуальной настройки каждого из агентов на этапе подготовки к применению группировки, достаточностью вычислительных

ресурсов для решения задач «легкой криптографии», возможностью динамической локализации агентов, естественной временной коллаборацией.

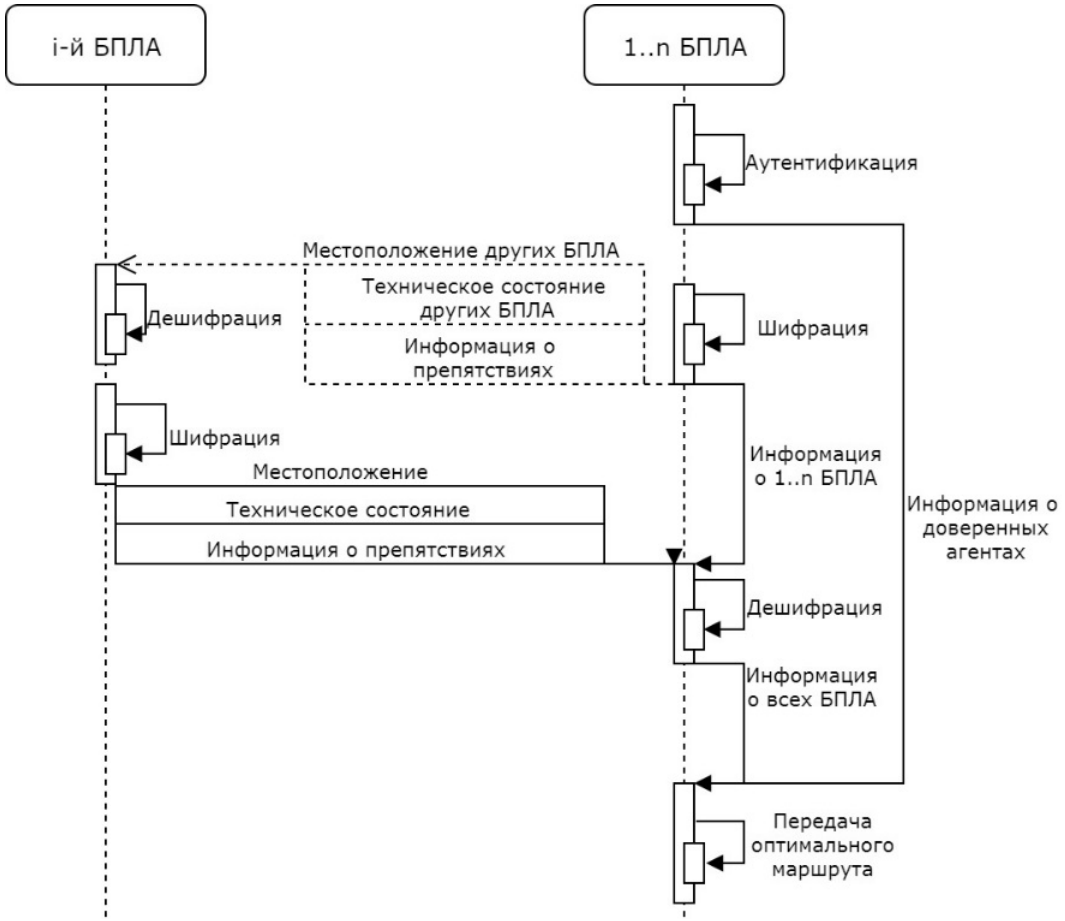


Рис. 2. Модель защищенного ИВ элементов группы БПЛА

Модель безопасного ИВ основывается на системе надежной аутентификации, использующий модернизированный подход POM [7], мобильную криптографию и временную оптимизации для использования в децентрализованной группе БПЛА.

Таким образом, с начала функционирования группы каждый определенный дискретный момент времени любой агент может быть назначен Police Officer (PO) – устройством, отвечающем за безопасность своей области.

При миграции агента в область, контролируемую PO, PO отправляет агенту программу, содержащую зашифрованную функцию и которую необходимо выполнить агенту, используя «секретную» информацию. Результат, полученный после выполнения, отправляется PO, после чего происходит процесс дешифрации, и PO сравнивает полученный результат с ожидаемым результатом.

Таким образом, РО проверяет доверенность агента и, в случае несовпадения результатов, оповещает всех других агентов о не доверенном, что ведет исключение последнего (скомпрометированного?) агента из процесса ИВ. Это позволяет предотвратить распространение деструктивной информации и защитить других агентов от ДИВ. Для ликвидации уязвимостей в процессе обмена информацией, предлагается использование криптосистемы с открытым ключом, что позволяет обеспечить семантическую целостность информации, в связи с исключением возможности изменения ИС сторонним агентом.

С методологической точки зрения целесообразно разделять угрозы по источнику их возникновения на преднамеренные, т. е. угрозы, исходящие от агента, целенаправленно реализующего ДИВ, и случайные, т. е. связанные с какими-либо аппаратно-программными или информационными неисправностями агентов, принадлежащих исходной группе.

Для разработки плана реагирования на преднамеренные угрозы целесообразно использовать классический подход определения уязвимостей, оценки рисков ИБ и прогнозирования сценария действий потенциального нарушителя ИБ.

Минимизация рисков от случайных угроз должна проводиться методом анализа надежности программно-технических систем и использованием традиционных подходов повышения надежности.

Вместе с тем, следует отметить, что вне зависимости от источника возникновения, перспективным направлением решения задачи *выявления* факта наличия скрытого информационного воздействия является подход, связанный с анализом косвенных признаков функционирования группировки, и построением «портретов» в специфических признаковых пространствах, характеризующих выполнение типовых операций [3]. По виду и степени отклонения от эталонных портретов можно сделать заключение о виде и интенсивности ДИВ.

Таким образом, предлагаемая модель безопасного ИВ элементов группировки БПЛА обеспечивает защиту, как взаимодействующего агента, так и информационное обеспечение группировки от ДИВ, происходящего от источника, не прошедшего аутентификацию.

Вместе с тем, представленная модель защищённого ИВ не свободна от недостатков. Например, она не позволяет нейтрализовать случайные угрозы нарушения семантической целостности информации, которые могут возникнуть вследствие аппаратных сбоев аутентичного агента. Однако выявление такого рода противоречий возможно уже только на основе анализа информации от большего числа агентов, например, с использованием поведенческих подходов [8].

Список используемых источников

1. Национальная технологическая инициатива [Электронный ресурс]. URL:http://nti.one/technology/docs/Technological_barriers_Aeronet_Contest.pdf (дата обращения 21.03.2018)
2. Юрьева Р. А., Комаров И. И., Дородников Н. А. Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением // Программные системы и вычислительные методы. 2016. №. 1. С. 42–48.
3. Комаров И. И., Дранник А. Л., Юрьева Р. А. Моделирование проблем информационной безопасности мультиагентных систем // В мире научных открытий. 2014. №. 4. С. 61–70.
4. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов: монография. М. : ФИЗМАТЛИТ, 2009. 280 с.
5. Комаров И. И., Юрьева Р. А., Дранник А. Л., Масленников О. С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем // Наука и бизнес: пути развития. 2015. №. 3. С. 66–72.
6. Viksnin I. et al. Flocking factors' assessment in case of destructive impact on swarm robotic systems // Proceedings of the 18th Conference of Open Innovations Association FRUCT. FRUCT Oy, 2016. PP. 357–363.
7. Zikratov I. A. et al. Security model of mobile multi-agent robotic systems with collective management // Nauchno-Tekhnicheskii Vestnik Informatsionnykh Tekhnologii, Mekhaniki i Optiki. 2017. Т. 17. №. 3. С. 443.
8. Viksnin I. et al. Assessment of stability of algorithms based on trust and reputation model // Proceedings of the 18th Conference of Open Innovations Association FRUCT. FRUCT Oy, 2016. PP. 364–369.

УДК 004.946

МОДЕЛИ И АЛГОРИТМЫ АТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИЕЙ

Г. В. Верхова, А. Л. Иофик

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

В статье рассмотрены модели и алгоритмы управления научно-технической информацией. Данные модели могут быть использованы при автоматизации планирования, выполнения и анализа научно-исследовательских и опытно-конструкторских работ, а также в системе «электронная редакция». Применение данных моделей и алгоритмов позволит повысить качество планирования направлений и объемов научных работ, обеспечит рациональный выбор коллектива исполнителей, сократит объемы рутинной работы при создании отчетов. Предложенные модели и алгоритмы ориен-

тированы на использование в рамках единой киберсреды постиндустриального общества.

модель, научно-техническая информация, интернет, жизненный цикл.

Характерной чертой развития современной науки является большой поток новых научных данных, получаемых в результате исследований. Важной составной частью национальных информационных ресурсов являются непубликуемые источники: научно-технические отчеты, диссертации и переводы. Они являются важным каналом научных коммуникаций, носителями информации, необходимой для решения практических задач. Непубликуемые источники НТИ (научно-технической информации) существуют всего в нескольких экземплярах, поэтому доступ к ним обеспечивается созданием на федеральном уровне централизованных фондов.

Для увеличения скорости отбора необходимой документации из общего объема и повышения эффективности труда создана государственная система научно-технической информации (ГСНТИ), которая представляет собой совокупность научно-технических библиотек и организаций, специализирующихся на сборе и обработке научно-технической информации (рис. 1) и взаимодействующих между собой с учетом принятых на себя системных обязательств.

В состав ГСНТИ входят [1]:

– федеральные органы научно-технической информации и научно-технические библиотеки;

– отраслевые органы научно-технической информации и научно-технические библиотеки;

– региональные центры научно-технической информации.

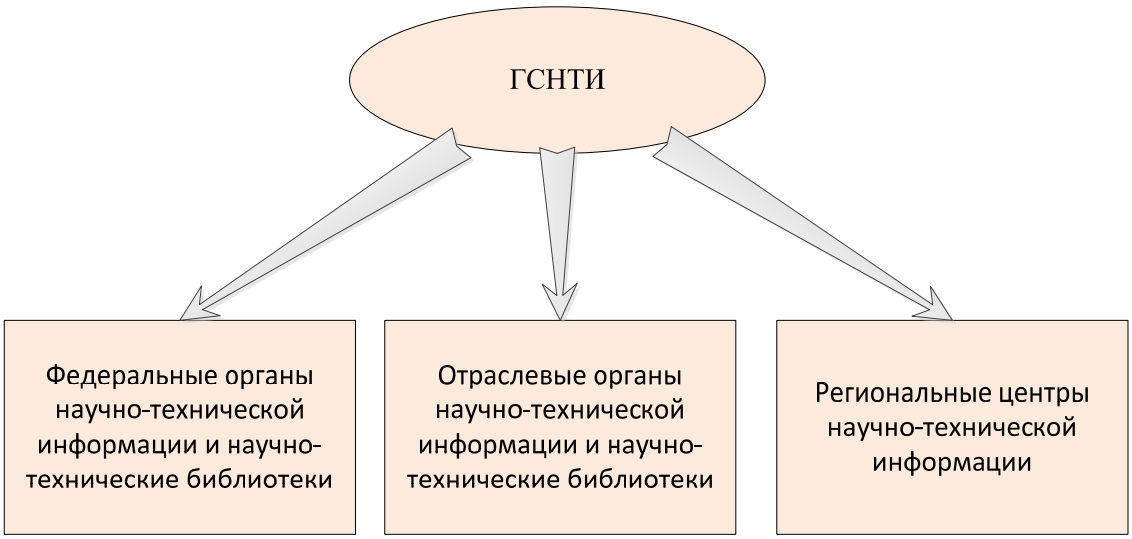


Рис. 1. Состав ГСНТИ

В настоящий момент перед всеми участниками создания и потребления научно-технической информации стоит ряд проблем, основными из которых являются (см. рис. 2 ниже):

– управление коллективной работой авторского коллектива;

– передача рукописи статьи, доклада или депонируемой рукописи в редакцию или любой другой орган научно-технической информации посредством «одного клика»;

– организация удаленного взаимодействия издательств, оргкомитетов конференций и других органов научно-технической информации с авторским коллективом, через единое информационное пространство, с использованием модели управления версиями в режиме работы над единым документом;

– передача обработанных документов и информационных продуктов издательствами и другими органами научно-технической информации в наукометрические системы, библиотеками и магазинами посредством «одного клика» или минимального внесения дополнительной информации, которая не была сохранена на предыдущих этапах.

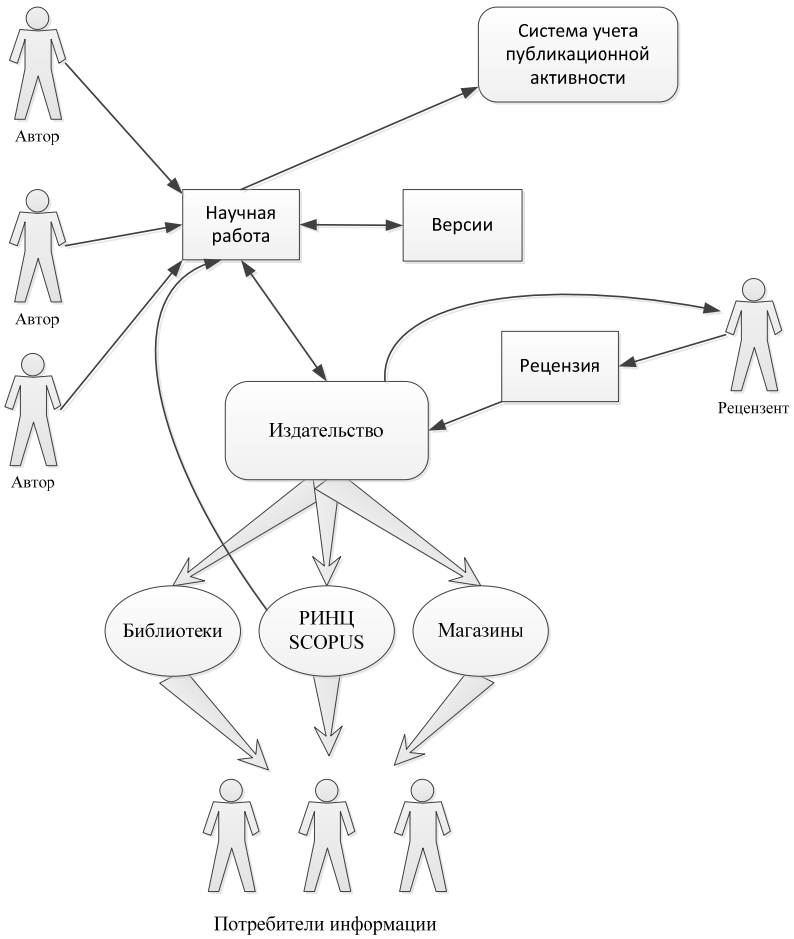


Рис. 2. Информационные потоки, демонстрирующие работу алгоритмов управления жизненным циклом научно-технической информации

Решение основных проблем управления научно-технической информацией, представленной в настоящий момент времени в основном электронными документами, можно решить, лишь используя новейшие информационные технологии построения киберсред, объединяющих как модели и алгоритмы управления собственно научно-технической информацией, так и отношениями между участниками [2].

Технология, положенная в основу такой среды должна базироваться на трех базовых принципах:

– агентности или индивидуального представительства, который предполагает формирование мультиагентной сети, в которой каждый участник (юридическое или физическое лицо) самостоятельно регистрируется в виде независимого агента, имея полный контроль над собственным информационным профилем и установлением информационных связей с другими агентами;

– информационного самообслуживания, заключающимся в представление информации в киберсреде ее непосредственными обладателями, которые одновременно являются заинтересованными лицами в ее распространении для ограниченного или неограниченного круга лиц;

– управляемой информационной открытости, когда свободное распространение информации на основе набора лицензий, задающих ограничения на распространение, а также модификацию и удаление информации.

В данной системе должны использоваться комплексные модели, обеспечивающие многоаспектное представление информации об объектах и процессах.

$$CXM = <P^{(1)}, I, E, I^E, R, P^{(2)}, Eval, Valid>,$$

где $P^{(1)}$ – первичные параметры объекта, E – информация о компонентах (подсистемах), составляющих объект, I – информация об интерфейсах моделируемого объекта, I^E – информация об интерфейсах компонентов (подсистем), R – коммутационное пространство, $P^{(2)}$ – вторичные параметры объекта, *Eval* – правила вычисления вторичных параметров объекта, *Valid* – правила валидации объекта.

Разработка и внедрение данных моделей и алгоритмов является возможность использования на всех этапах жизненного цикла: от требований к будущему продукту научно-технической информации или авторской задумки, до распространения информационного продукта и мониторинга его востребованности и оценки влияния (индекс цитирования).

Список используемых источников

1. Алехина Г. В., Петрик Е. А. Мировые информационные ресурсы М. : Москва, 2004. 52 с.

2. Верхова Г. В., Акимов С. В. Технологии виртуальных предприятий в формировании единой научно-образовательной киберсреды // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2017. Сборник материалов XIII Международной научно-технической конференции. 2017. С. 105–107.

УДК 004.75

УНИФИЦИРОВАННАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА СЕНСОРНОГО СЛОЯ ДЛЯ IIoT

Г. В. Верхова, Я. А. Плетнев

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

Представлены результаты исследований в области создания концепции программно-аппаратной платформы сенсорного слоя для промышленного интернета вещей. Целью создания программно-аппаратной платформы является унификация взаимодействия датчиков физических величин в рамках сенсорного слоя единой киберсреды постиндустриального общества. Показана возможность использования технологии виртуальных предприятий для создания инфраструктуры интернета вещей. Представлены варианты использования технологии для мониторинга любых техногенных объектов, как промышленных, так и бытовых.

интернет вещей, датчики, инфраструктура IIoT, мониторинг.

В 2017 г. распоряжением Правительства РФ была утверждена программа «Цифровая экономика Российской Федерации» [1] (далее – Программа), реализация которой осуществляется в соответствии с целями и задачами государственной политики РФ. Указывается, что данные в цифровой форме являются ключевым фактором производства и они обеспечивают экономический рост и повышают конкурентоспособность страны, качество жизни граждан. Данный документ предполагает развитие промышленных сенсоров (увеличение объема их использования) и также промышленного интернета.

Согласно Программе, ко второму кварталу 2019 г. будут разработаны проекты стандартов и технических регламентов, регулирующих сферу интернета вещей (индустриального интернета).

Увеличение использования датчиков физических величин также обуславливается вступившим в силу 1 марта 2017 г. приказа Министерства здравоохранения РФ № 646н «Об утверждении Правил надлежащей практики хранения и перевозки лекарственных препаратов для медицинского

применения», в котором говорится о необходимости ведения учета температуры и влажности как помещения в целом, так и его отдельных зон [2].

Настоящая нормативно-правовая база Российской Федерации изменяется таким образом, что использование большего числа датчиков переходит из зоны привилегий в зону обязанностей каждой организации. Предприятия для сохранения конкурентоспособности будут вынуждены переходить к Индустрии 4.0 (рис. 1).

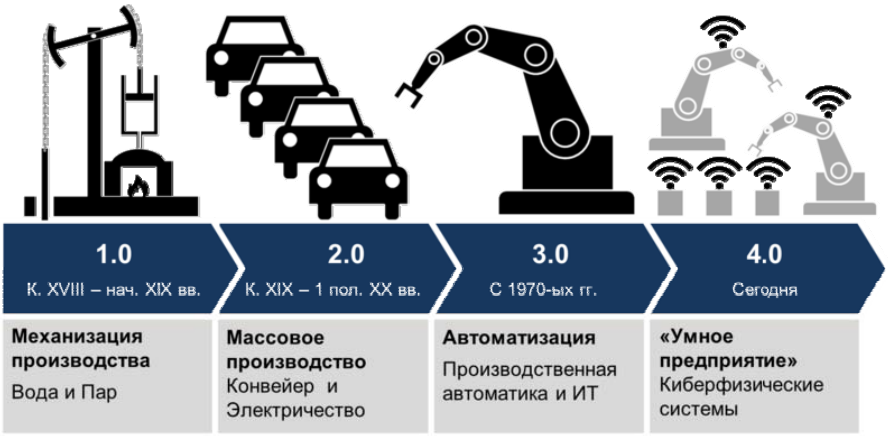


Рис. 1 Хронология промышленных революций

В настоящее время остро стоит проблема стандартизации взаимодействия датчиков различных физических величин. Изменяющаяся правовая система Российской Федерации диктует такие условия, в рамках которых организациям приходится наращивать количество оборудования мониторинга и контроля, начиная с различного рода вычислительных сетей (серверных кластеров) и заканчивая вышеупомянутыми датчиками, а это дополнительные расходы. Однажды вложив порой немалые средства в решение той или иной компании – закупка и установка контроллеров и датчиков – становятся «заложниками» данной структуры. В данном случае создается некая конкурентная монополия, в которой датчики одной фирмы-производителя могут работать только с контроллерами датчиков этой же фирмы.

Переходя от IIoT к рынку IoT, можно наблюдать схожую ситуацию. В настоящее время не существует комплексного решения данной проблемы. Существующее разнообразие доступных в ценовом отношении рядовому пользователю датчиков, устройств системы «умный дом» и других приборов «интернета вещей» пугает своим количеством и бессистемностью. Отсутствие единой «шины» с принципом работы «Plug&Play» во многом ограничивает стремление и желание заказчиков – как отдельных пользователей, так и различных предприятий – в приобретении и установке систем данного класса.

Решением этой проблемы будет создание единой платформы, которая позволяла бы пользователям использовать преимущества как IoT, так и IIoT без больших затрат и высокого порога вхождения.

Предлагается использовать магистрально-модульный принцип построения с возможностью использования принципа работы «Plug&Play». Необходимо также отметить, что в целях наибольшего удобства для конечного пользователя предлагается произвести интеграцию в киберсреду виртуальных предприятий [3] – веб-ресурс, в состав которого входит личный кабинет пользователя, возможность установления связи датчиков со структурным подразделением и, в свою очередь, подразделения с должностными лицами, имеющими авторизованный доступ.

На ресурсе обеспечивается процесс верификации и аутентификации пользователя. После успешной авторизации пользователю будет доступен личный кабинет с информацией в числовом либо графическом представлении со всех подключенных к его аккаунту датчиков, о состоянии отдельных аудиторий, о производственных помещений, о различных транспортных средствах (рис. 2).

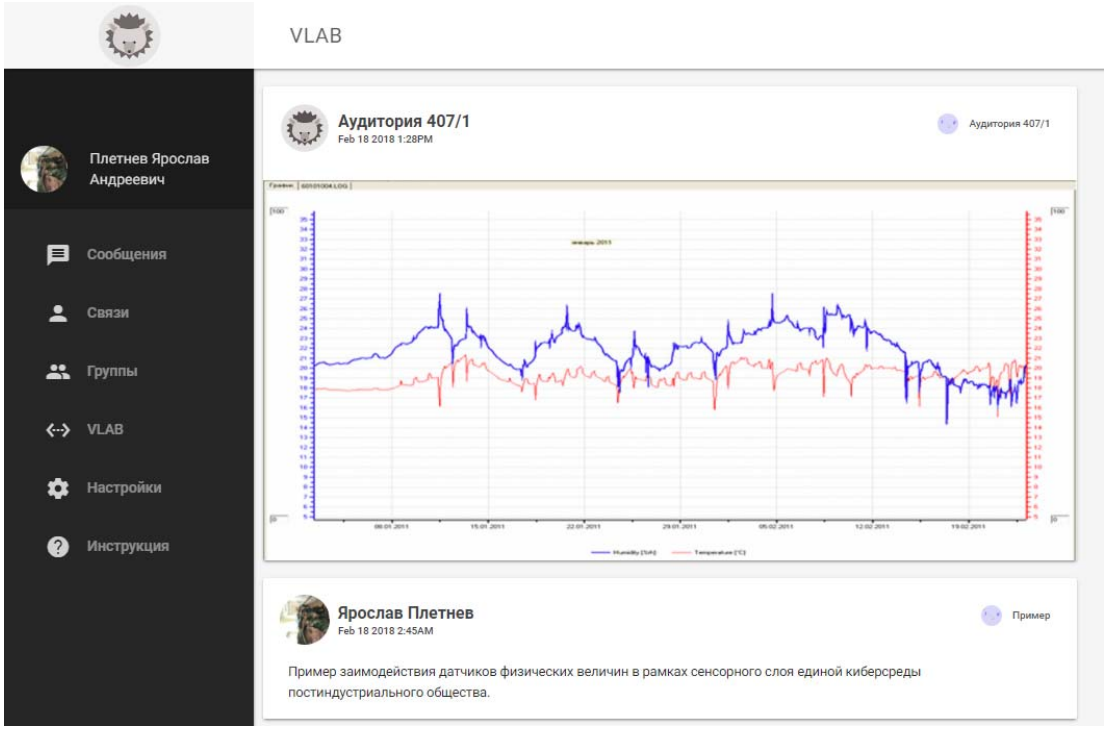


Рис. 2. Система мониторинга

В настоящий момент на кафедре «Автоматизации предприятий связи» разработан действующий прототип унифицированной программно-аппаратной платформы сенсорного слоя с интеграцией в киберсреду виртуальных предприятий. В данной системе реализованы основные функции мониторинга и контроля показаний датчиков через веб-интерфейс:

– установление связи датчиков с помещением, за которым ведется контроль;

– установление связи помещения с определенным физическим или юридическим лицом, либо группой лиц;

– разграничение прав доступа к добавлению, редактированию, удалению различной информации.

Контроллер обработки и передачи данных, поступающих на его вход с датчиков физических величин, программируется на язык с С-подобным синтаксисом. Система киберсреды виртуальных предприятий написана на языке программирования C# в рамка технологии ASP.NET.

Аппаратная основа устройства-прототипа приема и последующей передачи данных состоит из платформы NodeMCU с микроконтроллером ESP8266 с поддержкой передачи данных через сети WI-FI.

Внедрение предлагаемых технологий обеспечит быстрое и удобное развертывание системы мониторинга и контроля, возможность использования датчиков различных производителей в единой связке, возможность получения данных в режиме реального времени через удобный веб-интерфейс.

Список используемых источников

1. Об утверждении программы «Цифровая экономика Российской Федерации»: Распоряжение Правительства РФ от 28.07.2017 N 1632-р. Собрание законодательства Российской Федерации. 2017. N 32, ст. 5138.

2. Об утверждении Правил надлежащей практики хранения и перевозки лекарственных препаратов для медицинского применения: Приказ Министерства здравоохранения РФ от 31 августа 2016 г. № 646н. Электронные текстовые данные. URL: https://www.garant.ru/products/ipo/prime/doc/71482808/ (дата обращения 22.03.2018).

3. Акимов С. В., Верхова Г. В. Формирование киберсреды виртуальных предприятий // Информация и космос. 2016. № 4. С. 89–95.

УДК 004.946

ЭЛЕКТРОННЫЕ ФОРМЫ КОММУНИКАЦИИ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ НА БАЗЕ КИБЕРСРЕДЫ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ

Г. В. Верхова, К. А. Фролова

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

Рассмотрена проблема информатизации общеобразовательных учреждений Санкт-Петербурга. Выявлены недостатки существующих ресурсов, обеспечивающих

коммуникацию между учениками, учителями и родителями. Предложены пути эволюции таких систем с целью развития современных образовательных процессов.

общеобразовательные учреждения, электронное обучение, киберсреда, дистанционное обучение, социальная сеть.

В связи с развитием цифровой экономики в Российской Федерации возникла проблема информатизации всех сфер деятельности, включая общее и высшее образование. Появилась потребность в разработке технологий, обеспечивающих модификацию педагогических процессов общего и среднего образования на основе внедрения инфокоммуникационных технологий.

Правовую основу информатизации средней школы составляют Конституция Российской Федерации, Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации», Программа «Цифровая экономика Российской Федерации» [1], «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» [2]. В «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» для области образования обозначена необходимость формирования информационного пространства знаний, включая развитие различных образовательных технологий (дистанционное и электронное обучение) при реализации образовательных программ [2]. Одной из основных задач применения информационных и коммуникационных технологий для развития социальной сферы является создание различных технологических платформ для дистанционного обучения в целях повышения доступности качественных образовательных услуг [2].

Основным электронным ресурсом для образовательных учреждений Санкт-Петербурга является государственная информационная система «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», которая была создана согласно постановлению Правительства Санкт-Петербурга от 23.06.2011 N 802 «О создании государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» [3]. Данная система состоит из нескольких подсистем, особое место среди которых занимают подсистема «Портал «Петербургское образование» и подсистема «Параграф».

Подсистема «Портал «Петербургское образование» [URL: http://www.petersburgedu.ru] предназначена для предоставления пользователям доступа к сведениям об образовательных учреждениях Санкт-Петербурга и интерактивным возможностям ресурса. В её состав входят сервис «Электронный дневник», который состоит из элементов «Доступ к успеваемости», «Электронное портфолио», «Электронное домашнее за-

дание», «Социальное общение», и сервис «Мультимедиаинструменты образования», который, в свою очередь, состоит из элементов «Вебтрансляция открытых уроков» и «Поддержка видеоконференций».

Подсистема «Параграф» предназначена для хранения данных об образовательных учреждениях Санкт-Петербурга, обучающихся в образовательных учреждениях Санкт-Петербурга и педагогических кадрах образовательных учреждений Санкт-Петербурга, а также их автоматической передачи в другие подсистемы.

Несмотря на широкое распространение, «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» имеет ряд недостатков, среди которых:

– сложность установки, настройки и обслуживания подсистем для учителей и операторов, отвечающих за выгрузку на портал (подсистема «Параграф»);

– необходимость обучения пользователей подсистем;

– большое количество действий для регистрации учащегося на портале (регистрация на сайте, оформление заявление от родителя, личное присутствие при передаче заявления с подтверждением личности, наличие очередей при передаче заявления, ожидание подтверждения регистрации);

– отсутствие возможности электронного и дистанционного обучения.

Другой популярной образовательной платформой является «Дневник.ру» [URL: http://www.dnevnik.ru]. Она предоставляет доступ к оценкам, расписанию и домашним заданиям, электронному обучению, зачислению в образовательные организации, является социальной сетью для коммуникации «педагог – учащийся – родитель». Система «Дневник.ру» также обладает недостатками, такими как сложность регистрации, нестабильность работы, отсутствие возможности полноценного электронного обучения, примитивный уровень имеющихся возможностей.

В рамках совершенствования системы образования в Санкт-Петербурге представляется необходимым создание единой образовательной киберсреды, призванной устранить существующие недостатки. Киберсреда базируется на трёх основных принципах: агентности, информационного самообслуживания и управляемой информационной открытости [4, 5]. Киберсреда имеет развитые возможности гибкого управления информационными связями между участниками с учётом типа отношений, что особенно актуально для инфокоммуникационных систем общеобразовательных организаций, так как обеспечивает адаптивные механизмы управления доступом к информации на основе отношений между участниками, а также доступные в системе действия.

В среде должны быть реализованы коммуникационные, контрольные и образовательные сервисы, которые могут быть реализованы в виде следующих подсистем: учёта, образовательных ресурсов и коммуникаций.

Подсистема учёта включает в себя важнейшие функции для контроля успеваемости и организации занятий, такие как электронный дневник с оценками, электронное расписание, электронное домашнее задание.

Подсистема образовательных ресурсов состоит из электронной библиотеки методических материалов, аудио-, видеофайлов, презентаций по пройденным материалам дисциплин, электронные тесты, самостоятельные, контрольные и лабораторные работы для выполнения как удалённо, так и во время проведения практических и лабораторных занятий по дисциплинам.

Коммуникационная подсистема имеет сходства с социальными сетями, так как служит для обеспечения интерактивного общения между учениками, учителями и родителями в любых сочетаниях, но в отличие от социальных сетей содержит развитые средства анализа отношений между участниками, которые учитываются при управлении правами доступа и реализации специальных функций. Коммуникационная система предоставляет возможность участия в диалогах, конференциях, создания и ведения личных блогов, групп, просмотра новостей предстоящих событий, формирования портфолио (для учителей и учащихся), в котором аккумулируются достижения на протяжении всего периода обучения/педагогической деятельности (грамоты, дипломы, поощрения, результаты творчества, избранные сочинения, рефераты, публикации).

В новой системе предлагается упростить порядок регистрации по сравнению с описанной внедрённой в общеобразовательные учреждения Санкт-Петербурга системой «Портал «Петербургское образование». Предложенный электронный ресурс базируется на технологии, обеспечивающей независимую регистрацию участников. Установление связей реализуется по запросу с последующим подтверждением, что является аналогом формирования и подписания заявления для регистрации без личного присутствия и трудоёмкого заполнения необходимых полей. Учёт типов связей между участниками гарантирует целостность связей и предотвращение удаления связей, необходимых для функционирования системы (так, ученик не может самостоятельно удалить связь между классом, в котором он учится, и родителями).

Внедрение электронных форм коммуникации в общеобразовательные организации на базе киберсреды виртуальных предприятий обеспечит:

– развитие единого образовательного пространства в Российской Федерации;

– тиражирование лучших педагогических практик;

– интерактивную коммуникацию «учитель – ученик – родитель» для общеобразовательных учреждений;

– содействие построению цифровой экономики в Российской Федерации;

– снижение цифрового неравенства и повышение цифровой грамотности граждан;

– развитие информационного общества;

– содействие в реализации основных видов государственных услуг в электронном виде.

Список используемых источников

1. Об утверждении программы «Цифровая экономика Российской Федерации»: Распоряжение Правительства РФ от 28.07.2017 N 1632-р. Собрание законодательства Российской Федерации. 2017. N 32, ст. 5138.

2. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 N 203. Собрание законодательства Российской Федерации. 2017. N 20, ст. 2901.

3. О создании государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»: Постановление Правительства Санкт-Петербурга от 23.06.2011 N 802. Электронные текстовые данные. 2011. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SPB&n=149728#04801715007750169 (дата обращения: 23.02.2018).

4. Верхова Г. В., Акимов С. В., Гусев А. Н. Информационная среда подготовки высококвалифицированных кадров в системе непрерывного образования // Планирование и обеспечение подготовки кадров для промышленно-экономического комплекса региона. 2017. Т. 1. С. 85–88.

5. Акимов С. В., Верхова Г. В. Формирование киберсреды виртуальных предприятий // Информация и космос. 2016. № 4. С. 89–95.

УДК 53.087

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИНФРАКРАСНЫХ СИСТЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Ю. Н. Виноградов, В. А. Рогачёв

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

Для измерения параметров инфракрасных систем спроектирована и разработана компьютерная система. Назначение этой системы – измерение характеристик инфракрасных систем. Система построена на микрокомпьютере «Raspberry Pi» и инфракрасной CSI камере. Произведено измерение некоторых характеристик системы.

инфракрасные системы, микрокомпьютер «Raspberry Pi», инфракрасная CSI камера.

Инфракрасные (ИК) системы – способны обеспечить наблюдение объектов в темноте. В зависимости от температуры наблюдаемого объекта выделяют ближний ИК диапазон (сильно нагретые объекты) и средний диапазон (слабо нагретые объекты). Область применения ИК систем весьма широка [1, 2, 3, 4]:

1. Приборы ночного видения.
2. Термография.
3. Инфракрасное самонаведение.
4. Инфракрасный обогрев.
5. Инфракрасная астрономия.
6. Инфракрасная спектроскопия.
7. Передача данных.
8. Дистанционное управление.
9. Медицина.
10. Стерилизация пищевых продуктов.
11. Пищевая промышленность.
12. Проверка денег на подлинность.

Для оптимального применения ИК систем, необходимо знать их основные характеристики [5, 6, 7, 8]:

1. Чувствительность.
2. Спектральная характеристика чувствительности.
3. Пороговая чувствительность.
4. С.к.о. шума.
5. Переходная характеристика.
6. Энергетическая характеристика фототока.
7. Люксамперная характеристика.
8. Динамический диапазон.
9. Неравномерность чувствительности.

Для обеспечения точности, гибкости измерений, а также их мобильности был выбран микрокомпьютер «Raspberry Pi» – одноплатный компьютер размером с банковскую карту (рис. 1). На него была установлена операционная система, Rasbian, основанная на Linux ядре.

Рис. 1. Микрокомпьютер Raspberry Pi 3B

Рис. 2. Камера OV5647 с ИК подсветкой

Получение изображения осуществлялось с помощью CSI камеры OV5647 (рис. 2).

Параметры:

1. OV5647 датчик.
2. Разрешение 5 мегапикселей.
3. Объектив: 1/4 5 м.
4. Размер CCD: 1/4 дюйма.
5. Диафрагма (f): 1.8.
6. Фокусное расстояние: 3.6 мм регулируется.
7. Угол диагонали: 60 градусов.
8. Максимальное разрешение сенсора: 1080 P.
9. Питание (3,3 В выход).

В качестве источника излучения был использован ИК-светодиод, оборудованный светочувствительным датчиком (рис. 3). Интенсивность излучения может изменяться.

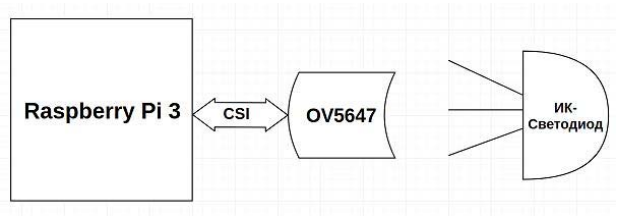


Рис. 3. Структурная схема ИК-системы на базе Raspberry Pi

Параметры:

1. Длина волны: 940 нм.
2. Напряжение питания: 3,3–5 В.
3. Угол излучения: 30°.

С помощью светофильтра ИКС3 был отсечен видимый диапазон (только ИК), как показано на рис. 4.

Рис. 4. Полученные изображения с светофильтром ИКС3 на расстоянии 3 и 1 метр

Полученные изображения были проанализированы: выделена строка с сигналом, рассчитана амплитуда сигнала, дисперсия и т. д.

Таким образом, выполнение данной работе позволило получить следующие результаты (рис. 5):

1. Спроектирована и реализована инфракрасная система на основе микрокомпьютера Raspberry Pi.

2. С помощью CSI инфракрасной камеры OV5647 получены изображения на различных дальностях и произведена оценка их характеристик.

3. Созданная система служит основой для развития комплекса оценки характеристик фотоприемников.

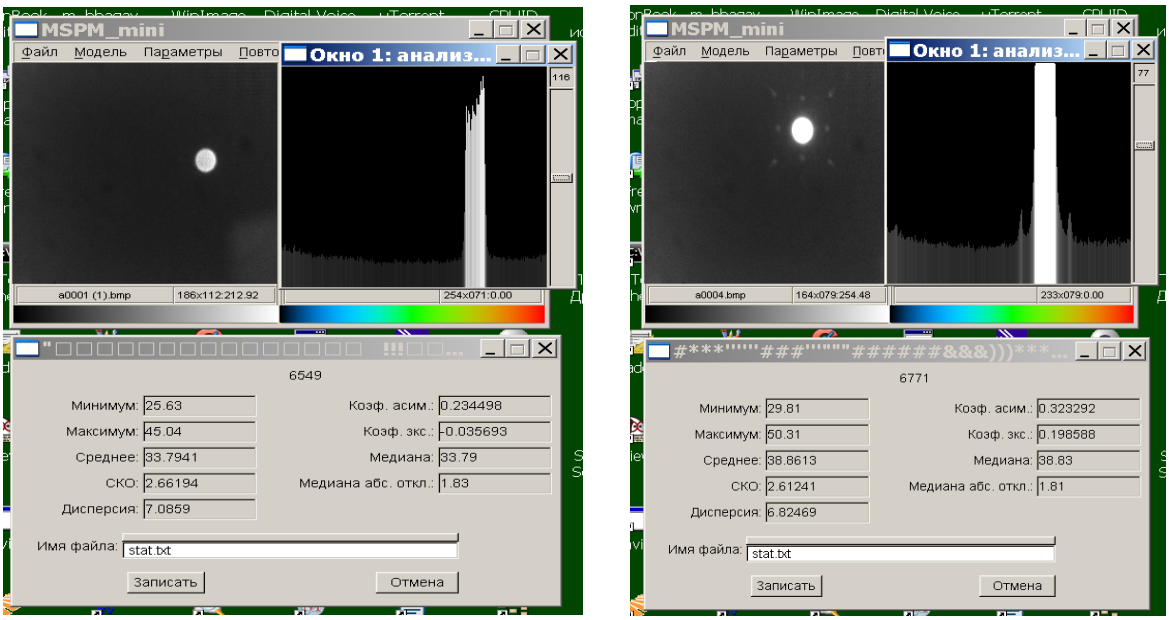


Рис. 5. Результаты программной обработки полученных изображений

Список используемых источников

1. Ллойд Дж. Системы тепловидения: пер. с англ. под редакцией А. И. Горячева. М. : Мир, 1978. 414 с.

2. Хадсон Р. Инракрасные системы. М. : Мир. 1972. 536 с.

3. Козелкин В. В., Усольцев И. Ф. Основы инфракрасной техники. М. : Машиностроение. 1967. 308 с.

4. Богомолов П. А., Сидоров В. И., Усольцев И. Ф. Приемные устройства ИК-систем. М. : Радио и связь. 1987. 208 с.

5. ГОСТ-21934-83 Приемники излучения полупроводниковые фотоэлектрические и фотоприемные устройства. Термины и определения. М. : Стандартинформ, 2005. 170 с.

6. Ишанин Г. Г., Панков Э. Д. Источники и приемники излучения. СПб. : Политехника. 1991. 240 с.

7. Ткаченко А. П., Кириллов В. И. Техника телевизионных измерений. Минск : Высшая школа. 1976. 224 с.

8. Васильченко Н. В. И др. Измерение параметров приемников оптического излучения. Ь. Радио и связь. 1983. 320 с.

УДК 004.415.25

АРХИТЕКТУРА МАКЕТА СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО КОНТРОЛЮ СОСТОЯНИЯ И УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ СЕТИ СВЯЗИ И ПРИМЕНЯЕМЫЕ ПРОГРАММНЫЕ ТЕХНОЛОГИИ НА ЯЗЫКЕ JAVA

М. Ю. Винокуров, Д. Д. Корякин

Военная академия связи имени Маршала Советского Союза С. М. Буденого

В настоящее время вооруженные силы активно развивает направление по автоматизации контроля состояния и управления узлами в различных распределенных технических системах. Организация структуры и внутренней иерархии узлов в подобных системах (например, полевой транспортной сети связи) представляет собой сложную задачу построения системы, комплекса систем, и возникает необходимость в реализации отзывчивого графического интерфейса в виде информационной системы для эффективного управления таким комплексом. Предлагается реализация такого графического интерфейса в виде веб-приложения, на базе сервис-ориентированной архитектуры.

сервис-ориентированная архитектура, веб-приложение, Vaadin, Spring.

Сервис-ориентированная архитектура

Сервис-ориентированная архитектура (СОА) — модульный подход к разработке программного обеспечения, основанный на использовании распределённых, слабо связанных заменяемых компонентов, оснащённых стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам. Программные комплексы, разработанные в соответствии с сервис-ориентированной архитектурой, обычно реализуются как набор веб-служб, взаимодействующих по протоколу SOAP, но существуют и другие реализации (например, на базе CORBA, на основе REST). Интерфейсы компонентов в сервис-ориентированной архитектуре инкапсулируют детали реализации (операционную систему, платформу, язык программирования) от остальных компонентов, таким образом обеспечивая комбинирование и многократное использование компонентов для построения сложных распределённых программных комплексов, обеспечивая независимость от используемых платформ и инструментов разработки, способствуя масштабируемости и управляемости создаваемых систем [1].

Сервис-ориентированная архитектура позволит, во-первых, создать систему, эффективно масштабируемую, во-вторых, позволит этой системе эффективно справлять с большим числом пользовательских запросов за счет распределения нагрузки.

Язык программирования Java для создания информационных систем на базе СОА

Информационная система на базе сервис-ориентированной архитектуры состоит из сервисов, инкапсулирующих детали реализации. Для реализации графического интерфейса и высокоуровневой работы с источниками данных предлагается использовать фреймворки Vaadin и Spring, предназначенные для использования в информационных системах, реализованных с помощью языка программирования Java. Выбор данного языка программирования основывается на его отличительных характеристиках [2]:

1) Технология Java позволяет работать в безопасной вычислительной среде, изолированной виртуальной машине – JVM.

2) Кроссплатформенность.

3) Создание программ, работающих в веб-браузере и имеющих доступ к веб-службам.

4) Объединение приложений или служб с использованием языка Java для создания высокоспециализированных приложений или служб.

5) Создание многофункциональных и эффективных приложений для мобильных телефонов, удаленных процессоров, микроконтроллеров, беспроводных модулей, датчиков, шлюзов, потребительских продуктов.

6) Поддержка лямбд, замыканий, встроенные возможности функционального программирования.

7) Множество вариантов реализации многопоточных программ.

Таким образом, язык Java позволяет реализовывать платформ-независимые сервисы, реализовывать интерфейсы различных типов и для различных устройств, объединять различные программные интерфейсы, эффективно обрабатывать данные.

Фреймворк Vaadin для создания графического интерфейса информационной системы

Специальное программное обеспечение по контролю состояния и управления оборудованием сети связи подразумевает функциональный графический интерфейс. Предлагается реализовать этот интерфейс в виде веб-приложения, доступного через браузер. Такой интерфейс позволит пользователям обращаться к информационной системе без необходимости установки специфических программных средств, и избавит его от необхо-

димости следить за своевременным обновлением установленного программного комплекса. Для реализации графического интерфейса системы предлагается использовать фреймворк Vaadin.

Vaadin – свободно распространяемый фреймворк для создания RIA-веб-приложений, разрабатываемый одноимённой финской компанией. В отличие от библиотек на Javascript и специфических плагинов для браузеров, Vaadin предлагает сервер-ориентированную архитектуру, базирующуюся на Java Enterprise Edition. Использование JEE позволяет выполнять основную часть логики приложения на стороне сервера, тогда как технология AJAX, используемая на стороне браузера, позволяет интерактивно взаимодействовать с пользователем, не отставая от аналогичных десктоп-приложений. Для отображения элементов пользовательского интерфейса и взаимодействия с сервером на стороне клиента Vaadin использует Google Web Toolkit [3]. Архитектура фреймворка Vaadin представлена на рис.

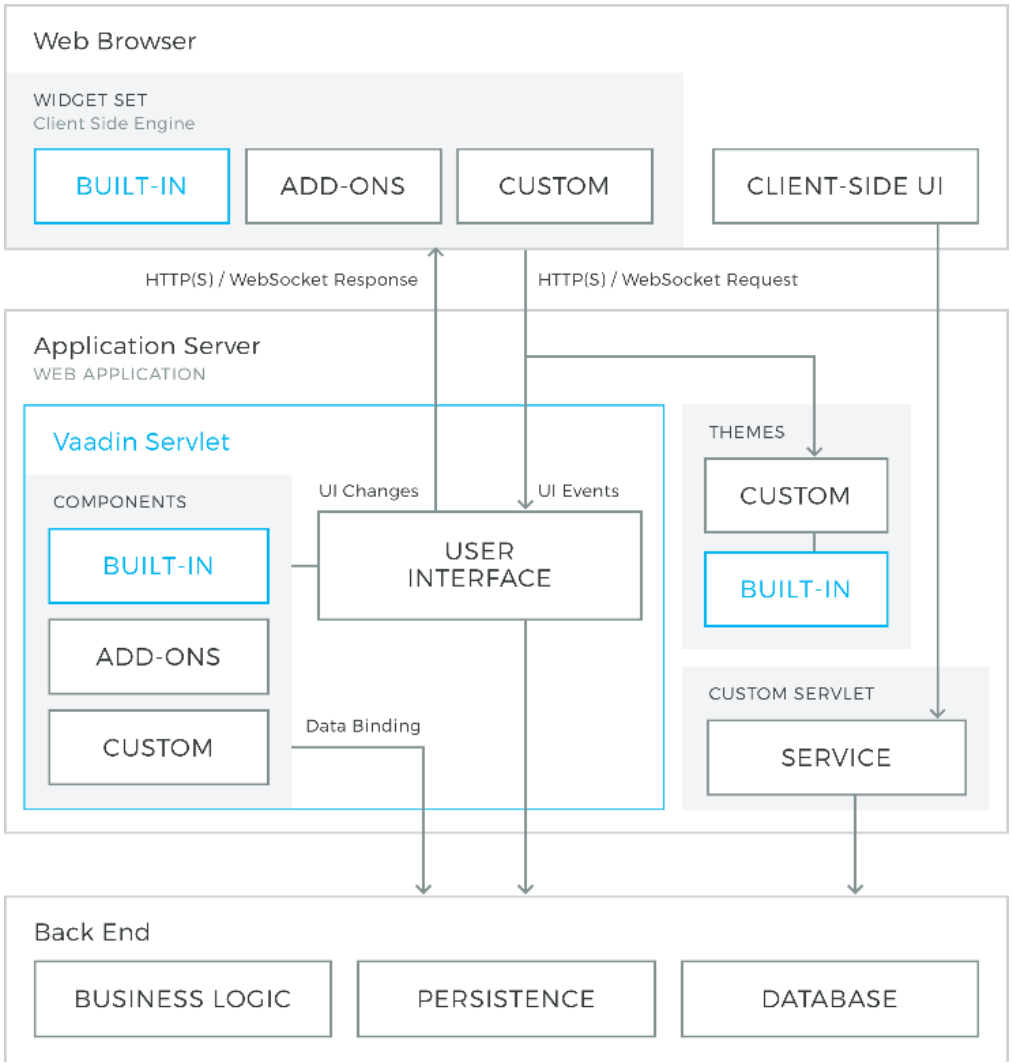


Рисунок. Архитектура фреймворка Vaadin [3]

Использование Java как единственного языка программирования при создании веб-приложений и веб-контента – одна из наиболее значимых функций в Vaadin. Фреймворк использует событийную модель и определенные элементы пользовательского интерфейса, виджеты, что делает её очень близкой к модели разработки настольных приложений на Java с использованием HTML и Javascript.

Организация модели данных и виджетов позволяет отображать в браузере большие объёмы данных без значительной загрузки оперативной памяти и без дополнительных действий со стороны разработчика. Использование Google Web Toolkit для отображения страниц с результатами поиска и обработки действий пользователя (наподобие терминального клиента). Так как Google Web Toolkit функционирует только на стороне клиента, Vaadin добавляет дополнительную валидацию данных на стороне сервера: это решает проблемы безопасности, связанные с возможностью подмены данных или кода Javascript. Соответственно, при изменении и повреждении данных, поступающих от браузера, сервер, определив это, не пропускает запросы.

Расширяемость обеспечивается возможностью использования дополнительных виджетов, написанных для GWT, а также кастомизации при помощи CSS. Однако стандартное приложение, создаваемое на Vaadin, не требует программирования именно на GWT и последующей компиляции GWT-компилятором, если только разработчик не добавляет в проект нестандартные виджеты.

Фреймворк Spring для создания сервисов

Spring Framework (или коротко *Spring*) – универсальный фреймворк с открытым исходным кодом для Java-платформы. Spring может быть рассмотрен как коллекция меньших фреймворков или фреймворков во фреймворке. Большинство этих фреймворков может работать независимо друг от друга, однако они обеспечивают большую функциональность при совместном их использовании. Эти фреймворки делятся на структурные элементы типовых комплексных приложений [4]:

– Inversion of Control-контейнер: конфигурирование компонентов приложений и управление жизненным циклом Java-объектов.

– Фреймворк аспектно-ориентированного программирования: работает с функциональностью, которая не может быть реализована возможностями объектно-ориентированного программирования на Java без потерь.

– Фреймворк доступа к данным: работает с системами управления реляционными базами данных на Java-платформе, используя JDBC- и ORM-средства и обеспечивая решения задач, которые повторяются в большом числе Java-based environments.

– Фреймворк управления транзакциями: координация различных API управления транзакциями и инструментарий настраиваемого управления транзакциями для объектов Java.

– Фреймворк MVC: каркас, основанный на HTTP и сервлетах, предоставляющий множество возможностей для расширения и настройки.

– Фреймворк удалённого доступа: конфигурируемая передача Java-объектов через сеть в стиле RPC, поддерживающая RMI, CORBA, HTTP-based протоколы, включая web-сервисы (SOAP).

– Фреймворк аутентификации и авторизации: конфигурируемый инструментарий процессов аутентификации и авторизации, поддерживающий много популярных и ставших индустриальными стандартами протоколов, инструментов, практик через дочерний проект Spring Security (ранее известный как Acegi).

– Фреймворк удалённого управления: конфигурируемое представление и управление Java-объектами для локальной или удалённой конфигурации с помощью JMX.

– Фреймворк работы с сообщениями: конфигурируемая регистрация объектов-слушателей сообщений для прозрачной обработки сообщений из очереди сообщений с помощью JMS, улучшенная отправка сообщений по стандарту JMS API.

– Тестирование: каркас, поддерживающий классы для написания модульных и интеграционных тестов.

Потенциал представленных фреймворков удовлетворяет созданию сложной распределенной системы, а информационная база их сообществ позволяет максимально использовать возможности этих фреймворков.

Список используемых источников

1. Сервис-ориентированная архитектура. URL: https://ru.wikipedia.org/wiki/Сервис-ориентированная_архитектура (дата обращения: 06.02.2018).

2. Java. URL: https://ru.wikipedia.org/wiki/Java (дата обращения: 06.02.2018).

3. Введение в Vaadin. URL: https://vaadin.com/docs/v8/framework/introduction/intro-overview.html (дата обращения: 06.02.2018).

4. Spring Framework. URL: https://ru.wikipedia.org/wiki/Spring_Framework (дата обращения: 06.02.2018).

Статья представлена доцентом кафедры организации связи ВАС, кандидатом военных наук В. Г. Ивановым.

УДК 004.056

КОНВЕРГЕНЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ САНКТ-ПЕТЕРБУРГА

Л. А. Виткова, Е. Ю. Герлинг, Ю. А. Головлёва, М. М. Ковцур

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

В данной статье рассматривается трансформация понятия «конвергенция информационных технологий», а также вопросы повышения эффективности управления информационным пространством, теории управления рисками информационной безопасности и некоторые аспекты оптимизации в системах управления ИБ, а именно: оперативность, ресурсоёмкость и обоснованность процессов оптимизации.

конвергенция информационных технологий, управление информационным пространством, система управления информационной безопасностью.

Понятие «конвергенция» широко распространено и употребляется во множестве наук. Оно означает процесс сближения или слияния каких-либо независимых друг от друга признаков, элементов или объектов.

В сфере инфокоммуникационных технологий конвергенция – это взаимное влияние и взаимопроникновение технологий, междисциплинарная работа на стыке областей и в результате получение новых, усовершенствованных технологий.

В сетях связи рассматривается три аспекта конвергенции [1, С. 132–134.]:

1) конвергенция услуг обеспечивает новые расширенные функциональные возможности для пользователей;

2) конвергенция процессов позволяет провайдерам услуг работать с оборудованием различных производителей и различными технологиями с тем, чтобы предлагать экономически эффективные услуги;

3) конвергенция сетей означает конвергенцию технологий, которая определяет возможность конвергенции различных сетевых услуг.

Конвергенцию можно рассмотреть на примере технологии NGN (*new generation networks* – сети нового поколения), которая подразумевает трансформацию традиционных сетей с коммутацией каналов в сети с коммутацией пакетов.

В начале XXI века телефонная сеть общего пользования (ТфОП), сеть подвижной связи (СПС) и сеть передачи данных (СПД) являлись тремя разными объектами. Средняя часть рис. 1 отражает фазу конвергенции сетей за счет пересечения трех эллипсов, которые соответствуют ТфОП, СПС и СПД. Результатом процесса конвергенции является практически полное объединение сетей – правая часть рис. 1. В итоге формируется сеть нового поколения [2].

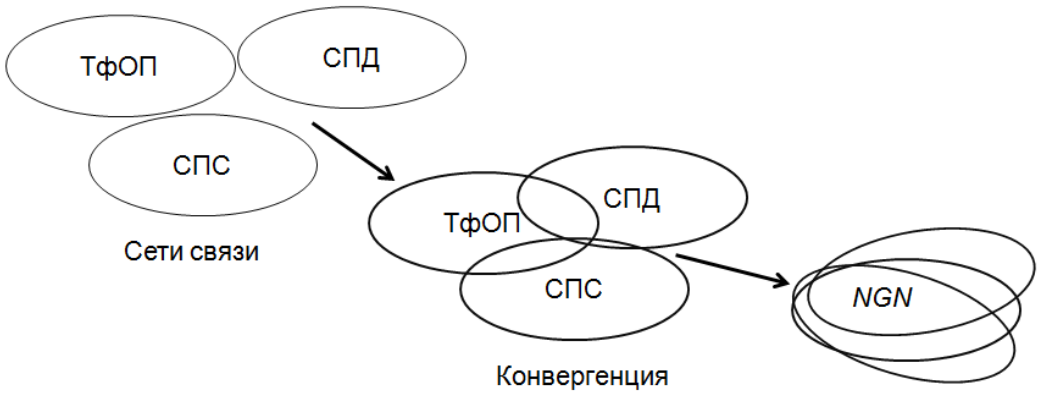


Рис. 1. Эволюция сетей связи

В информационном пространстве города конвергенцию следует рассматривать с точки зрения безопасности.

В городе существуют различные физические организации, у которых нет общего обмена информацией. Рассмотрим пример на рис. 2.

Есть данные, которые предоставляют операторы связи (ОС), операторы сетей передачи данных (СПД), аналитический центр (АЦ), данные систем пожаротушения в государственных учреждениях (ПТ), данные от транспортных служб (ТС).

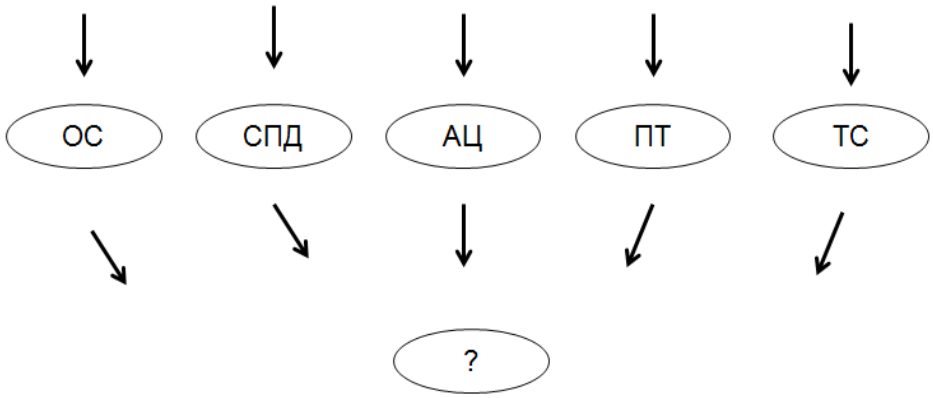


Рис. 2. Информационное пространство города

В данном случае конвергенция – это объединение технологических решений, принимаемых в разных организациях.

Информационная безопасность начинается с анализа рисков, в котором существует три основных понятия: риск, вероятность реализации и уязвимость.

Уязвимость – это брешь в системе безопасности. Вероятность реализации – вероятность того, что данная уязвимость будет эксплуатирована для реализации риска. Риск – это возможность понести какие-либо потери в связи с реализацией уязвимости.

Вся работа по управлению рисками сводится либо к снижению вероятности реализации, либо к минимизации потерь от реализации. Соответственно риски могут быть приемлемыми и неприемлемыми [3].

Следующим этапом являются аспекты оптимизации в системах управления ИБ – это: оперативность, ресурсоёмкость и обоснованность.

При объединении нескольких систем в одну увеличивается оперативность: оповещение о той или иной угрозе можно приходит раньше. Ресурсоёмкость уменьшается: потребуется один центр обработки данных вместо пяти. Однако затраты на эти решения могут превышать затраты на угрозы или потери.

Если угрозой является чрезвычайная ситуация или катастрофа, то выигрыш во времени приводит к экономии на возможных потерях – человеческих или экономических. Однако, если угроза – это, например, недоступность какой-либо информации (ИБ должна обеспечивать доступность информации), то траты на решения будут необоснованными.

Поэтому при разработке решений для конвергенция информационных технологий в информационном пространстве города в первую очередь нужно учитывать аспекты оптимизации систем управления ИБ, и главное – обоснованность.

Список используемых источников

1. Кох Р., Яновский Г. Г. Эволюция и конвергенция в электросвязи. М. : Радио и связь, 2001. 280 с.

2. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: учебник для вузов. СПб. : БХВ–Санкт-Петербург, 2010. 400 с.

3. Живетин В. Б. Введение в анализ риска: учебное пособие. М. : Институт проблем риска, ООО Информационно-издательский центр «Бон Анца», 2008. 288 с. ISBN 978-5-98664-036-5, 978-5-903140-13-8.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК004.056.5

ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Л. А. Виткова, М. Н. Дудникова, А. Е. Петрова

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

На данный момент существуют устоявшиеся методики технической защиты, но современные госты по менеджменту в информационной безопасности не решают текущие задачи. В данной статье авторы рассмотрят необходимость обновление методик для управления информационной безопасности и использование процессного подхода.

информационная безопасность, система управления информационной безопасности, политика безопасности.

В настоящее время информация представляет собой один из самых главных бизнес-активов любой организации, имеющим ценность для организации, находящимся в ее распоряжении и обеспечивающим добавочную стоимость и вследствие этого нуждающимся в защите. Вовремя не устраненные и известные злоумышленникам уязвимости в обеспечении ИБ могут привести к катастрофическим финансовым потерям и нанести непоправимый ущерб бизнес-процессам. Поэтому вопрос разработки эффективной СУИБ и ее квалифицированного внедрения и использования сегодня актуален как никогда прежде.

Для начала стоит определить, что под информационной безопасностью (ИБ) понимается следующее [1]:

1) Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

2) Механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации.

3) Свойство информации сохранять конфиденциальность, целостность и доступность.

Таким образом, ИБ представляет главным образом, проблему управления, а обеспечение информационной безопасности (ОИБ) – это процесс поддержания состояния защищенности активов организации, который должен осуществляться постоянно и поэтому им необходимо управлять.

Для организации общий подход и намерения в области ОИБ, официально выраженные руководством, отражаются в разработанном, утвержденном им и строго выполняемом на практике всеми ее сотрудниками и бизнес-партнерами документе – политике ОИБ организации (политика ИБ). Политика ИБ определяет стратегию и тактику построения в организации системы защиты информации. Политика ИБ – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распространение ценной информации.

Политика ИБ делится на две категории: административная, выполняемая людьми, и техническая, реализуемая с помощью оборудования и программ.

Организационная или административная излагается в документах трех уровней. Документы верхнего уровня носят общий характер определяют политику ИБ для организации в целом. Второй уровень выделяют в случае структурной сложности организации или при необходимости обозначить специфические области деятельности, подразделения, технологии, подсистемы и т.п. Третий уровень относиться к конкретным службам или подразделениям организации и детализирует верхние уровни политики ИБ.

Техническая политика ИБ – это совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и аппаратным обеспечением ИС.

Политика ИБ только определяет, что должно быть защищено и какова ответственность в случае несоблюдения ее положений. Защитные меры определяют, как конкретно защитить активы организации. Они являются механизмом реализации ПолИБ на практике и представляют собой полный перечень всех рекомендаций и действий, которые должны предприниматься в определенных обстоятельствах и при определенных условиях.

Политика ИБ содержит общие требования по ОИБ организации в цело. При этом обязательно учитываются особенности организации и ее деятельности, а также выделяются основные направления, связанные с ОИБ организации, и формулируются общие требования по каждому из этих направлений. На рис. 1 изображен жизненный цикл политики ИБ.

Рис. 1. Жизненный цикл ПолИБ

Система управления информационной безопасности (СУИБ) часть общей системы управления организации, основанную на подходе оценки и анализа бизнес-рисков, предназначенную для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ, и включающий организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ.

На рис. 2 видно, что все документальное обеспечение СУИБ проходит несколько стадий жизненного цикла: начальная оценка необходимости разработки документа исходя из намеченных целей, собственно его разработка специально определенной группой лиц соответствующими полномочиями и предоставленными для этого ресурсами, утверждение уполномоченным лицом и установление дат его введения и пересмотра, публикации внутри организации, использование документа непосредственное исполнение его положений, сопровождение с последующим внесением изменений или изъятием из обращения после процедуры пересмотра. Если принято решение о внесении изменений и выпуске следующей редакции, то новый цикл традиционно начинается со стадии разработки [2].

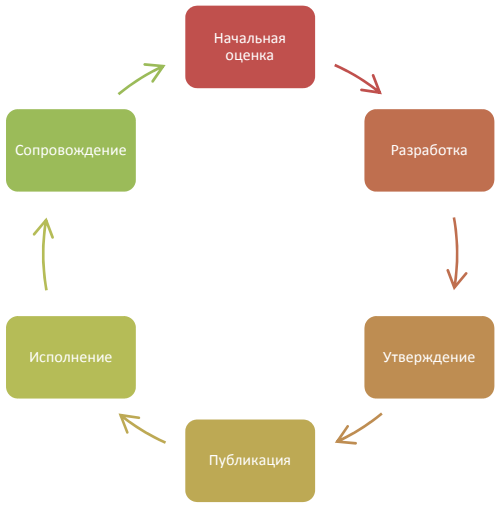


Рис. 2. Жизненный цикл документального обеспечения СУИБ

Чтобы функционировать эффективно, организация должна идентифицировать различные вида осуществляемой деятельности и управлять ими. Как было отмечено ранее, любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс [3].

К управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации.

СУИБ принимает в качестве входных данных требования по ОИБ и ожидания заинтересованных сторон и в результате ряда необходимых действий и процессов на выходе получается управляемая ИБ, которая удовлетворяет этим требованиям и ожиданиям. На рис. 3 изображен цикл процессного подхода СУИБ.

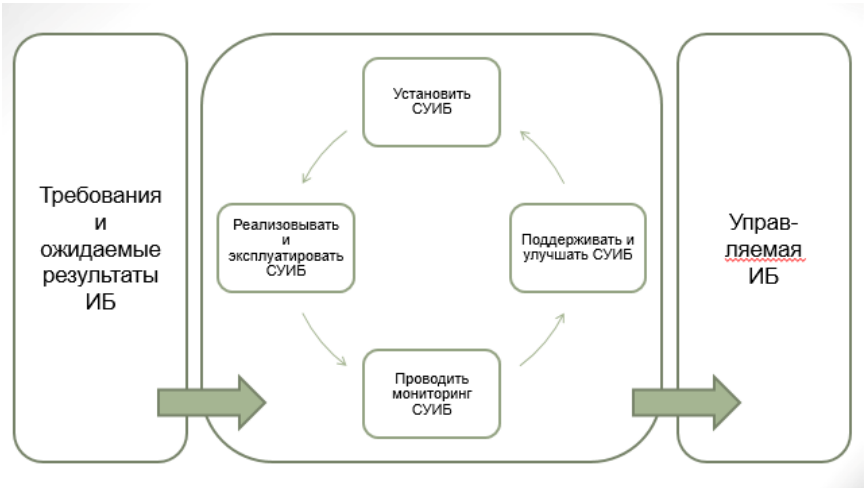


Рис. 3. Цикл PDCA в применении к процессам СУИБ

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски ИБ, предлогается соответвующий план обработки этих рисков.

На стадии реализации внедряются решения, принятые во время планирования.

На стадиях проверки и совершенствования усиливают, исправлют и совершенствуют решения СУИБ, которые были определены и уже реализованы.

Рассмотренные авторами выше основные вопросы управления информационной безопасностью, в настоящее время, требуют обновления применяемых методик. К примеру, использование процессного подхода для систем управления информационной безопасностью.

Список используемых источников

1. Курило Л. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Основы управления информационной безопасностью, 2-е изд., испр. М.: Горячая линия-Телеком, 2014. 244 с.

2. Голованов В. Б., Зефиров С. Л., Курило А. П. Аудит информационной безопасности. М. : БДЦ-Пресс, 2006. 305 с. ISBN: 5-93306-100-х.

3. Репин В., Елиферов В. Процессный подход управлению. Моделирование бизнес-процессов, М: Стандарты и качество, 2004. 405 с. ISBN 5-94938-028-2.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 65.011.56

ИССЛЕДОВАНИЕ И ОЦЕНКА УЯЗВМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БАНКИНГА ДЛЯ ФИЗИЧЕСКИХ ЛИЦ МЕТОДОМ ДЕЛЬФИ

Л. А. Виткова, М. Н. Дудникова, А. Н. Петрова

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

Развитие IT-технологий породило бесчисленное множество удобств, как для физических, так и для юридических лиц. Актуальность данной статьи обусловлена тем, что с ростом услуг, которые предоставляются через интернет, появился новый сектор экономики – электронная коммерция, частью которого является электронный банкинг. В данной статье анализируются существующие уязвимости, угрозы и методы защиты в сфере электронного банкинга.

информационная безопасность, угрозы, уязвимость, электронный банкинг.

Развитие IT-технологий ежедневно открывает новые возможности и горизонты для общества. Интернет стал универсальной средой, он предоставил возможность повышения качества и скорости взаимодействия как для физических, так и для юридических лиц. Число пользователей глобальной компьютерной сети стремительно растёт. На современном этапе развития науки и техники, информатизации различных областей жизни общества, появились новые технические возможности проведения денежных расчётов и взаимозачетов. В нынешних условиях коммерческие банки стремятся предоставлять своим клиентам усовершенствованные банковские услуги, которые связаны с электронными системами расчетов.

Актуальность данной статьи обусловлена тем, что количество сервисов и услуг растёт, глобальная сеть Интернет стала универсальной коммерческой средой, ежедневно между серверами банков, электронными сервисами и клиентами происходят миллиарды транзакций, ведется активная финансовая деятельность. Как следствие, появляются новые уязвимости и угрозы информационной безопасности в новом секторе экономики, в частности в электронной коммерции, частью которой является электронный банкинг. В сфере ЭБ существует и такая проблема, как не разработанность методических аспектов обеспечения информационной безопасности для физических лиц.

В сфере электронного банкинга наиболее уязвимыми для преступников являются такие формы бизнеса, как информационно-развлекательные сервисы, электронная коммерция, интернет-банкинг и онлайн-торговля. В кибермошенничестве под кражей понимается хищение и присвоение не материальных вещей или денег, а конфиденциальной информации, которая и наносит урон организации или человеку, а уже в дальнейшем, с помощью этой информации преступник может и украсть деньги [1, 2].

Сегодня в России угрозам информационной безопасности противостоят тысячи профессионалов, сотни компаний, государственные службы, банки, но халатность и не осведомленность пользователя сервисов наносит не меньший ущерб. Угрозы были и остаются одной из наиболее распространенных причин ущерба конфиденциальности, целостности и доступности информационных систем, и все же, несмотря на огромные усилия технического и экспертного сообщества, убытки, приносимые инцидентами информационной безопасности в электронном банкинге, продолжают расти.

Согласно Базельскому комитету по банковскому надзору электронный банкинг получил такое определение: «электронное банковское дело или электронный банкинг (*e-banking*), включает в себя предоставление розничных и незначительных по объёму банковских продуктов, услуги через электронные банковские каналы, а также значительные по объёму электронные платежи и другие оптовые банковские услуги электронным способом».

Рынок электронных платежей стремительно растёт с каждым годом, вместе с ним растёт число компьютерных преступлений. Ежедневно тысячи людей становятся жертвами сетевых аферистов.

Сейчас наиболее востребованным способом безналичных расчетов является осуществление платежей через банковские карты. В нашей стране число дебетовых карт превышает численность граждан почти в 2 раза. На январь 2016 г. их количество составило 243 929 тыс. ед.

Из статистики ЦБ РФ за 2015 г. следует, что мошенники чаще всего пытаются украсть суммы от 10 до 50 тысяч рублей, количество инцидентов с каждым кварталом 2015 г. росло, и только во втором квартале удалось предотвратить 21 % от суммы нелегально выводимых денежных средств [3].

Рост популярности систем электронного банкинга, не только в западных странах, но и в России, еще раз подтверждает, что у этого вида банковских услуг появился устойчивый и платёжеспособный спрос.

Идентификация угроз информационной безопасности в сфере электронного банкинга приводит к очень большому числу сценариев возможных инцидентов. В статье приведён анализ угроз с более высокими уров-

нями рисков. Формально риск можно определить следующим образом: риск = угроза * уязвимость [4].

Таким образом, устранение уязвимости и уменьшение вероятности реализации угрозы непосредственно приводят к снижению риска.

Для оценки и анализа существующих угроз информационной безопасности в сфере электронного банкинга для мобильных устройств использован один из инструментов выбора и оценки решения – метод Дельфи. Метод характеризуется меньшей предвзятостью, субъективностью и влиянием авторитета отдельных участников. При оценке коэффициента уязвимости была введена шкала баллов от 0 до 10, где 10 – наиболее часто встречающаяся по мнению экспертов угроза.

Экспертные оценки опираются на авторское исследование конъюнктуры информационной безопасности, на базе статистики представленной Лабораторией Касперского на виртуальной карте угроз для России и для мира. Период первый квартал 2016 г., четвёртый квартал 2015 г., третий квартал 2015 г., второй квартал 2015 г. [5].

В целях дальнейшего вычисления уровня риска каждой угрозы, введён коэффициент угрозы, по шкале от одного до трёх, где «3» – максимальный уровень угрозы, то есть последствия её реализации – это нарушение целостности, нарушение доступности, нарушение конфиденциальности. Коэффициент «1» в этой шкале означает, что в последствиях этой угрозы может быть только одно из вышеприведённых нарушений.

В таблице 1 приведён перечень рассмотренных детектируемых угроз из банка данных угроз ФСТЭК.

ТАБЛИЦА 1. Перечень угроз из БДУ и их коэффициентов

№ УБИ в БДУ	Название угрозы	Коэффициент угрозы
УБИ.173	Угроза «спама»	1
УБИ.170	Угроза неправомерного шифрования информации	1
УБИ.127	Угроза подмены действия пользователя путём обмана	3
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	1
УБИ.036	Угроза исследования механизмов работы программы	2
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	2
УБИ.042	Угроза межсайтовой подделки запроса	3
УБИ.172	Угроза распространения «почтовых червей»	3
УБИ.006	Угроза внедрения кода или данных	3

В таблице 2 показаны выставленные экспертами оценки для каждой вышеописанной угрозы методом Дельфи.

Результаты рассчитанного риска угроз представлены в таблице 3.

ТАБЛИЦА 2. Выставленные экспертами оценки

	УБИ 173	УБИ 127	УБИ 116	УБИ 086	УБИ 036	УБИ 042	УБИ 172	УБИ 170	УБИ 006
Эксперт 1	10	6	4	2	3	1	2	1	2
Эксперт 2	10	8	7	3	3	2	2	1	1
Эксперт 3	10	7	6	4	8	1	5	1	1
Эксперт 4	8	6	5	3	10	2	2	1	1
Эксперт 5	7	2	2	6	4	7	6	4	2
Эксперт 6	10	5	6	4	2	5	3	2	2

ТАБЛИЦА 3. Полученные коэффициенты и риск угроз

Средняя оценка	УБИ 173	УБИ 127	УБИ 116	УБИ 036	УБИ 086	УБИ 172	УБИ 042	УБИ 170	УБИ 006
Коэффициент уязвимости	9,2	5,7	5	5	3,6	3,3	3	1,7	1,5
Коэффициент угрозы	1	3	1	2	2	3	3	1	3
Риск	**9,2**	**17,1**	**5**	**10**	**7,2**	**9,9**	**9**	**1,7**	**4,5**

Проанализировав полученные результаты, видим, что наиболее опасной угрозой является угроза подмены действий пользователей путём обмана.

Следует отметить, что из года в год совершенствуются техники обмана пользователей. Так, в последних версиях Android при отправке текстового сообщения на премиум-номер система спросит у пользователя разрешения. Изобретатели SMS-троянца Tiny поверх этого диалогового окна выводят свое, которое не перекрывает при этом кнопки оригинального окна.

Вторыми наиболее опасными являются угрозы УБИ.036 и УБИ.172.

Через «почтовые черви», к которым и относятся загрузчики, нарушитель устанавливает вредоносное ПО на устройство пользователя, когда risktool же часто помогают вышеперечисленным вредоносным программам оставаться незаметными легально, посредством выключения тех или иных процессов, приложений.

Угроза «спама» на сегодняшний день находится на третьем месте. Количественно её очень много, но угрозы как таковой она не представляет.

УБИ.042, угроза межсайтовых подделок запросов на четвёртом месте.

Банкеры напрямую крадут учётные данные от систем интернет-банкинга, мобильного банкинга и платёжных систем.

УБИ.086 на пятом месте.

Основная функция – перенаправить SMS-транзакции, осуществляемые во время оплаты пользователем контента или продуктов приложениях так, чтобы средства ушли на счёт к злоумышленнику. На сегодняшний день Triada – самый сложный зловред данного типа.

Угроза перехвата данных, передаваемых по вычислительной сети занимает всего лишь шестое место, на общем фоне угроз.

Сюда же входят spy-трояны, которые воруют персональные данные пользователей, в том числе входящие SMS (*mTAN*) от банков.

Остальные угрозы на общем фоне обладают наименьшим риском для физических лиц.

Ключевым преимуществом электронного банкинга является возможность доступа к счетам в любое время и из любого места. Клиенту теперь не обязательно посещать банк для выполнения платежей или получения выписки – он может всё это сделать, не отходя от своего рабочего места и имея под рукой лишь телефон, с выходом в интернет.

Многие банки предлагают своим клиентам такие услуги, как мобильный банк, позволяющий отслеживать все движения по счету, 3D-Secure, как двухфакторную аутентификацию, выпуск виртуальной карты, и открытие дополнительного накопительного счета. Но на сегодняшний день все эти решения не обеспечивают гарантированную защиту. Универсального «способа защиты от мошенничества» нет, как и нет действенного способа защиты от обмана вообще. Возможно, что высокая степень защищённости от мошеннических операций может быть достигнута за счет следования тактике, основанной на общепринятых принципах безопасного поведения совместным использованием специализированных механизмов. Современные методические аспекты в области обеспечения информационной безопасности для физических лиц требуют доработки и совершенствования. Защите в сфере информационной безопасности электронного банкинга сейчас крайне необходимы преобразовании и инновация.

Список используемых источников

1. Волков Д., Кибермошенничество в России: эволюция угроз // Банковские технологии. 2015. № 1. С. 26–28.

2. Статистика Центрального Банка Российской Федерации по ДБО за 2015 год [Электронный ресурс]. URL: http://www.cbr.ru/statistics/ (дата обращения 03.05.2016).

3. Мастяева И. Н., Мирзаханян Р. Э. Методы и модели рисков в различных областях // Фундаментальные исследования. 2014. № 9-2. С. 399–402.

4. Интерактивная карта киберугроз/Касперский [Электронный ресурс]. URL: https://cybermap.kaspersky.com/stats/ (дата обращения 10.05.2016).

5. Банк данных угроз безопасности информации / Федеральная служба по техническому и экспортному контролю [Электронный ресурс]. URL: http://bdu.fstec.ru/threat (дата обращения 01.05.2016).

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ НАРУШЕНИЯ КРИТИЧЕСКИХ СВОЙСТВ ИНФОРМАЦИОННОГО АКТИВА НА ОСНОВЕ CVSS МЕТРИК УЯЗВИМОСТЕЙ

Л. А. Виткова, М. Н. Дудникова, А. Н. Петрова

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

В статье авторы разрабатывают метод для определения вероятности нарушения критических свойств информационного актива на основе Common Vulnerability Scoring System version 3.0 метрик уязвимостей на основе риск-ориентированного подхода, предложенного стандартом ISO/IEC 27005. На основе разработанного метода приводится формула для оценки уязвимости информационных активов.

информационная безопасность, CVSS v3.0, метод оценки риска.

Одной из первых и наиболее популярных по сей день моделей безопасности является модель, предложенная Зальцером и Шредером. Авторы постулировали, что все возможные нарушения информационной безопасности всегда могут быть отнесены, по меньшей мере, к одной из трех групп: нарушения конфиденциальности, нарушения целостности или нарушения доступности.

Требования к безопасности могут меняться в зависимости от назначения информационной системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой нарушения целостности и доступности не представляли бы опасности, вместе с тем обеспечение конфиденциальности не всегда является обязательным.

Практически любой ИС присущи уязвимости, обуславливающие возможность реализации угроз обрабатываемой в ней информации. Процесс управления уязвимостями включает обнаружение, классификацию, оценку и устранение уязвимостей. Большинство современных сканеров уязвимостей решают также задачу классификации, используя данные из опреде-

лённой базы уязвимостей, например, Common Vulnerabilities and Exposures (CVE). Существуют различные системы оценки уязвимостей. Наиболее распространенная и проверенная на практике – Common Vulnerability Scoring System (CVSS).

Система оценки общеизвестных уязвимостей (CVSS) позволяет выделить основные характеристики уязвимости и дать количественную (числовую) оценку степени ее серьезности, а также текстовое представление этой оценки.

Особо остро стоит задача определения эффективности их применения для устранения обнаруженных уязвимостей. Для решения данной задачи предлагается использовать риск-ориентированный подход.

Цель исследования – разработать метод для определения вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей. Данный метод позволит оценить риск, связанный с эксплуатацией уязвимостей ИС, и определить эффективность использования дополнительных мер и средств защиты для их устранения.

Согласно наиболее распространённому подходу, зафиксированному в стандарте ISO/IEC 27005 [1], значение риска может быть определено по формуле:

$$R = \sum_{j=1}^{n} P_r^j * I^j \ ,$$

где R – значение риска; P_r^j – вероятность реализации j-й угрозы; I^j – значение ущерба от реализации j-й угрозы; n – число угроз.

В стандарте NIST 800-37 представлен трехуровневый подход к оценке риска, в соответствии с которым выделяют уровень информационных систем (ИС), уровень бизнес-процессов и уровень организации [2]. На уровне ИС происходит идентификация ИА, уязвимостей и угроз, а также применяемых средств и мер защиты. Этой информации достаточно для определения вероятности возникновения ущерба.

Процесс обеспечения информационной безопасности направлен на обеспечение свойств КЦД. В методе предлагается отдельно определять значения риска от потери конфиденциальности, целостности и доступности. При этом сумма значений риска, связанных с потерей отдельных критических свойств, будет составлять полный риск. С учетом этого формула для определения величины полного риска ИА приобретает вид:

$$R = P_c * I_c + P_i * I_i + P_a * I_a,$$

где P_c, P_i, P_a – вероятности нарушения конфиденциальности, целостности и доступности ИА соответственно; I_c, I_i, I_a – значения ущерба, возникающего при нарушениях конфиденциальности, целостности и доступности ИА соответственно.

Преимущество данного подхода в том, что нет необходимости для каждой пары «угроза-уязвимость» определять значение ущерба. Это позволяет отдельно оценивать вероятности нарушения критических свойств ИА и значения ущерба от нарушения этих свойств. Вместо вероятности реализации угрозы определяется вероятность эксплуатации уязвимости, которая учитывает, как вероятность наличия уязвимости, так и вероятность её использования хотя бы одной из угроз.

Сам факт успешной эксплуатации уязвимости не обязательно влечёт за собой нарушение свойств КЦД. Поэтому для каждой уязвимости необходимо определять вероятности того, что её эксплуатация приведет к нарушению критических свойств КЦД. Считается, что уязвимости независимы друг от друга, поэтому эксплуатация одной из них не обязательно приведёт к эксплуатации других. С учетом этого для расчета вероятностей нарушения критических свойств ИА предлагаются следующие формулы:

$$P_c = (1 - \prod_{j=1}^{m}(1 - P_e^j * P_c^j)), P_i = (1 - \prod_{j=1}^{m}(1 - P_e^j * P_i^j)),$$
$$P_a = (1 - \prod_{j=1}^{m}(1 - P_e^j * P_a^j)),$$

где P_e^j – вероятность эксплуатации j-й уязвимости; P_c, P_i, P_a – вероятности нарушения конфиденциальности, целостности и доступности.

Использование метрик CVSS для определения вероятности нарушения критических свойств ИА. Система CVSS включает три группы метрик: базовые, временные и контекстные (рис. 1).

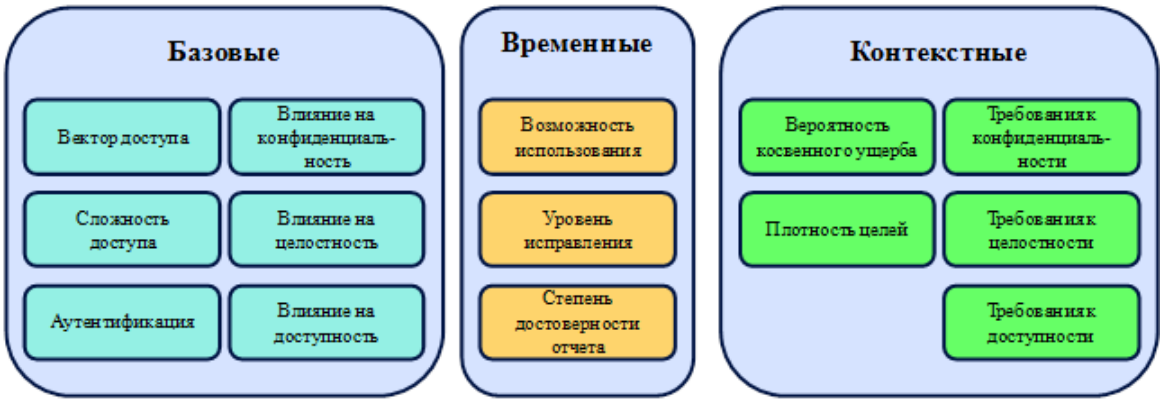


Рис. 1. Метрики CVSSv3.0

Базовые метрики отображают основные характеристики уязвимости, которые не изменяются со временем и не зависят от среды. Они подразделяются на метрики возможности эксплуатации и метрики воздействия. Временные метрики представляют характеристики уязвимости, изменяющиеся со временем и не зависящие от среды. Контекстные метрики пред-

ставляют характеристики, связанные со средой пользователя, и позволяют оценить уровень ущерба в относительных величинах.

В методе определения вероятности нарушения критических свойств ИА используются базовые и временные метрики, значения которых определяются аналитиками, производителями продуктов в области ИБ или производителями приложений. Поскольку определение величины ущерба выносится за рамки данного исследования, контекстные метрики в работе не используются.

Для определения вероятности эксплуатации уязвимости предлагается использовать базовые метрики возможности эксплуатации, а также временные метрики (табл. 1).

ТАБЛИЦА 1. Используемые метрики для определения вероятности уязвимости

Метрический показатель	Метрическое значение	Количественное значение
Attack Vector Modified Attack Vector (AV/MAV)	Network Adjacent Network Local Physical	0,85 0,62 0,55 0,20
Attack Complexity Modified Attack Complexity (AC/MAC)	Low High	0,77 0,44
Privilege Required Modified Privilege Required (PR/MPR)	None Low High	0,85 0,62 0,27
User Interaction Modified User Interaction (UI/MUI)	None Required	0,85 0,62
C,I,A Impact Modified C,I,A Impact (C, I, A, MC, MI, MA)	High Low None	0,56 0,22 0,0
Exploit Code Maturity (E) Временная метрика	High Functional Proof of Concept Unproven	1,00 0,97 0,94 0,91
Remediation Level (RL) Временная метрика	Unavailable Workaround Temporary Fix Official Fix	1,00 0,97 0,96 0,95
Report Confidence (RC) Временная метрика	Confirmed Reasonable Unknown	1,00 0,96 0,92
Security Requirements – C,I,A Requirements (CR, IR, AR)	High Medium Low	1,5 1,0 0,5

Представленные в таблице 1 метрики являются факторами, влияющими на вероятность эксплуатации уязвимости, которая находится по формуле:

$$Pe = AV*AC*Au*E*RL*RC.$$

Для определения вероятности нарушения критических свойств ИА от эксплуатации уязвимости используются базовые метрики воздействия и дополнительно вводимая метрика взаимосвязи ИА и ПО, у которого была обнаружена уязвимость. Так, ИА может создаваться, изменяться, использоваться ПО, храниться с ПО на одном хосте, разных хостах с возможностью удаленного доступа, либо они могут быть не связанными.

С учетом этого вероятности нарушения конфиденциальности, целостности и доступности определяются по формулам:

$$Pc = C*IR;\ Pi = I*IR;\ Pa = A*IR.$$

В дальнейшей работе совершенствовать метод определения оценки уязвимости и состояния защищенности информационной системы на основе CVSSv3 и Гексады Паркеры. Данный метод позволит оценить риск, связанный с эксплуатацией уязвимостей ИС направленных не только на такие свойства информации как конфиденциальность, целостность и доступность, но и дополнительных свойств из Гексады Паркера – аутентичность и владение. С помощью этого метода можно будет определить эффективность использования дополнительных мер и средств защиты для устранения приведенных уязвимостей.

Список используемых источников

1. ISO/IEC 27005, Информационные технологии – Методы защиты – Системы менеджмента информационной безопасности – Требования [Электронный ресурс]. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en:sec:G (Дата обращения 25.03.2018).

2. NIST 800-37 NIST SP 800-37, Руководство по сертификации и аккредитации безопасности Федеральных информационных систем [Электронный ресурс]. URL: https://nvlpubs.nist.gov/ (Дата обращения 25.03.2018).

3. Спецификация метода оценки уязвимостей CVSSv3 [Электронный ресурс]. URL: https://www.first.org/cvss/ (Дата обращения 25.03.2018).

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53

РАССЛЕДОВАНИЕ И ОЦЕНКА УЯЗВИМОСТИ НУЛЕВОГО ДНЯ МЕТОДОМ COMMON VULNERABILITY SCORING SYSTEM VERSION 3.0

Л. А. Виткова, М. Н. Дудникова, А. Н. Петрова

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

В статье авторы проводят расследование инцидентов информационной безопасности при эксплуатации уязвимости нулевого дня. Проводится исследование и анализ таргетированной атаки с помощью вируса-шифровальщика. Приведены сигнатуры вируса, в антивирусном программном обеспечении, которое уже обнаружило данный вредоносный файл, приведен код исполняющегося файла, описан процесс работы вируса no_more_ransom, последствия заражения, способы предотвращения заражения компьютера, варианты расшифровки данных и современные методы защиты от атак zer0-day. Приведена оценка уязвимости методом common vulnerability scoring system version 3.0

информационная безопасность, CVSSv3.0, уязвимость 0-day, вирус-шифровальщик, no_more_ransom.

Человечеству с незапамятных времен известно шифрование. А шантаж, наверное, известен со времен еще более древних. Пару десятков лет назад эти методы объединили и обратили против большого количества людей. В 1989 г., когда биолог, доктор Джозеф Л. Попп, создал первого трояна-вымогателя. Доктор Попп написал вредоносный код и распространил его на конференции, посвященной СПИДу, которую проводила Всемирная организация здравоохранения. Зловред распространялся на дискетах с наклейкой «Вводная информация о СПИДе» с отдельно напечатанным предупреждением о том, что программное обеспечение на носителях может повредить компьютеры.

В 2016 г. в мире началось организованное противостояние вымогателям. В июле был запущен проект No More Ransom, объединивший усилия Национальной полиции Нидерландов, Европола, компаний Intel Security и «Лаборатория Касперского»; в октябре к проекту присоединились ещё 13 организаций. В рамках проекта в открытом доступе были размещены бесплатные утилиты для расшифровки данных.

В конце 2016 г. в России вспыхнула активность шифровальщика по иронии названным «no_more_ransom» [2]. Предполагается, что его создатели связаны с такими вирусами как better_call_saul и da_vinci_code.

Интересно, что в подавляющем большинстве случаев сообщения, посредством которых распространялся вирус были «из налоговой». Часть писем сообщают о необходимости оплаты счета, другие предлагают посмотреть свежий прайс-лист и т. д. В сообщении был прикреплённый архив, который в свою очередь содержал файл, название и иконка которого на первый взгляд не вызывали подозрений, например, в отчет _xls.js.

При попытке открытия этого файла выполняется javascript-код и происходила активизация вируса. No_more_ransom вирус зашифровывает файлы разнообразных форматов на компьютере жертвы. Со стороны жертвы, всё выглядело так, что после окончания процесса шифрования, все знакомые файлы исчезали, а в папках, где хранились документы, появлялись новые файлы со странными именами и расширением .no_more_ransom. Кроме этого на рабочем столе появлялась устрашающая заставка с сообщением как на слайде (рис. 1).

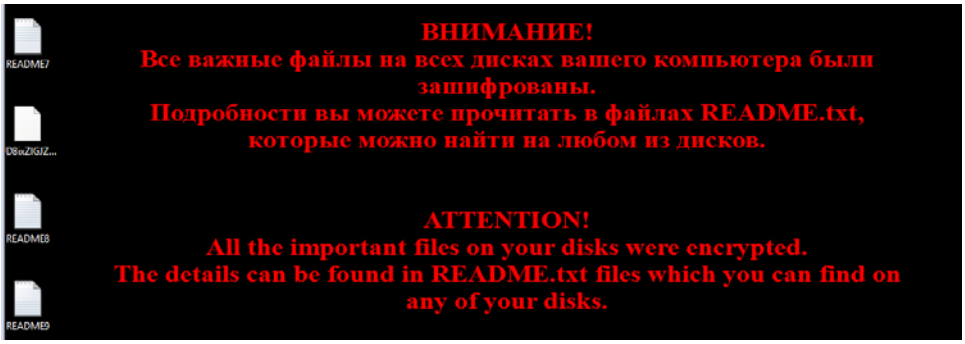


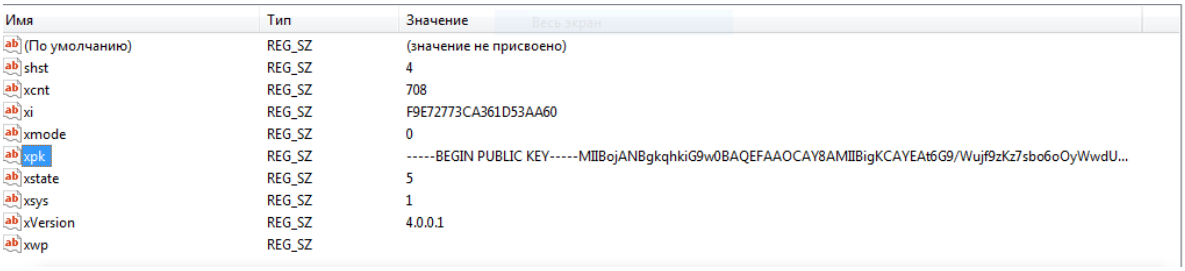
Рис. 1. Рабочий стол зараженного компьютера

Сценарий javascript кода очень запутан. При первом запуске No_More_Ransom собирает различную информацию о системе и на её основе генерирует для себя уникальное имя, представляющее собой бессмысленный набор некоторого количества латинских букв, но видно, что он использует объект ActiveXObject, который является расширением Microsoft и поддерживается только в Internet Explorer. Вирус по специальному алгоритму генерирует доменные имена и пытается присоединиться к ним. Попытки подключения к серверу продолжаются до тех пор, пока не будет сгенерировано актуальное имя на данный момент. В ходе выполнения сценария JS-код пытается загрузить тело вредоносного файла из других источников: http://clidis.pt/helpconfig.exe либо из 40.77.226.250 IP-адрес (*Microsoft Corporation in Dublin, Dublin, Ireland*) или из 34.172.18.212 IP-адреса (*rev.vodafone.pt*). Затем файл helpconfig.exe загружается на зараженный компьютер. Файл загружется по следующему пути: %AppData%\Local\Microsoft\Windows\TemporaryInternetFiles\Content.IE5\643WD09Y\helpconfig.exe. На самом деле, helpconfig.exe используется в качестве установщика.

После выполнения этих шагов вредоносная программа будет пытаться подключиться к некоторым C&C серверам (часть из которых является TOR узлами): 40.77.229.250, 40.77.229.125, 194.109.206.212, 195.154.92.155, 131.215.172.214, 21.219.28.99.

В случае успешного подключения на сервере генерируется пара ключей для RSA шифрования. Публичный ключ передаётся на компьютер жертвы и хранится в реестре, закрытый ключ, предназначенный для расшифровки, остается на сервере, вместе со сгенерированным идентификатором компьютера жертвы.

Вирус вносит изменения в реестр. Для сохранения содержимого ключей No_More_Ransom постоянно мониторит их состояние и восстанавливает в случае необходимости. На рис. 2 показан добавленный ключ HKCU\Software\System32\Configuration.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
shst	REG_SZ	4
xcnt	REG_SZ	708
xi	REG_SZ	F9E72773CA361D53AA60
xmode	REG_SZ	0
xpk	REG_SZ	-----BEGIN PUBLIC KEY-----MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAt6G9/Wujf9zKz7sbo6oOyWwdU...
xstate	REG_SZ	5
xsys	REG_SZ	1
xVersion	REG_SZ	4.0.0.1
xwp	REG_SZ	

Рис. 2. Параметры и значений ключа реестра HKCU\Software\System32\Configuration

На рис. 3 показано, что для обеспечения своего запуска одновременно с запуском системы троян создает в реестре в ветках автозапуска ключ HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Client Server Runtime Subsystem

(По умолчанию)	REG_SZ	(значение не присвоено)
Client Server Runtime Subsystem	REG_SZ	"C:\ProgramData\Windows\csrss.exe"
Google Update	REG_SZ	C:\Users\bobby\AppData\Local\Google\Update\1....

Рис. 3. Параметры и значений ключа реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Run\

Этим вирус обеспечивал себе возможность продолжить шифрование. если по каким-либо причинам компьютер был выключен. Он будет создавать копию себя под именем процесса CSRSS (процесс Windows, устранение которого приведет к синему экрану смерти). На рис. 4 показано дерево процессов вируса.

На этом этапе начинается процесс шифрования. Вирус шифрует огромное количество разных видов файлов, форматы приведены на слайде. Судя по названиям зашифрованных файлов, в хвосте указан зашифрованный сессионный ключ. При старте шифрования генерируется случайный

ключ для AES, им шифруется всё, сам сгенерированный ключ шифруется публичным RSA-3072. В случае неуспешного подключения выбирается один из зашитых в троянец RSA-ключей.

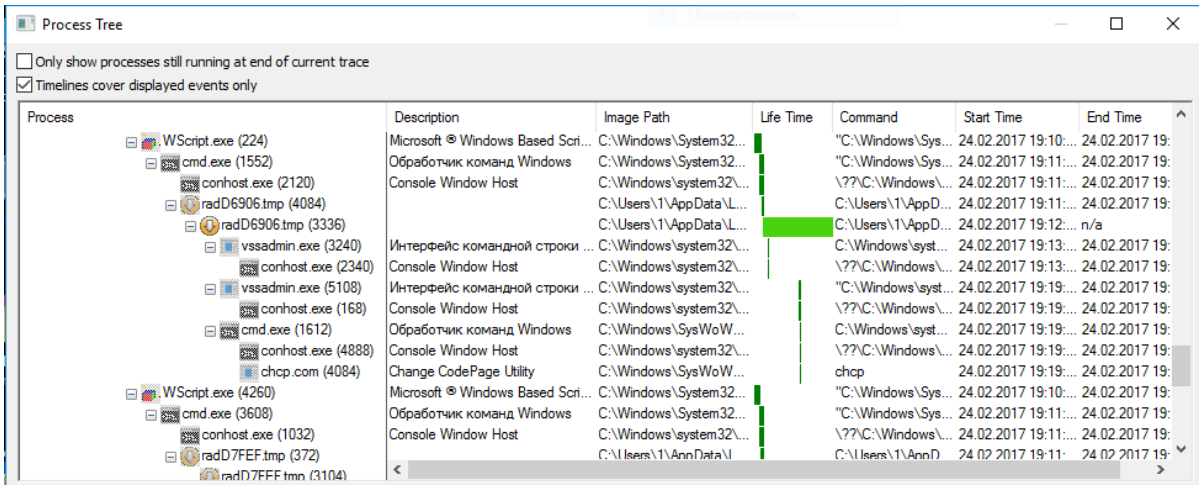


Рис. 4. Дерево процессов вируса no_more_ransom

Вирус не шифрует файлы в системных папках. После шифрования файлов вирус создает на всех дисках и рабочем столе идентичные текстовые документы README.txt, README1.txt, README2.txt…

В файле Readme.txt, жертва получает указание связаться с lukyan.sazonov26@gmail.com, чтобы получить дальнейшие инструкции. Этот адрес электронной почты ранее был связан с вымогателями better_call_saul и da_vinci_code.

Если ответ не получен от этого адреса в течение 48 часов, жертва должна заполнить контактную форму, расположенную в сети TOR.

Большинство современных сканеров решают также задачу классификации найденных уязвимостей, используя данные из определённой базы уязвимостей, например, Common Vulnerabilities and Exposures (CVE). Существуют различные системы оценки уязвимостей. Наиболее распространенная и проверенная на практике – Common Vulnerability Scoring System (CVSS). В CVSS для каждой уязвимости рассчитывается базовая оценка в интервале от 0 до 10. Затем определяется уровень опасности уязвимости по специальной шкале. Таким образом, CVSS позволяет ранжировать найденные уязвимости и определять приоритеты их устранения.

На основе этого метода оценим уязвимость вируса No_more_ransom. По критериям метода CVSSv3 построили вектор CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H. На рис. 5 представлены вводные данные метрик в калькулятор CVSSv3 и результирующая оценка.

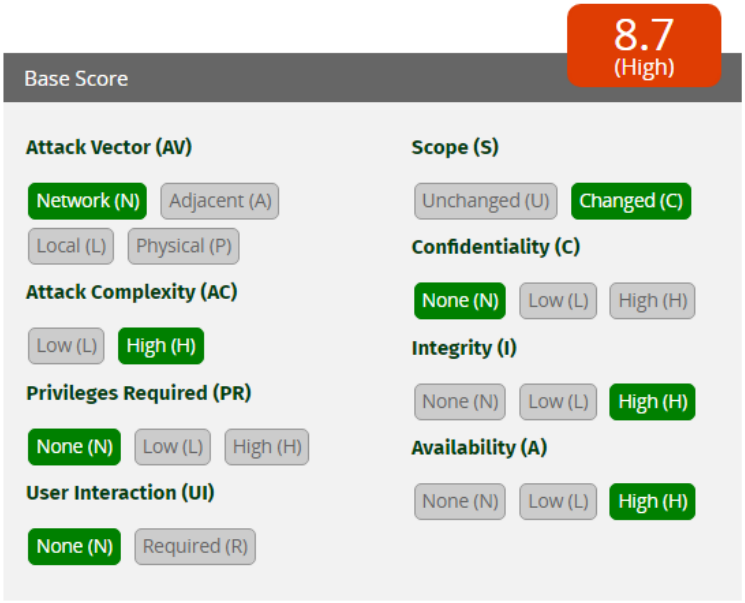


Рис. 5. Расчет оценки уязвимости с помощью CVSSv3.0

На сегодняшний день нет доступного декриптора no_more_ransom файлов. Так как используется очень сильный алгоритм шифрования RSA-3072 без личного ключа, расшифровать файлы практически невозможно. Использовать метод подбора ключа нецелесообразно, из-за большой длины ключа, на это уйдет много лет. Настоятельно рекомендуется делать резервные копии важных файлов, или целой ОС.

В некоторых случаях восстановить файлы можно с помощью утилит, таких как ShadowExplorer, позволяющих восстанавливать теневые копии файлов, которые создаются автоматически ОС.

Для предотвращения заражения компьютера вирусами-вымогателями используйте встроенные средства систем защиты от проникновения и активизации, которые есть у большинства антивирусных программ. Например, используйте CryptoPrevent. Kaspersky Virus Removal Tool (KVRT) и Malwarebytes Anti-malware (MBAM) могут обнаруживать разные типы активных вирусов-шифровальщиков и легко удалят их с компьютера.

Список используемых источников

1. Трояны-вымогатели: чума 2016 года [Электронный ресурс]. URL: https://blog.kaspersky.ru/fighting-ransomware/13650/ (Дата обращения 25.03.2018).

2. Virustotal онлайн-сканер вирусов, вредоносных файлов [Электронный ресурс]. URL: https://www.virustotal.com/en/ (Дата обращения 25.03.2018).

3. Спецификация метода оценки уязвимостей CVSSv3 [Электронный ресурс]. URL: https://www.first.org/cvss/ (Дата обращения 25.03.2018).

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК004.056.5

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И ТИПЫ АТАК НА СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Л. А. Виткова, М. Н. Дудникова, А. Н. Петрова

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

В современном мире онлайн-банкинг, электронные деньги, кошельки и прочие нововведения создают иллюзию уверенности в том, что заработанные деньги надежно спрятаны от злоумышленников. Однако эволюция в банковской сфере дала толчок для развития способов незаконной наживы, и других угроз финансовых махинаций, поэтому актуальность данной темы растет изо дня в день. Авторы исследуют понятия распределенных систем хранения данных и обработки денежных средств. Описывают понятия, виды электронного представления денежных средств и рассматривают существующие наиболее типичные уязвимости и угрозы информационной безопасности.

системы хранения данных, распределенные системы, электронные денежные средства, большие данные.

По оценкам международной консалтинговой компании J’son & Partners Consulting, в 2012 г. оборот рынка дистанционных финансовых сервисов увеличился на 48 % по сравнению с аналогичным показателем 2011 г., составив 896 млрд рублей (рис.). С 2012 по 2017 гг. среднегодовой темп роста (CAGR) составил 24 %, а к концу 2017 г. рынок превысил 2,6 трлн рублей. За это время рынок ЭПС (электронные платежные системы) рос и увеличивал свою долю относительно других способов оплаты. Ключевым драйвером развития ЭПС стали дистанционные финансовые сервисы, которые увеличили свою долю в ЭПС с 49 % в 2012 г. до 70 % в 2017 г.

Немобильные банковские сервисы (интернет-банкинг), в структуре оборота рынка дистанционных финансовых сервисов, на конец 2012 г. составили 66 %, при этом доля мобильных сервисов составила 3 %. В 2017 г. произошли небольшие изменения в структуре рынка – доля банковских немобильных сервисов увеличилась до 70 % за счет уменьшения доли небанковских сервисов, а доля мобильных сервисов выросла до 4 % [1]. Данная статистика подтверждает, что на сегодняшний день проблемы безопасности дистанционных финансовых систем продолжают оставаться актуальными.

Рисунок. Оборот рынка дистанционных финансовых сервисов, млрд рублей, 2008–2017

Чтобы лучше вникнуть в суть темы, следует вначале разобрать основные понятия. Управление информационной безопасностью – это циклический процесс, включающий в себя несколько этапов и мер:

– сбор и анализ данных о состоянии информационной безопасности в организации и оценка информационных рисков;

– планирование мер по обработке рисков;

– реализация и внедрение соответствующих механизмов контроля, оперативная работа по осуществлению защитных мероприятий;

– мониторинг работы механизмов контроля, а также оценка их эффективности и соответствующие корректирующие воздействия.

Распределенная система – система, для которой отношения местоположений элементов (или групп элементов) играют существенную роль с точки зрения функционирования системы, а, следовательно, и с точки зрения анализа и синтеза системы. Типичной распределённой системой является Интернет.

Система Хранения Данных – это комплексное программно-аппаратное решение по организации надёжного хранения информационных ресурсов и предоставления гарантированного доступа к ним.

Система обработки данных – это комплекс взаимосвязанных методов и средств получения и обработки данных, необходимых для организации управления объектами.

Далее следует разобрать виды представления электронных денег. Их принято классифицировать по форме денежных знаков: фиатные и нефиатные.

Фиатные электронные деньги – электронные деньги, являющиеся одним из видов денежных единиц платежной системы государства и выраженные в одной из государственных валют. Фиатные электронные деньги могут быть на базе сетей, туда можно отнести: международную платежную систему PayPal. Также фиатные электронные деньги бывают на базе смарт-карт, к ним относятся: предоплаченные банковские карты Visa Cash, предназначенные для совершения небольших платежей.

Нефиатные электронные деньги представлены широкой сетью различных платежных систем, таких как QIWI, WebMoney, «Яндекс.Деньги», а также «криптовалютными» платежными системами (*Bitcoin*, *Litecoin* и т. п.). Иным примером нефиатных электронных денег является криптовалюта – это подвид электронных валют, эмиссия и учет которых основывается на криптографических методах, а работа самой платежной системы происходит децентрализовано в распределенной компьютерной сети.

Безопасность подключения пользователей к интернет-банкам, которые являются основными системами электронных денег, обеспечивается использованием протоколов SSL/TLS. Существует ряд известных уязвимостей, позволяющих расшифровывать сессии, перехватывать и подменять данные, передаваемые между пользователем и сервером. К примеру, некоторые банки могут по-прежнему использовать небезопасные параметры обмена ключами Diffie-Hellman, а часть банков может быть уязвима к FREAK-атакам. С помощью данной атаки посторонний злоумышленник может перехватывать защищённые соединения и форсировать использование слабой криптографии из «экспортного» набора шифров RSA. Немалая часть веб-ресурсов имеет уязвимость POODLE. С помощью данной уязвимости злоумышленники могут получить доступ к зашифрованной информации, передаваемой между сервером и клиентом. Считается небезопасным использование протоколов SSL2 и SSL3, так как они использует небезопасную криптографическую хеш-функцию MD5 и слабо защищенные шифры. Значительная часть веб-ресурсов может иметь уязвимость Logjam, которая была обнаружена совсем недавно. Как и уязвимость FREAK, Logjam позволяет злоумышленнику форсировать использование клиентским браузером слабой криптографии DH с 512-битными ключами. Также небезопасным считается использование алгоритма хеширования SHA-1, он считается слабым и небезопасным.

Следует помнить о том, что не реализованная или реализована лишь частично настройка безопасности протоколов согласования ключа – Forward Secrecy может повлечь за собой то, что ключи будут скомпрометированы при компрометации закрытого ключа [2].

Далее авторы рассматривают основные типы атак на системы дистанционного банковского обслуживания, зафиксированные центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфе-

ре главного управления безопасности и защиты информации Банка России FinCERT:

1. Целенаправленные атаки, сопряженные с подменой входных данных для АРМ.

2. Рассылка электронных сообщений, содержащих в себе вредоносное ПО. Данный тип атак является наиболее распространенным.

3. Атаки, направленные на устройства самообслуживания. За отчетный период FinCERT зафиксировал рост количества атак злоумышленников на устройства самообслуживания, в том числе на банкоматы и POS-терминалы.

4. DDoS-атака. Целью данной атаки является отказ в обслуживании легитимных клиентов, вплоть до полной невозможности работы с сервисом. В некоторых случаях, DDoS-атака используется для сокрытия факта целенаправленной атаки.

5. Reversal-атаки. За период с 01 июня 2015 г. по 31 мая 2016 г. FinCERT зафиксировал атаку с использованием поддельных сообщений об отмене платежной операции. Данная атака связана с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. Чаще всего, процессинговые центры не проверяют подлинность такого запроса, в связи с отсутствием контроля ряда полей указанной операции.

Как правило, большинство атак являются мультивекторными, то есть для усложнения атаки используется одновременно несколько способов воздействия на целевую систему, поэтому, защититься от нее становится значительно труднее [3].

Возможным вариантом решения проблем систем дистанционного банковского обслуживания может оказаться использование алгоритмов Big Data.

Big Data – это технологии, которые позволяют быстро обрабатывать большие объемы информации разного формата. Однако представители финансовой отрасли в подавляющем большинстве имеют в виду частный случай Big Data – большие объемы накопленных однородных данных. Как известно, банки и страховые компании хранят все: анкеты, истории транзакций и общения с клиентами, внутреннюю информацию [4].

По оценкам исследовательской компании Gartner, на сегодня 34 % банков по всему миру инвестировали в развитие этих технологий. По данным исследования McKinsey & Company, 25 % Big Data владеет финансовая индустрия, и в среднем на каждую компанию приходится по 3,8 петабайта данных. По результатам опроса того же McKinsey, 76 % банков заявляют, что Big Data позволяют привлекать новых клиентов, лучше взаимодействовать с ними и поддерживать их лояльность.

Современные технологии вполне позволяют обрабатывать накопленные массивы данных. Проблема в том, что они делают это недостаточно быстро. Именно технологии Big Data способны решить старые долговременные задачи быстро, дав время для маневра и обдуманных действий [5].

Из всего колоссального накопленного количества информации, по различным оценкам участников рынка банковской и страховой автоматизации, в жизни организации используется в наилучшем случае лишь половина информации. Поэтому вопрос монетизации хранения данных так же вечен для банков, как проблема загрязнения окружающей среды – для промышленных мегаполисов. Только технологии Big Data могут обеспечить экономическое обоснование этого хранения, так как без Big Data извлечь ценность из накопленного богатства информации невозможно.

Колоссальные перспективы раскрывает перед банком сочетание Big Data и геоаналитики. Например, клиент заявил о потере карты и одновременно по этой же карте в магазине совершена покупка. Банк оперативно идентифицировал местонахождение телефона клиента и может доказать, что клиент пытается смошенничать (если телефон и карта находятся рядом). Или заблокировать транзакцию, не дожидаясь заявления клиента о потере карты (если телефон и карта находятся на приличном расстоянии друг от друга).

Рассмотренные авторами выше возможные уязвимости и атаки на дистанционные финансовые сервисы подтверждают, что эволюция в банковской сфере дала толчок для развития способов незаконной наживы и других угроз финансовых махинаций. Поэтому в современном мире стоит уже по-другому подходить к вопросам управления информационной безопасности таких систем. Авторы обращают внимание на то, что следует рассматривать возможности алгоритмов Big Data для систем финансовой индустрии.

Список используемых источников

1. Российский рынок дистанционных финансовых сервисов [Электронный ресурс] // Отчет J’son & Partners Consulting. Режим доступа: http://web.json.ru/poleznye_materialy/free_market_watches/analytics/rossijskij_rynok_distancionnyh_finansovyh_servisov/

2. Хант Т. Безопасность SSL/TLS интернет-банкинга [Электронный ресурс]. Режим доступа: https://www.troyhunt.com/2015/05/do-you-really-want-bank-grade-security.html

3. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г. – 21 с. Режим доступа: http://www.gproxx.com/http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf

4. Mayer-Schönberger V., CukierK. Big Data: A Revolution That Will Transform How We Live, Work, and Think, 2014.

5. Карев А. С., Бирих Э. В., Сахаров Д. В, Виткова Л. А. Проблемы информационной безопасности в интернете вещей // Интернет вещей и 5G. 2-я международная научно-техническая конференция студентов, аспирантов и молодых ученых. 2016. С. 66–70.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

М. А. Власенко, Д. А. Иванов, С. И. Кузнецов, О. С. Лаута

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье описан подход к обеспечению защищенности канала управления робототехническим комплексом, основанный на анализе обмена между оператором и комплексом с использованием протоколов пакетной передачи данных. Для анализа предлагается использовать различные типы нейронных сетей. В статье рассмотрены типовые задачи, решаемые различными типами нейронных сетей, и вопросы сводимости данных задач к задаче обнаружения аномалий в процессе обмена данными управления между робототехническим комплексом и оператором.

роботизированные системы; система управления; беспроводное управление; протоколы управления; защита информации; искусственные нейронные сети.

На текущем этапе развития технологий робототехнические комплексы (РТК) выполняют широкий спектр задач в различных областях деятельности человека: научной, промышленной, медицинской. Отдельную нишу занимают РТК, выполняющие задачи специального назначения: военные РТК, РТК, обеспечивающие ликвидацию последствий чрезвычайных происшествий и других задач, связанных с риском для жизни человека.

Одной из важнейших задач при построении РТК как специального назначения, так и некоторых других типов, является обеспечение управления комплексом. Под управлением РТК понимается решение комплекса задач, связанных с адаптацией робота к кругу решаемых им задач, программированием движений, синтезом системы управления и её программного обеспечения [1].

Наибольший интерес для решения задач, связанных с риском для жизни человека, представляют интерактивные системы управления, так как при решении сложных задач пока что избежать необходимости участия оператора избежать не удаётся. При этом, более перспективным методом интерактивного управления РТК является дистанционное беспроводное управление. Применение данного метода управления позволяет изолировать оператора от опасных для жизни факторов, а также обеспечить максимально мобильный процесс управления, не требующий наличия какого-либо материального носителя для передачи сигналов управления [2, 3].

Протоколом управления называется стандарт, описывающий правила взаимодействия объекта и оператора. Для решения задачи интерактивного управления РТК чаще всего приходится использовать несколько протоколов, объединённых в так называемый «стек протоколов». На нижнем уровне стека располагается протокол, описывающий физический процесс передачи сигналов управления, а на верхнем – протокол, описывающий непосредственные команды управления, принимаемые роботом и передаваемые им сигналы.

Важнейшим вопросом, при построении и использовании РТК специального назначения, а в особенности, РТК, применяемых силовыми структурами, является обеспечение защищённости канала управления комплексом. Получение злоумышленником передаваемых сведений, их подмена, искажение или подавление могут привести к различными негативным последствиям вплоть до того, что могут погибнуть люди.

Можно выделить два основных подхода к обеспечению безопасности передачи сигналов управления РТК:

1. Использование средств защиты передаваемой информации, предоставляемых протоколом передачи.

2. Внедрение дополнительных средств защиты.

Большинство рассмотренных методов полагаются на криптографические механизмы защиты передаваемой информации. Данный подход является эффективным с точки зрения защиты от получения, подмены и искажения данных злоумышленником, но при этом абсолютно утрачивает свою эффективность в случае, когда злоумышленник обладает секретными ключами, используемыми для шифрования и подписи передаваемых данных.

Для того, чтобы обнаружить уязвимости в протоколе управления РТК, осуществляют процедуру аудита для информационной безопасности.

Можно выделить три основных подхода к обнаружению аномалий в протокольном обмене в процессе управления РТК:

У нейронных сетей присутствуют две главные проблемы [4]:

1 – непонятность полученных результатов: нейронная сеть приняла решение, но не может объяснить, почему именно оно было принято;

2 – нехватка адекватного материала для обучения: невозможно создать базу со всеми типами аномалий.

Главный недостаток экспертных систем – неумение выявлять (и, как следствие, отражать) атаки неизвестных типов [5].

Выявление аномальной активности статистическими методами основано на том, что происходит сравнение краткосрочного поведения и долгосрочного. Проводятся измерения значений части параметров работы субъектов (аппаратуры, приложений, пользователей [6].

Выявление аномальной активности относится к внутреннему аудиту информационной системы.

Применение методов искусственного интеллекта для обнаружения аномалий протокольного обмена также основывается на построении профиля нормального поведения, но в отличие от статистического подхода, данный подход использует менее структурированный профиль, который не строится согласно заданным метрикам, а может включать в себя произвольный набор данных, характеризующих те или иные протоколы, включённые в используемый стек. В дальнейшем, анализ этих данных в режиме реального времени и сравнение их с профилем нормального поведение также позволит обнаружить отклонения от нормального поведения и сделать вывод о наличии несанкционированных воздействий.

Хорошо зарекомендовавшим себя подходом к решению подобных задач с применением методов искусственного интеллекта является использование искусственных нейронных сетей (ИНС). ИНС представляют математически-формализованную модель естественного мыслительного процесса человека, основанного на передаче информации между простейшими структурными единицами – нейронами. Данный подход является одним из наиболее перспективных и позволяет решать широкий спектр задач: классификация, оптимизация, кластеризация, аппроксимация функций, прогнозирование и др. [7, 8].

Процесс построения профиля нормального поведения в случае с нейронными сетями сводится к созданию обучающей выборки, состоящей из примеров, содержащих данные нормального обмена РТК с оператором, и дальнейшего обучения ИНС с использованием этих данных. Алгоритмы обучения, обычно, выбираются на основе выбранного типа ИНС. Параметры ИНС выбираются эмпирическим путём в зависимости от конкретной задачи.

В случае же, когда профиль нормального поведения содержит данные протокола непосредственной передачи команд управления, характеристиками могут служить связанные между собой последовательности команд. Такой подход является более эффективным, так как анализ закономерностей в последовательностях команд позволяет получить более конкретные сведения о действиях и намерениях оператора в процессе его взаимодейст-

вия с РТК и более точно произвести обнаружение аномалии при её наличии.

На практике были рассмотрены различные задачи, решаемые с использованием ИНС, типы ИНС, используемые для решения этих задач и методы применения данных задач к процессу обнаружения аномальных событий в процессе управления РТК.

Учитывая динамический и последовательный характер процесса управления РТК, такой подход может показаться наиболее подходящим при построении систем обнаружения аномалий, так как возможность учитывать взаимосвязь между различными командами позволит системе более эффективно выполнять свои функции.

Задача прогнозирования в контексте обнаружения аномалий управления РТК будет заключаться в определении возможной следующей команды РТК на основе информации о предыдущих. При этом, если полученная команда будет значительно отличаться от возможных прогнозируемых, то можно сделать вывод об аномальном поведении.

Кроме того, рекуррентные нейронные сети могут быть использованы и для решения задач классификации как персептроны, при этом, при анализе потоковых данных, к которым относятся последовательности команд управления РТК, они способны выдавать лучшие результаты [9].

К сожалению, появление обратных связей привносит некоторые сложности, связанные с изменением структуры ИНС. Классические алгоритмы обучения, используемые для сетей прямого распространения, не могут быть использованы для обучения таких ИНС.

Становится понятно, что ИНС позволяют эффективно решать различные задачи, связанные с обнаружением аномального поведения в процессе управления РТК. Таким образом, использование ИНС позволит повысить защищённость систем дистанционного беспроводного управления РТК и обеспечить более высокий уровень безопасности процесса управления по сравнению с традиционно-используемыми средствами защиты, так как помимо криптографического подхода использует подход, построенный на анализе поведения системы.

Список используемых источников

1. Жук А. П., Осипов Д. Л., Гавришев А. А., Бурмистров В. А. Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 2. С. 38–42.

2. Лаута О. С., Никитин В. В., Клиншов И. А., Лаута А. С. Нормативно-правовые документы США, регламентирующие политическую и военную деятельность в киберпространстве // Материалы конференций ГНИИ «НАЦРАЗВИТИЕ», ноябрь 2016. С. 118–125.

3. Коцыняк М. А., Лаута О. С., Осадчий С. А. Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика» // Информация и космос. 2013. № 3–4. С. 25–27.

4. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Модель таргетированной кибернетической атаки // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 90–98.

5. Баранов В. В., Иванов Д. А., Коцыняк М. А., Московченко В. М., Нечепуренко А.П. Применение метода топологического преобразования стохастической сети для моделирования системы воздействия // Актуальные проблемы обеспечения информационной безопасности труда. Межвузовской научно-практической конференции. 2017. С. 38–43.

6. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. 2017. С. 420–425.

7. Елисеев А. И., Долгов А. А., Хорохорин М. А., Лаута О. С., Набатов К. А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести) // Вестник Воронежского института ФСИН России. 2013. № 1. С. 91–94.

8. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83–89.

9. Васюков Д. Ю., Коцыняк М. А., Коцыняк М. М., Лаута О. С., Лаута А. С. Устройство обнаружения удаленных компьютерных атак. Патент на изобретение RUS 2540838 03.03.2014.

УДК 004.94

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ ДЛЯ СОЗДАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

Д. В. Волошинов, Р. Т. Кантарбаев, А. М. Сосновских

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

Разработка мобильных приложения в последние 10 лет является одним из самых перспективных и быстроразвивающихся направлений на рынке программного обеспечения. Использование технологии отображения объектов на экранах различных устройств позволяет пользователю получать информацию не только в текстовом виде,

но и в графическом, что, несомненно, ускоряет процесс получения информации и улучшает ее общее восприятие. В статье предлагается новая методика реализации процесса отображения трехмерных объектов с помощью графических меток.

аргумент, реальность, 3D, единство, виртуальная реальность.

Несмотря на бурное развитие технологий разработки приложений с дополненной реальностью, в настоящее время не существует какого-либо универсального подхода к решению таких задач, а также унифицированных программных систем для их реализации. Это связано, прежде всего, с большим разнообразием целевых условий, ставящихся перед подобными приложениями. Таким образом, задачи проектирования приложений с дополненной реальностью строятся с применением систем моделирования, предназначенных, в основным, для иных, нежели дополненная реальность, задач геометрического моделирования и компьютерной графики. Проводимые авторами исследования направлены на поиск единых методик проектирования дополненной реальности и консолидации этих средств в виде программного комплекса под управлением конструктивного геометрического моделирования.

Для оперативной разработки мобильного приложения с дополненной реальностью предлагается реализовать следующий сценарий проектирования:

– осуществить синтез трехмерной полигональной модели отображаемого объекта;
– разработать сцену в программной среде Unity;
– настроить библиотеку отображения трехмерных объектов;
– применить изменения к графическим меткам.

Выбор в качестве средства моделирования трехмерной полигональной модели обусловлен следующими соображениями. В отличие от твердотельного, полигональное моделирование формы трехмерных объектов имеет ряд преимуществ. Среди этих преимуществ следует отметить, во-первых, относительную простоту синтеза полигональной модели конструктивными геометрическими методами, а во-вторых, доступность средств преобразования полигональных моделей в референсные модели системы программирования сцен дополненной реальности Unity. Немаловажным является также и то обстоятельство, что большое количество доступных для применения программ трехмерного моделирования, таких как: Cinema4d, 3dsMax, Blender имеют средства оперативной редакции и синтеза полигональных моделей сложных геометрических форм, которые практически невозможно реализовать в системах твердотельного моделирования [1].

В настоящем исследовании для иллюстрации результатов проектирования приложения была применена система полигонального моделирования Cinema4D от компании Maxon, а в качестве объекта визуализации взята регулярная геометрическая конструкция, представленная полигональной трехмерной моделью здания часовни Святой Параскеева. Использование шейдера позволяет увидеть позволяет продемонстрировать на (рис. 1) полигональную сетку, что является исключительно важным для оценки целостности модели и отсутствия в ней ошибок, поиск и устранение которых является трудноформализуемой задачей [2].

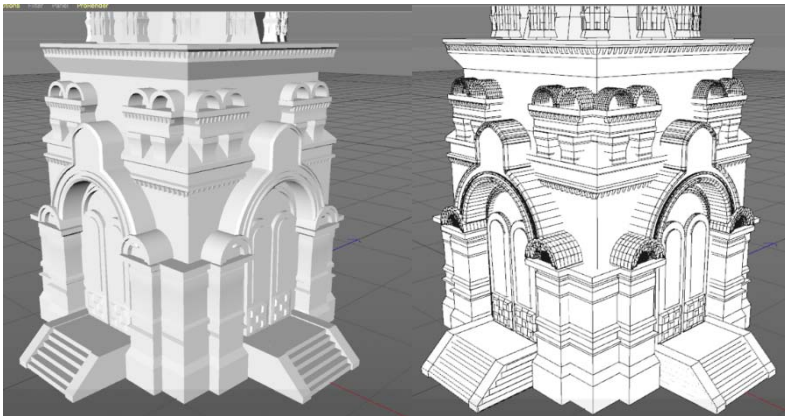


Рис. 1. Отображение полигональной сетки на трехмерном объекте

После создания трехмерной модели и контроля целостности полигональной сетки можно прейти к этапу экспорта полигональной модели. Безусловно, для этого должна быть обеспечена совместимость передаваемых между системами данных. Поскольку дальнейшие манипуляции с трехмерными моделями предполагается производить в программе Unity, необходимо выбрать формат передачи данных, совместимый с этой системой, например, 3ds (3D *StudioMax*, *Autodesk*), dae (*Collada*), obj (*Wavefront* OBJ). Возможно также использование формата обмена данными dxf, однако ввиду его насыщенности избыточными тегами и записями, объем такого файла в задачах полигонального моделирования становится невероятно большим, и его вряд ли можно рекомендовать для передачи подобных данных [3].

Для создания сцены с учетом работы мобильного приложения с дополненной реальности необходимо загрузить дополнительную библиотеку, позволяющую отображать трехмерные полигональные файлы на области видео и содержащую заданную в программе метку. Для проведения исследований была выбрана библиотека EasyAR, так как она совместима со средой Unity и имеет бесплатную версию, удовлетворяющую всем вышеперечисленным требованиям.

Основная проблема отображения полигональных моделей на основе графических меток, которая присуща большинству библиотек, это отсутствие возможности создания и использования в них графических меток пользователя. В связи с этим в исследовании была поставлена и решена задача загрузки в библиотеки собственных меток, а также прикрепление этих меток к полигональным объектам.

Таким образом, была обеспечена возможность по использования любых графических элементов в качестве объектов отображения, что невозможно было бы сделать с использованием стандартных библиотек.

Проведенный анализ показал, что в качестве меток, в принципе, могут быть использованы любые изображения, однако лучшие результаты их распознавания и более надежная работы программ, достигается, если метки монохромны и имеют асимметричную форму. В связи с этим было предложено использовать для целей распознавания QR-коды с именами объектов, дополненные графическими элементами (рис. 2).

После добавления всех необходимых файлов можно приступать к заполнению сцены. Для этого на сцену следует поместить пресет «EasyAR_startup», в котором содержатся настройки камеры, контроллер меток и плоскость, на которую будет проецироваться видео. Для работы приложения необходимо создать ключ на сайте библиотеки. Созданный ключ вносится в соответствующее поле на пресете.

Рис. 2. QR метка

Далее на сцену добавляется примитив метки. В качестве хранилища следует выбрать «Assets», установить размеры метки, задать имя файла со списком меток и имя, присвоенное в нём для необходимой метки.

Для прикрепления модели к метке достаточно просто добавить его на сцену в качестве объекта, зависимого от метки. После установки масштаба и поворота модели к метке также добавляется объект, отображающий его имя.

Так как метка будет закреплена на стене, то доступ к объекту будет ограничен. Для удобства просмотра к каждой модели предложено добавить анимация поворота. Анимация создавалась с использованием методов Unity. После этого необходимо добавить изменяемый параметр – поворот. Последний шаг – создание тринадцати точек на временной шкале, в которых задаётся угол поворота в определённый момент, и установка плавности перехода между ними во вкладке «Curves».

Для создания исполняемого файла под определенную операционную систему, необходимо сгенерировать исполняемый файл для установки на мобильное устройство.

Таким образом, в результате проведенных исследований и разработок показано, что использование программного пакета Unity при наличии трехмерной полигональной модели, библиотеки EasyAR с предложенными программными изменениями и внедрением собственных графических изображений в виде меток, позволяет получить полноценное кроссплатформенное мобильное приложение, отличающееся повышенными характеристиками надежности отображения и распознавания меток.

Использование сложных графических двухмерных изображений в качестве объектов отображения и внедрения таких объектов в библиотеки Unity, позволяет сделать предположение о том, что возможности отображения трехмерных объектов на основе трехмерных объектов тоже возможно с применением сложных текстур.

Списки используемых источников

1. Туголукова М. А., Борисова Е. П. Техническое обеспечение создания виртуальной и дополненной реальности // Виртуальная и дополненная реальность – 2016: состояние и перспективы. Сборник материалов Всероссийской научно-методической конференции, 28–29 апреля 2016 г. С. 62–63.

2. Кираковский В. В., Коротаев А. Н., Пылькин А. Н. Использование технологии дополненной реальности для получения информации о зданиях и сооружениях различного типа // Виртуальная и дополненная реальность – 2016: состояние и перспективы. Сборник материалов Всероссийской научно-методической конференции, 28–29 апреля 2016 г. С. 41.

3. Якунова И. А. Об образе виртуальной реальности // Виртуальное пространство культуры. Конференция 11–13апреля 2000 г. СПб.: Санкт- Петербургское философское общество, 2014. С. 62–63.

УДК 004.921

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ГРАФИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ВИЗУАЛИЗАЦИИ ДАННЫХ

Д. В. Волошинов, В. С. Селезнев

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

Актуальной проблемой на сегодняшний день является создание и поддержка различного рода геометрических алгоритмов в различных САПР системах. В большинстве современных САПР используются почти одинаковые представления данных. В верхней части находятся сборки, с деталями внизу и отдельными чертежами. Части определяются либо параметрические, либо явно с их топологией, определенной с помощью модели сплошного граничного представления, состоящей из поверхностей NURBS (не-

равномерного рационального сплайна). Эти поверхности плотно связаны друг с другом с использованием данных допусков. Все осложняется еще тем что различные системы САПР обрабатывают допуски по-разному. Чаще всего при переводе файла из одной системы в другую принимающая система пропускает некоторые допуски, что приводит к модели с отверстиями или зазорами. Модель будет часто появляться в виде поверхностных патчей, которыми вы затем управляете, и смотрите, сможет ли программа сшить эти поверхности в сплошную модель. Причина, по которой системы CAD имеют проблемы с допуском, связана прежде всего с неточностями математических алгоритмов, написанных для ядер геометрического моделирования.

геометрические алгоритмы, модель, данные, система.

Причина, по которой системы CAD имеют проблемы с допуском, связана прежде всего с неточностями математических алгоритмов, написанных для ядер геометрического моделирования. Более того, собственные форматы САПР еще больше увеличивают сложность, поскольку каждая система САПР рассматривает поверхности и топологию по-разному. Стандартные форматы, такие как IGES и STEP, имеют свои собственные проблемы. Поскольку они открыты, любой может попытаться написать файлы в формате, независимо от того, компетентен (валидирован) он или нет, что может привести к множеству ошибок. Но на самом деле проблема лежит еще глубже из-за неосознанности того что CAD(САПР) системы представляют конченый вариант геометрической модели и не является по сути своей работающей программой. Что не позволяет этой модели проявить все свои закономерности и свойства. Конечно, в большинство CAD систем имеют в себе встроенный программные интерфейс, такой как AutoLISP в AutoCAD и Python в Maya. Такие интерфейсы позволяют добавить логику в модель, но являются по сути своим инструментом, облегчающим и автоматизирующим построение модели. Для пользователей, которые не знакомы с программированием будет сложно освоить данный инструмент.

Такой интерфейс, для разработки геометрических алгоритмов, является менее подходящим. Так как пользователю приходиться работать не только с самой моделью и реализующим его алгоритмом, но и логикой самого интерфейса. Создание и изменение программного кода выполняется вручную. Такой псевдокод требует транслирования на язык ЭВМ. Интерпретатору требуется время на выполнения этих команд. Обычный простой цикл выполняется очень медленно. Такие инструменты приводят к увеличению времени, которые необходимы на обработку скриптом.

Наилучшим вариантом разработки геометрического алгоритма является программный подход, основанный на визуальном динамическом программировании геометрических данных. Суть которого состоит в том, что разработчик работает над геометрическими сущностями как с обычными объектами в ООП. Не задумываясь над тем как описать логику вы-

полнения того или иного алгоритма так как вся логика поведения объектов уже описана.

Достаточно знать основные понятия конструктивной геометрии, чтобы начать работать.

Одной из разработок является программа Simplex, автор которой Волошинов Д. В., в которой при создании объектов получается динамическая модель. При изменении параметров, на выходе получают не только измененную модель, но и программный код реализующий геометрический алгоритм. С каждым разом в данное ПО внедряются новые улучшения для работы с экспортом геометрических алгоритмов в MaxScript, SVG, Pascal.

На примере преобразования поляритета создадим алгоритм в ПО Simplex. Поляритет, полярное преобразование, – корреляцияр, для которой $p^2 = id$, то есть $p(y) = x$, тогда и только тогда, когда $p(x) = y$. Поляриет разбивает все подпространства на пары, в частности, если пара образована подпространствами S_0 и S_{n-1}, где $S_0 = n(S_{n-1})$ – точка, а $S_{n-1} = P(S_0)$ – гиперплоскость, то S_0 наз. полюсом гиперплоскости S_{n-1}, а S_{n-1} называют полярой точки S_0. Пространство $P_n(k)$ над телом *K* обладает поляритет, тогда и только тогда, когда тело допускает инволютивный инверсный автоморфизм *a* (т. е. $a^2 = id$). Пусть p представляется полубилинейной формой $f_a(x, y)$. Тогда p будет поляритетом в том и только в том случае, когда из $f_a(x, y) = 0$ следует $f_a(y, x) = 0$ [1].

Поляра точки *P* относительно невырожденной кривой второго порядка – множество точек *N*, гармонически сопряжённых с точкой *P* относительно точек *M*1 и *M*2 пересечения кривой второго порядка секущими, проходящими через точку *P* [2].

Пусть на плоскости заданы две коники и точка. Тогда, принимая точку за полюс, мы с вами можем построить две поляры: одну, используя красную конику, другую – используя синюю конику. Поскольку поляры являются прямыми и в нашем случае не совпадают, то найдут точку пересечения (оранжевая точка на чертеже).

Тем самым задали преобразования т.н. квадратичной инволюции, переводящей исходную черную точку в ее образ – точку оранжевую. Данное преобразование можно увидеть на рис. 1.

Инволюционным является такое преобразование, которое переводят исходную точку и ее образ друг в друга. И в этом преобразовании наблюдается именно это явление. Чтобы получить дополнительные образы возьмем прямую линию. Оказывается, прямая линия квадратичной инволюцией преобразуется в конику на рис. 2.

Если будут использоваться три различные прямые и преобразуются в три коники. Они будут пересекать друг друга в постоянных точках, на рис. 3 можно увидеть данное пересечение.

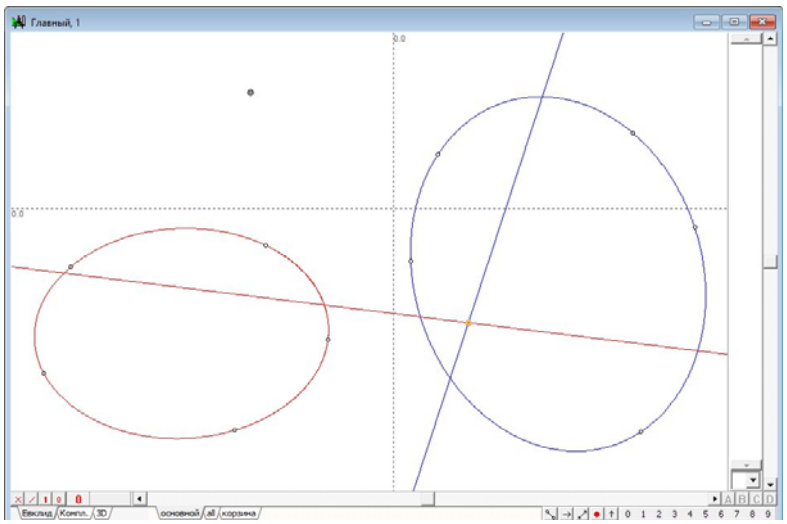


Рис. 1. Заданы на плоскости две коники и точка. Получена инволюция

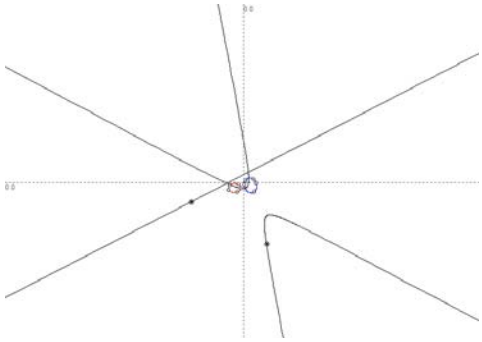


Рис. 2. Преобразование прямой линии квадратичной инволюции преобразуется в конику

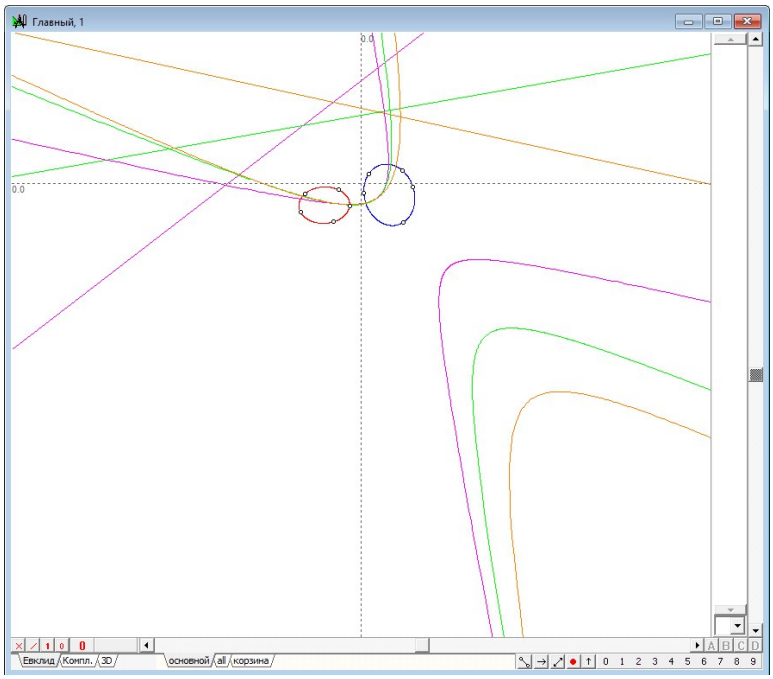


Рис. 3. Пересечение 3-х прямых в постоянных точках

Это вершины автополярного треугольника. И получить их можно заранее, даже не пересекая только что полученные точки, показаны на рис. 4.

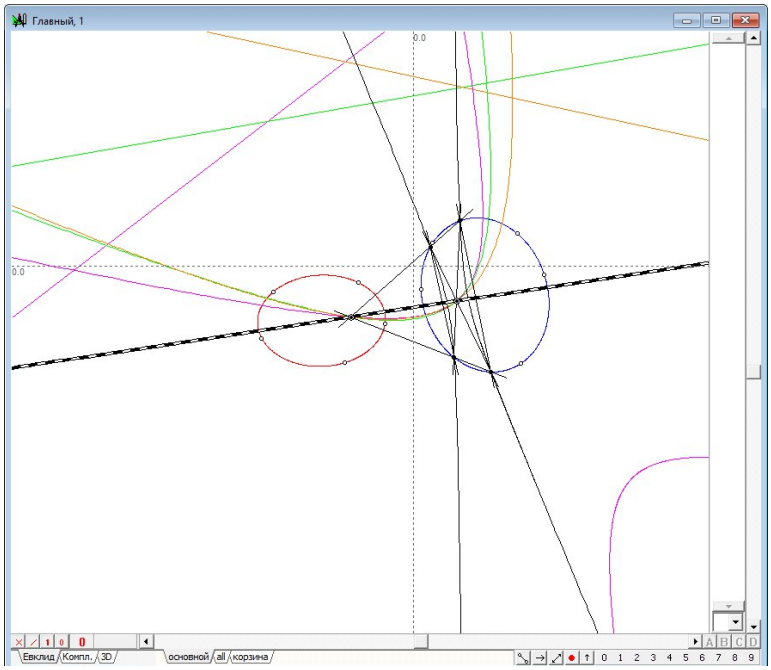


Рис. 4. Автополярный треугольник

Три вершины автополярного треугольника носят название фундаментальных точек. Фундаментальны они тем, что они строго фиксированы и определяются взаимным положением коник, задающих преобразование квадратичной инволюции.

В данном примере получилось инволюционное преобразование. Это значит, что если прямая переходит конику, то и коника переходит в прямую. Но не любая коника плоскости, а только та, что проходит через фундаментальные точки преобразования. Другие коники преобразуются в более сложные кривые четвертого порядка.

Произвольная коника задается пятью точками. На примере имеется три фиксированные точки, значит свободных остается две. А через две произвольные не совпадающие точки плоскости, как следует из аксиом Эвклида, проходит одна и только одна прямая. Это значит, что в примере, коника – это прямая. Прямую невозможно отличить, опираясь на аксиомы несмотря на то, что визуально выглядит «кривой».

В ходе улучшения данного ПО Simplex и улучшения восприятия данных полученными через данное ПО ввести поддержку или конвертацию формата в читаемый для браузеров. Сейчас для браузеров распространена библиотека для графического отображения WebGL позволяющая на языке JavaScript создавать различные графические объекты [3]. На данный момент поддержка частично реализована и на примере преобразования поля-

ритетов в браузере 2D изображение включая интерактив изображено на рис. 5:

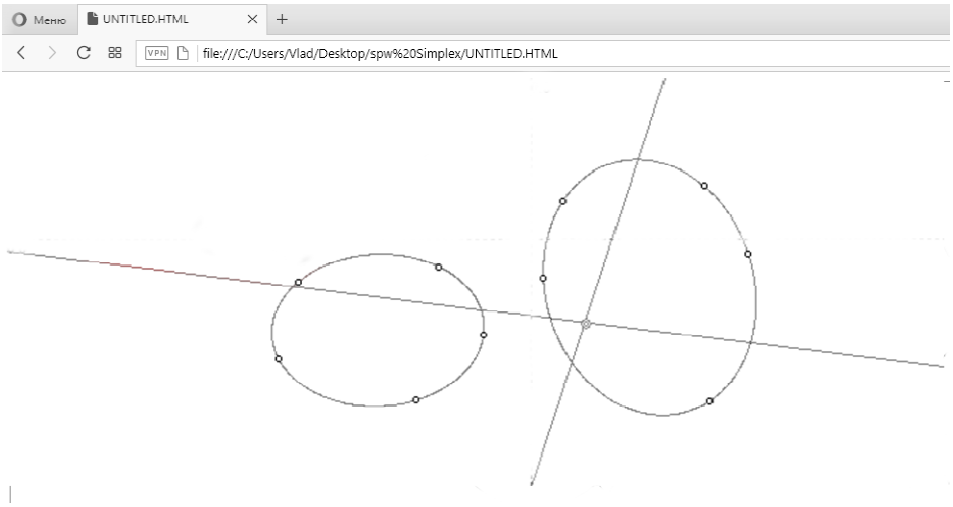


Рис. 5. Отображение графического алгоритма в браузере

Список используемых источников

1. Ефимов Н. В., Высшая геометрия, 6 изд., М., 1978. 576 с.
2. Постников М. М., Аналитическая геометрия, М., 1973. 754 с.
3. Коичи Мацуда, Роджер Ли, А. Киселев, WebGL. Программирование трехмерной графики. 2015. 494 с. ISBN 978-5-97060-146-4.

УДК 30.607.8

ИССЛЕДОВАНИЕ СТИЛЕВЫХ ОСОБЕННОСТЕЙ ЛОГОТИПОВ В ТОРГОВОЙ ОБЛАСТИ ДЛЯ ОПТИМИЗАЦИИ ПРОЕКТИРОВАНИЯ ФИРМЕННОГО СТИЛЯ

Д. В Волошинов, Е. А Склярова

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

На сегодняшний день, понятие фирменного стиля устойчиво вошло в лексикон как дизайнеров, так и рекламистов. Логотип – это основа фирменного стиля. Логотип должен отражать основную деятельность фирмы, быть узнаваем везде и в любом масштабе. Логотип является «негласной» рекламой и очень влияет на эмоциональную привязанность потребителей. Настоящая статья посвящена решению

проблем, связанных с задачами усовершенствования концепта создания логотипов средствами информационных систем.

фирменный стиль, логотип, дизайн.

Фирменный стиль – это достаточно уникальное и популярное явление в XX веке. На сегодняшний день это понятие устойчиво вошло в лексикон как дизайнеров, так и рекламистов. Профессиональный рынок растет с каждым днем, а вместе с ним и конкуренция между дизайн-студиями, которые предлагаю подобные услуги – создание фирменного стиля предприятия. Создание фирменного стиля всегда основано на концепции предприятия: чем оно занимается, что требуется создать, что требуется выделить. Необходимо выделить целевую аудиторию, которая потребляет продукт выбранного предприятия, место будущего объекта на рынке, а также уникальность торгового и бизнес предложения. И только после того, как были четко обозначены позиции предприятия, поставлены необходимые задачи, можно преступать к воплощению. Только после выше описанных задач возможна грамотная разработка фирменного стиля.

Фирменный стиль зародился далеко в древности. Изначально, все элементы были весьма примитивны. Мастера ставили на свои изделия персональное клеймо. Покупатели, приобретая изделия, искали продукцию именно с тем клеймом, чей мастер завоевал их доверие. Создавалась репутация мастера. Прототипом клейма на сегодняшний день является логотип, о котором и пойдет речь в данной статье.

Логотип – это основа фирменного стиля. Как правило, это знак, который состоит из текста и/или графического знака. Это знаки, образы, которые созданы для легкого распознавания. Он выделяет фирму среди других предприятий, работающих в такой же сфере. Логотип должен отражать основную деятельность фирмы, быть узнаваем везде и в любом масштабе. Некоторые люди считают, что логотип, это всего лишь некий символ, содержащий абстрактный или конкретный элемент. Однако логотип может быть и сочетанием графического символа и букв, цифр, знаков пунктуации. Буквенная часть может быть набрана фирменным шрифтом, быть сочетанием букв, инициалами и так далее. Иногда можно увидеть сочетание, где буква или несколько букв изображают собой некий образ, отражающий деятельность компании.

Целью проводимого исследования является создание методического и алгоритмического комплекса, обеспечивающего разнообразие выбора логотипов заказчиками и расширение возможностей проектирования логотипов их разработчиками. Для достижения поставленной цели потребовалось решить следующие задачи:

– рассмотреть теоретические основы развития фирменного стиля;

– изучить понятие фирменного стиля;

– изучить эволюцию создания фирменного стиля;

– изучить психологические особенности визуального восприятия фирменного стиля человеком;

– изучить роль фирменного стиля в создании имиджа компании;

– изучить методологию разработки логотипов. Правила и принципы создания;

– рассмотреть подходы к разработке логотипа;

– рассмотреть классификации логотипов;

– изучить программное обеспечение для реализации проектирования логотипов.

– воплотить полученные результаты в виде комплекса методик и алгоритмов проектирования.

В ходе исследования, было отобрано некоторое множество существующих логотипов и все они были отсортированы по категориям. Данная классификация была сделана на основе книги Майкла Эвами, который детально описал каждый из пунктов [1]. На рисунке (см. ниже) представлена классификация.

Все логотипы можно разделить на три большие категории:

1. Символьные – это те логотипы, при создании которых используются некие фигуры, зачастую самые простые (квадраты, круги, стрелки, треугольники и т. д.). Их можно разделить на три категории:

– Конкретные. Содержат в себе вполне конкретный, узнаваемый образ.

– Абстрактные. Чаще всего, это набор линий, фигур, очень редко текста.

– Репрезентативные. При создании этого логотипа использованы вполне конкретные образы, но созданные с помощью простых графических элементов и приемов.

– Комбинированные логотипы объединяют в логотипе и символьную и буквенную части.

2. Буквенные логотипы не менее популярны. Они используются для того, чтобы сделать акцент на узнаваемости имени компании.

С развитием интернет-технологий появилась тенденция создания интернет-магазинов. Зачастую, это магазины, которые не имею собственного офиса и работают исключительно в сети. С каждым днем появляется все больше интернет-магазинов, и у каждого появляется необходимость выделяться среди других, повышать популярность. В интернете, как правило, любой сайт встречают «по одежке», оценивают удобство пользования и насколько ответственно разработчики подошли к разработке дизайна и

эргономике сайта. Сайд, имеющий только белый фон и текст вызывает, скорее подозрение, чем интерес.

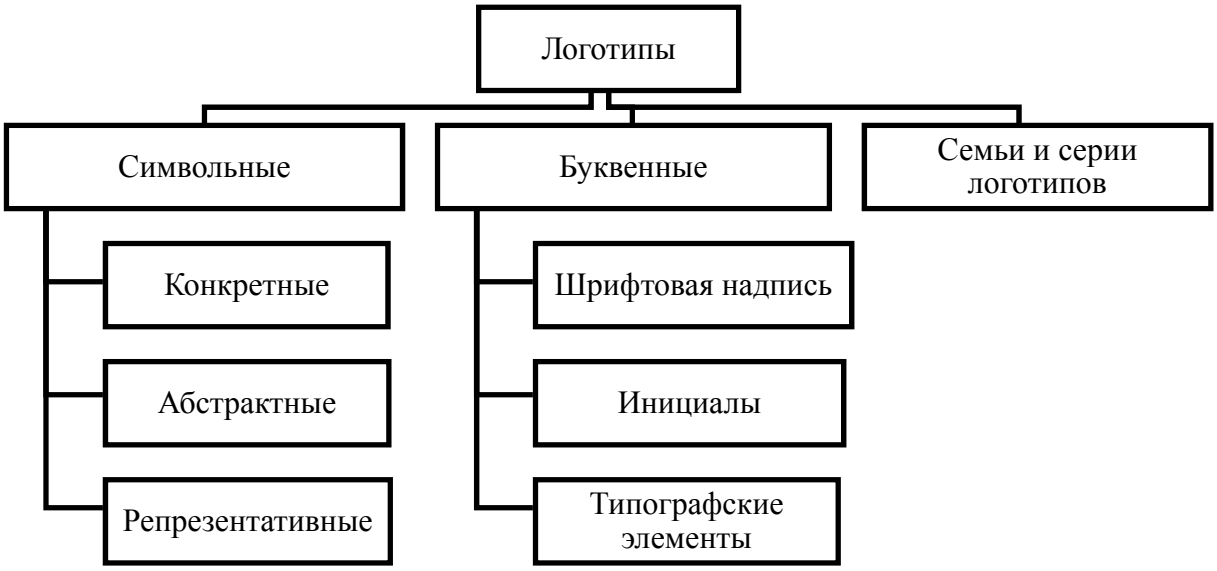


Рисунок. Классификация логотипов, представленная Майклом Эвами в [1]

Логотип для интернет-магазина является неотъемлемой частью дизайна. А цветовое решение логотипа в дальнейшем используется в дизайне всего сайта. И стоит отметить, что у логотипов для интернет-магазинов открывается много новых возможностей, которые нельзя отразить в логотипах для печати. Например, добавить флэш-анимацию или создать объемный логотип. При печати объемные логотипы теряют облик, который виден на экране. Но это не значит, что логотип может использоваться исключительно в интернете. Многие переносят его потом на визитки, флайеры и другие носители.

Из сказанного следует сделать вывод о том, что многоцелевое использование логотипа требует создания специальных методик его проектирования, поскольку проектировщику следует учитывать множество факторов визуально-графического представления информации, условия применения которых могут зачатую противоречить друг другу или быть не вполне определенными.

Следовательно, необходимо создать методику проектирования логотипов, с учетом вышеперечисленных факторов, которая могла бы претендовать на некоторую универсальность применения.

В результате проведенных исследований были получены следующие результаты:

1. Реализация методики показала, что многие привычные приемы графического дизайна, которые обычно используются для проектирования логотипов, недостаточны для реализации поставленной в исследовании

цели. Предложены новые приемы проектирования, которые обеспечивают синтез универсальной конструкции логотипа определенного класса, в результате чего логотип будет одинаково хорошо смотреться и на средствах представления электронных документов (на сайте), и на бумажных носителях.

2. Разрабатываемая методика позволяет расширять классификацию логотипов, предложенную Майклом Эвами новыми классами графических объектов, при этом предложенная методика их проектирования остается актуальной.

Список используемых источников

1. Майкл Эвами. LOGO. Создание логотипов. Самые современные разработки. СПб. : Питер, 2009. 352 с.

УДК 681.004

ОСОБЕННОСТИ ПРЕДОСТАВЛЕНИЯ УСЛУГ ТЕХНОЛОГИИ «УМНОГО ДОМА» НА БАЗЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

М. Ю. Волщуков, С. Р. Мамедов

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

В настоящие время информационные технологии стали объединять большое количество различных информационных систем. Они становятся взаимопроникающими, в связи с этим появляются новые возможности. Предоставление услуг потребителям является одной из актуальнейших задач в мире информационных технологий.

С появлением большого количества разнообразных систем, сервисов и технологий возникает проблема их взаимодействия, интеграции и использования. Оптимизировать информационные ресурсы и более гибко ими управлять позволяют разнообразные технологии, в частности на сегодняшний день для решения подобных задач широко используется технология облачных вычислений.

сетевая инфраструктура, технология, умный дом, гетерогенная среда, информационная система, ИТ.

На сегодняшний день информационные технологии объединяют все больше и больше разнообразных ИТ-систем [1]. Они становятся взаимопроникающими, предоставляя за счет этого новые возможности. Передача данных в сетях с распределенной архитектурой и предоставление услуг

потребителям является одной из актуальнейших задач в мире ИТ-технологий.

Развитие информационных технологий привело к ситуации, когда конкретная информационная система становится похожей на многомерные пазлы. Чтобы они совпали, должны быть соблюдены разнообразные требования: интерфейсы на уровне «железа», «состава данных», «программного обеспечения», правила обмена, физическая совместимость и т. д. и т. п.

Одним из необходимых требований к информационным системам становится поддержка ее функционирования в гетерогенной сетевой инфраструктуре.

Данное требование необходимо учитывать на всех уровнях формирования потребностей пользователей в различных сервисах и оценки совместного функционирования в целом всех частей инфотелекоммуникационных систем, проектирования ИТ-инфраструктуры, функционирования процессов обработки, хранения, передачи данных, оптимизации ИТ-ресурсов [1]. С появлением большого количества разнообразных сервисов потребителю становится трудно в них ориентироваться.

Оптимизировать ИТ-ресурсы и более гибко ими управлять позволит технология облачных вычислений [2].

Первые идеи об использовании вычислений как публичной услуги были предложены еще в 1960-х гг. известным ученым в области информационных технологий, изобретателем языка Lisp, профессором MIT и Стэнфордского университета Джоном Маккарти. Появление первой технологии, близкой к современному пониманию термина «cloud computing», приписывается компании Salesforce.com, основанной в 1999 году. Именно тогда и появилось первое предложение нового вида b2b продукта «Программное обеспечение как сервис» (“*Software as a Service*”, *SaaS*).

Далее, история облачных вычислений продолжала развиваться, концепция постепенно выкристаллизовывалась, до тех пор, пока в 2006 г. компания Amazon не запустила платформу Amazon Web Service (AWS), модернизировав свои центры обработки данных, которые, как и большинство компьютерных инфраструктур, использовали лишь 10 % от их емкости.

Облачные вычисления (рис. 1) стали результатом слияния большого количества технологий и направлений [2].

Можно считать, что компания Amazon сыграла ключевую роль в открытии рынка облачных вычислений во всем мире, оптимизировав как собственные ресурсы, так и начав получать с ранее простаивавших ресурсов прибыль. Спустя всего несколько лет, в 2008 г., были анонсированы облачные платформы от Microsoft и Google, Windows Azure и Google App Engine соответственно. В 2010 г. увидел свет первый выпуск платформы Windows Azure.

Рис. 1. Схема взаимодействия компьютеров в базовой эталонной модели OSI

Начиная, примерно 2008 г. рынок облачных вычислений (рис. 2) начал стремительно вырастать, заполняясь как типовыми игроками (*Amazon*, *Microsoft*, *Salesforce*, *Google*, HP, *Del*l, AT&T, *RackSpace*), так и организациями, предлагающими облачные ресурсы для решения конкретных задач (*Engine Yard*, *gCloud3*, *OrangeScape*).

Рис. 2. Ретроспектива развития ИТ технологий

На данный момент большинство облачных инфраструктур развернуто на серверах дата центров, используя технологии виртуализации, что фактически позволяет любому пользовательскому приложению использовать вычислительные мощности, совершенно не задумываясь о технологических аспектах. Тогда можно понимать «облако» как единый доступ к вычислениям со стороны пользователя. С понятием облачных вычислений

часто связывают такие сервис-предоставляющие (*Everything as a service*) технологии, как «Программное обеспечение как сервис» (“*Software as a Service*” или *SaaS*), «Инфраструктура как сервис» (“*Infrastructure as a Service*” или *IaaS*) и «Платформа как сервис» (“*Plaatform as a Service*”, *PaaS*).

SAP CIS (САП СНГ) и Forrester Russia представили в начале года результаты исследования рынка облачных технологий в России [3]. По результатам исследования, аналитики Forrester Russia сделали вывод, что отечественный рынок облаков будет расти быстрее, чем ИТ-рынок в целом, и к 2020 г. его объем составит 48 млрд руб. То есть при среднегодовом темпе в 21 % рынок облаков вырастет в 3 раза по сравнению с 2015 г. (рис. 3).

Рис. 3. Прогноз объема рынка облачных услуг в России в 2015–2020 гг.

Настоящий вопрос актуализируется ввиду не устоявшихся требований и часто противоречивого понимания облачных технологий, используемых в различных областях человеческой деятельности.

В современном мире все большую популярность набирает концепция Internet of Things, которая включает в себя и так называемые «Умные дома» или «Интеллектуальные здания». «Умные» электроприборы, автоматический контроль энергоснабжение и водоснабжения все чаще встречаются в домах обыкновенных пользователей, как за рубежом, так и в России.

Сегодня системы «умный дом» стали для нас такими же привычными, как и другие технологические разработки последнего поколения. Совре-

менные модели этих устройств оснащены новейшим ПО с интеллектуальным управлением и большим количеством разнообразных функций. Однако, чтобы получить столь совершенный продукт, была проделана огромная работа в разное время и разными людьми.

История технологии «Умного дома» началась в 1961 г., когда Джоэль и Рут Спира изобрели и запатентовали специальное устройство для плавной регулировки света. Именно это изобретение стало поводом для создания всемирно известной сегодня компании Lutron Electronics Company. Первым полноценным проектом «умного дома» стал небольшой жилой дом на южном берегу Англии.

В основу его автоматики легло использование широкополосной KNX-системы, отвечающей за управление освещением, сигнализацией, жалюзи, отоплением и дверями гаража. Также в данном доме был создан бассейн, который впоследствии дополнили LED-системой с оригинальными цветовыми эффектами.

Умный дом (рис. 4) это инженерная система и интерфейс управления всеми устройствами современного жилого пространства.

Рис. 4. Концепция технологии «Умного дома»

Система «Умный дом» – это высокотехнологичная система, позволяющая объединить все коммуникации в одну и поставить её под управление искусственного интеллекта, программируемого и настраиваемого под все потребности и пожелания хозяина [4].

Представим на рассмотрение смоделированную архитектуру сети, на которой будет предоставляться услуга (рис. 5).

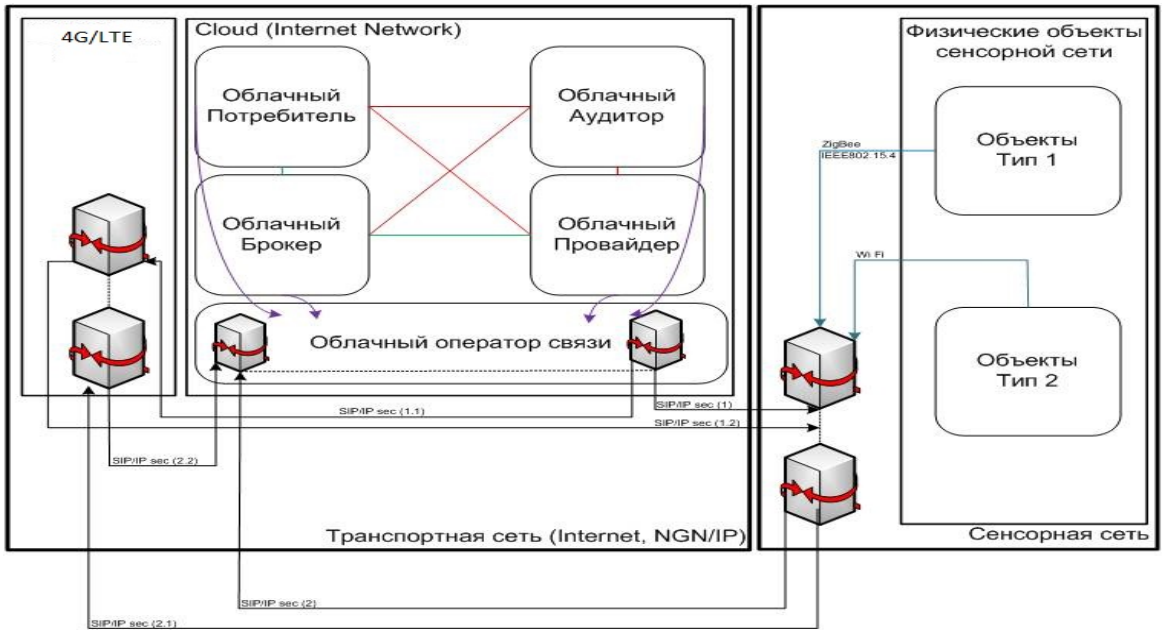


Рис. 5. Архитектура сети предоставления услуг технологии «Умного дома»

Подводя итоги, можно сказать, что в данной статье описываются актуальные вопросы, связанные с оказанием услуг на базе гетерогенных сетей, со значимостью аспекта взаимосвязанного функционирования (интеграции) всех частей инфотелекоммуникационных системы, а также внедрение новых технологий таких, как облачные вычисления и всех их компонентов [1].

В данной статье представлены тенденции развития облачных вычислений, а также требования к стадиям реализации ИТ-решений в гетерогенной среде, обеспечивающие гарантированный результат сбора, хранения, обработки, передачи и представления данных в информационной системе, «живущей» в гетерогенной среде.

Список используемых источников

1. Волщуков М. Ю. Аспекты функционирования информационных систем в гетерогенной сетевой инфраструктуре // Информационные технологии и телекоммуникации. 2017. Том 5. № 3. С. 23–29.

2. Гребнев Е. Облачные сервисы. Взгляд из России. М.: CNews, 2011. 282 с.

3. Литягин П. Е. Объемы и прогнозы развития мирового рынка облачных вычислений // Мир Телекома. 2013. № 1. С. 21–26.

4. Монахов Д. Н., Монахов Н. В., Прончев Г. Б., Кузьменков Д. А. Облачные технологии. Теория и практика М. : МАКС Пресс, 2013. 128 с. ISBN 978-5-317-04400-8.

Статья представлена научным руководителем, доктором технических наук, профессором А. Ю. Ивановым.

УДК 004.056.55

ОСОБЕННОСТИ ТЕМПОРАЛЬНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ

П. А. Волынкин

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

В статье рассмотрена технология шифрования сообщений на базе технологии AES, основанная на уникальной комбинации ключей, каждый из которых имеет свой идентификационный номер. Исследована эффективность темпорального алгоритма по сравнению со статическим методов формирования ключей.

cryptography, ciphers, AES-technology, temporal key formation, Julian date.

В сфере криптографической защиты данных существует несколько современных способов шифрования, комплексное использование которых позволяет обеспечить максимальный уровень сохранности информации и, соответственно, защитить информационные ресурсы от действий злоумышленников.

В данной работе объектом исследования является алгоритм шифрования AES (рис. 1) и способы формирования ключевой информации для создания алгоритма шифрования с высоким уровнем стойкости.

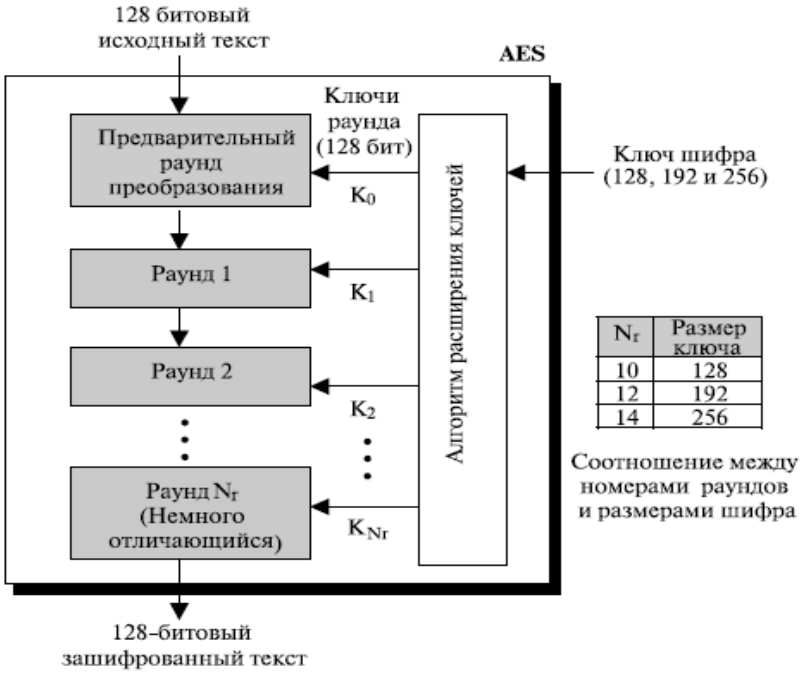


Рис. 1. Принцип AES-технологии шифрования

В процессе шифрования сформированная ключевая информация должна передаваться отправителю и получателю сообщений по защищенному каналу доставки ключевой информации. Под защищенным каналом передачи информации будем понимать канал, в котором нарушитель не способен на успешные пассивные или активные атаки.

Отправитель сообщений шифрует исходное сообщение *M*, принадлежащее пространству сообщений {*M*}, по ключу *e*, используя шифрующее преобразование *E*:

$$\boldsymbol{C = E_e(M).}$$

Образованная криптограмма *C* передается по незащищенному каналу передачи информации получателю. На приеме получатель способен из криптограммы однозначно восстановить сообщение *M* по ключу *d*, используя дешифрующее преобразование *D*:

$$\boldsymbol{M = D_d(C).}$$

Для однозначного восстановления сообщения из криптограммы требуется, чтобы дешифрующее преобразование *D* являлось обратным к шифрующему преобразованию *E* при использовании ключей *d* и *e* соответственно:

$$\boldsymbol{D_d^{-1} = E_e.}$$

Поэтому подставляя первое выражение во второе, имеем окончательный вид расшифрованного текста:

$$M = D_d(E_e(M)).$$

Вопросы выбора соответствующих способов шифрования при построении системы защиты информации включают в себя несколько основных этапов: определение и категорирование основных угроз информации, выбор одиночных или комплексных способов криптографической защиты, расчёт экономической эффективности внедрения выбранного способа и, непосредственно, включение способа криптографической защиты в общую информационную систему.

В качестве базового алгоритма шифрования для дальнейшего рассмотрения в работе выбран алгоритм AES (*Rijndael*) (рис. 2) [2].

Обоснование выбора алгоритма AES:

– высокие скорости на всех существующих платформах,

– одинаково качественная работа как в аппаратной реализации, так и в программной,

– имеется существенный потенциал к распараллеливанию,

– является победителем конкурса NIST (1997 г.) на стандарт симметричного шифрования данных,

– до настоящего времени неизвестно ни одного случая удачно проведённой атаки на AES с получением доступа к данным.

Алгоритм Rijndael стал новым стандартом шифрования данных AES благодаря целому ряду преимуществ перед другими алгоритмами [3]. Прежде всего, он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Кроме того, требования к ресурсам для его работы невысоки, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

В алгоритме AES длина ключа шифрования K равна 128, 192 или 256 бит. Длина ключа показана переменной N_k, равной 4, 6 или 8 и отражающей количество 32-битных слов (количество столбцов) в ключе шифрования. Количество раундов, выполняющихся в процессе работы алгоритма, зависит от длины ключа. Количество раундов показано переменной N_r, где $N_r = 10$, когда $N_k = 4$; $N_r = 12$, когда $N_k = 6$; и $N_r = 14$, когда $N_k = 8$.

Входом и выходом алгоритма AES являются последовательности из 128 бит. Количество бит в блоке называется длиной блока. Базовым элементом, которым оперирует алгоритм AES, является байт-последовательность из восьми бит, обрабатываемых как единое целое.

Алгоритм шифрования AES включает в себя один подготовительный и десять обычных раундов. Алгоритм шифрования заключается в применении четырёх процедур (*SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*) к матрице состояния или, иначе, двумерному массиву данных.

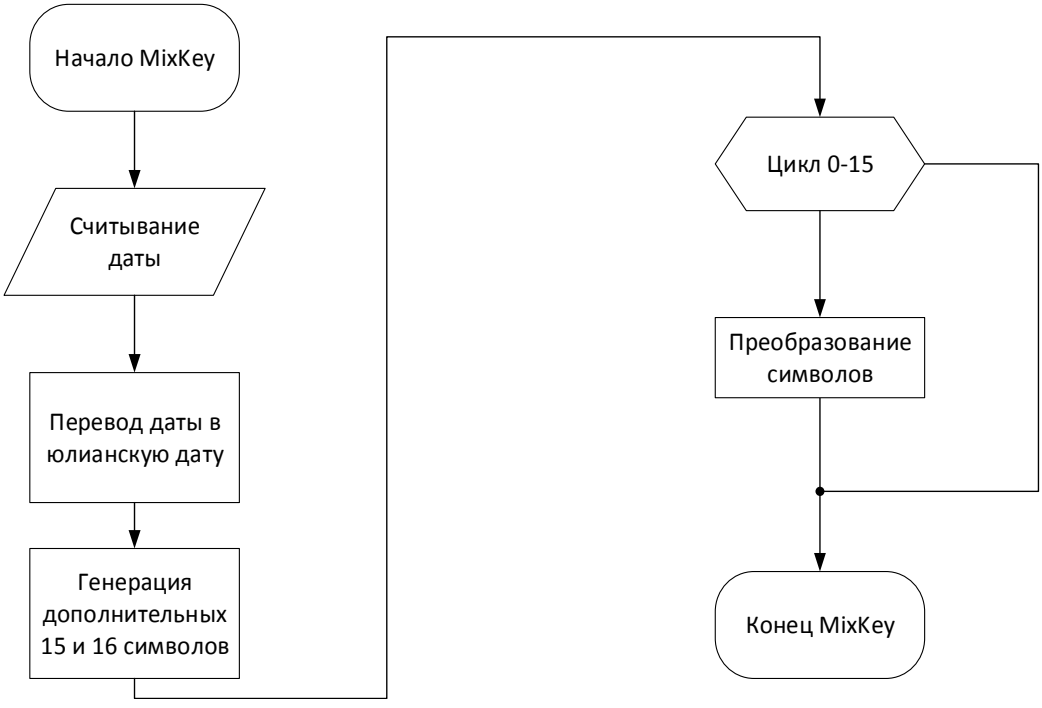


Рис. 2. Алгоритм шифрования информации при AES-технологии

В процедуре SubBytes каждому элементу в матрице состояний однозначно сопоставляется элемент из заданной матрицы – SBox. Сопоставление происходит следующим образом: каждый элемент S_i из матрицы состояния заменяется на соответствующий элемент SBox[S_i], то есть каждый элемент матрицы состояния является порядковым номеров элемента из матрицы SBox.

Процедура ShiftRows циклически сдвигает три последние строки матрицы состояния.

Процедура MixColumns заменяет столбцы матрицы состояния на векторы, полученные при умножении заменяемых столбцов на матрицу.

Процедура AddRoundKey выполняет побитовое сложение соответствующих элементов матрицы состояния с элементами блока RoundKey.

Сущность предлагаемой технологии **темпорального формирования ключевой информации** заключается в следующем.

При шифровании AES-технологией осуществляется многократное преобразовании текста с помощью простой функции, которая зависит от промежуточных ключей, и которая называется раундом шифрования. Чем больше раундов выполняется, тем труднее взломать шифр, но при этом процесс шифрования длится намного дольше, поэтому необходимо обращать внимание на количество раундов, и ограничиваться тем количеством, которое обеспечит надежность и быстродействие алгоритма одновременно.

В данной работе предлагается создание нового алгоритма, в основе которого будет лежать модернизированный алгоритм AES. Модернизацию алгоритма AES предлагается осуществить с помощью динамического формирования ключевой информации, где генерируемые ключи для сеанса шифрования ставятся в зависимость от времени создания текста.

Темпоральный ключ формируется на основе юлианской даты создания текстового сообщения, в дальнейшем он с помощью простых математических операций преобразуется в новый ключ, который и будет использоваться в сеансе шифрования (рис. 2).

Юлианская дата представляет собой вещественное число, целая часть которого увеличивается с каждым днем на единицу (начиная от гипотетической даты сотворения мира), а дробная равна части суток. Таким образом, юлианская дата «чувствительна» к тысячным долям секунды времени. После смешения целой и дробной частей юлианской даты получаем уникальную и меняющуюся каждую микросекунду последовательность цифр, каждая из которых позволяет задавать тот или иной ключ из исходного набора ключей для каждого раунда шифрования.

На основе описанного алгоритма разработана программа, позволяющая исследовать эффективность шифрования с использование темпорального формирования ключей (рис. 3).

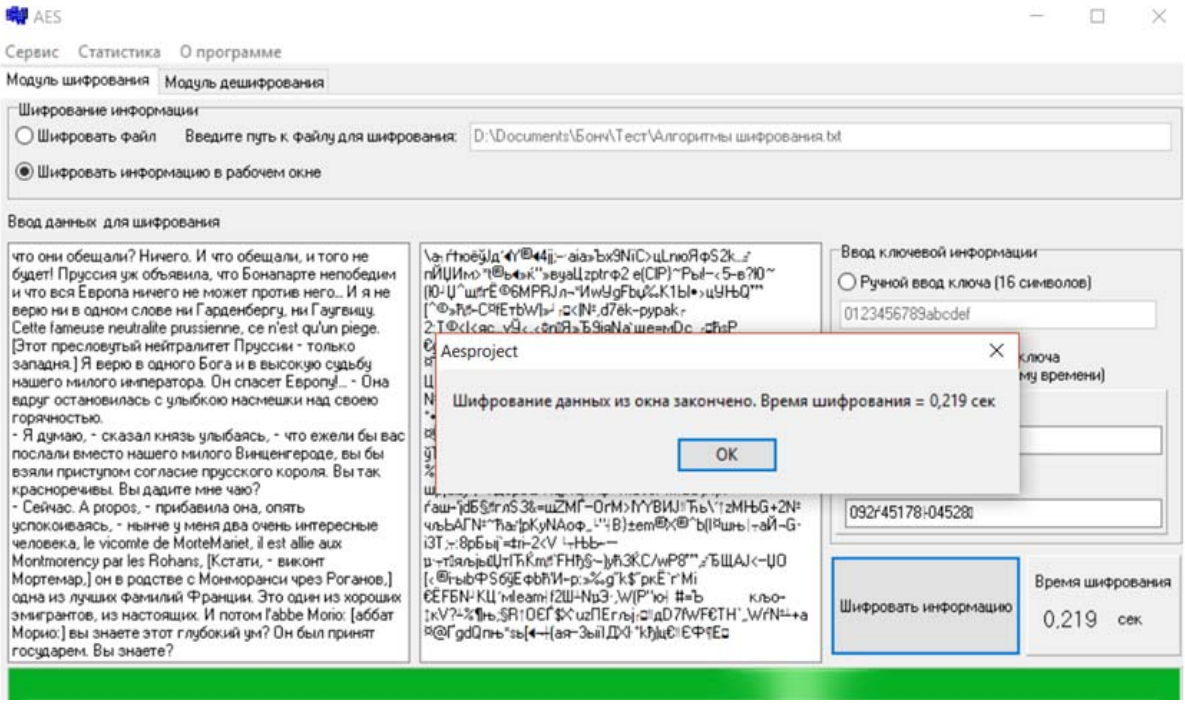


Рис. 3. Программа исследования технологии темпорального формирования ключей

Сравнительная оценка алгоритма темпорального формирования ключей по сравнению со статическим формирование показало, что темпоральное формирование дает выигрыш по производительности порядка 7 %.

Принципиально новая схема создания ключей показала:

– Возможность (теоретически и практически) адаптации технологии динамического формирования ключа для алгоритма шифрования AES.

– Проведенное исследование подтвердило улучшение характеристик шифрования по сравнению со стандартным алгоритмом на 7 процентов.

– Разработанные процедуры в дальнейшем могут быть использованы в других алгоритмах шифрования для улучшения их характеристик и криптостойкости.

Список используемых источников

1. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. М. : Радио и связь, 2001. 376 с.
2. http://mzdm.narod.ru/FIPS-197-Rus.pdf
3. https://csrc.nist.gov/csor/

УДК 004.056.55

ИССЛЕДОВАНИЕ МЕТОДОВ ФОРМИРОВАНИЯ ЧАСТОТНЫХ ПОРТРЕТОВ

П. А. Волынкин, Э. Э. Гянджиев

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

Для каждого человека характерен уникальный комплекс особенностей речевого поведения, который может быть использован для идентификации. Методы такого анализа условно можно разделить на две большие группы – экспертные и формальные. Посредством математических методов и алгоритмов можно сформировать так называемый частотный портрет автора текста. С точки зрения логики представления алгоритм методов частотного анализа основываются в основном на автороведческой экспертизе, используется математическая модель последовательности букв текста. Рассматриваются предпосылки к созданию алгоритма определения авторства текста, а также выявления непринадлежности текста тому или иному автору.

частотный портрет, полиграммы, частоты букв, частоты биграмм, статистический анализ, лингвоанализатор.

Как известно, частоты использования тех или иных букв (одограмм), пар букв (биграмм) и полиграмм (слов) в рамках того или иного языка довольно существенно различаются. Такой набор частот можно называть *частотным портретом языка*.

Кроме этого, даже в рамках одного и того же языка частоты могут существенно различаться в зависимости от темы, области, группы людей (сфера науки, культурной области и т. д.). Будем называть такой *частотный портрет тематическим*.

Более того, текст, написанный автором, содержит в себе помимо смысловой составляющей еще и информацию о личности автора, его индивидуальности и лингвистических особенностях. Такой индивидуальный стиль автора можно назвать *персональным частотным портретом*. Тексты, написанные одним и тем же автором, имеют похожий стиль, свойственный его составителю, а тексты, написанные разными авторами – различаются. Таким образом, если удастся подобрать подходящее правило сравнения текстов, можно формально отличить одного автора от другого, а также решить непосредственно саму задачу авторства или подложности какого-то произведения, текста.

Предметом исследования статьи является изучение, обработка и анализ текстовой информации с целью определения, распознания автора текста или выдачи списка наиболее близких к нему по стилистике авторов

из числа входящих в некоторый заранее заданный перечень «эталонных» авторов, а также дальнейшая разработка собственных методов идентификации текстовой информации.

Универсального метода определения принадлежности или подложности текста априори не существует, поскольку писательский труд – процесс творческий, а не алгоритмический. Так, например, в технических текстах редкая буква ***Ф*** может стать довольно частой в связи с частым использованием таких слов, как функция, дифференциал, диффузия, коэффициент и др., но возможно, что мера, близкая к оптимальной, обнаружится в ходе перебора достаточно большого количества разных вариантов сравнения.

Еще большие отклонения от нормы в частоте употребления отдельных букв наблюдаются в некоторых художественных произведениях, особенно в стихах. Поэтому для надежного определения средней частоты букв желательно иметь набор различных текстов, заимствованных из разных источников.

Известны исследования, где наилучшая точность идентификации автора получены в норме суммируемых функций, благодаря чему авторы текстов определены с качественно более высокой достоверностью.

Также стоит вопрос о том, какой объем текста достаточен для достижения требуемой точности в оценке.

Так, на сегодня, например, для математически точного различения литературных стилей и жанров широко используется *статистический анализ*, который также применяется для установления авторства анонимных текстов, описания поведения различных языковых единиц (букв, морфем, слов) в тексте (их распределение, сочетаемость, частота употребления), восстановления текстов и языков по их фрагментам и определения уровня родства.

Одним из первых исследованиями в этой области занимался известный математик А. А. Марков («Об одном применении статистического метода», «Пример статистического исследования над текстом «Евгения Онегина», иллюстрирующий связь испытаний в цепь»: [1, 2]). Его метод представляет из себя формальную математическую модель последовательности букв текста в виде реализации цепей (цепи Маркова). По тем произведениям автора, которые достоверно им созданы, вычисляется матрица переходных частот употреблений пар букв (биграмм). Она служит оценкой матрицы вероятностей перехода из буквы в букву. Матрица переходных частот строится для каждого из авторов. Для каждого автора оценивается вероятность того, что именно он написал анонимный фрагмент текста. Автором анонимного текста полагается тот, у которого вычисленная оценка вероятности больше. Такой метод оказывается удивительно точным для естественно-языковых текстов.

Текст состоит из слов, слова из букв. Количество букв в разных языках отличаются, их можно перечислить. Повторяемость букв, пар букв – биграмм, и вообще m-граммм, сочетаемость букв друг с другом, чередование гласных и согласных и др. являются важной характеристикой текста, которая устойчива.

Идея состоит в подсчете чисел вхождений каждой n^m возможных m-грамм в достаточно длинных открытых текстах $T = t_1t_2...t_l$, составленных из букв алфавита $\{a_1, a_2, ..., a_n\}$. При этом просматриваются подряд идущие m-граммы текста: $t_1t_2...t_m$, $t_2t_3...$ t_{m+1}, ..., $t_{i-m+1}t_{l-m+2}...t_l$.

Если L $(a_{i1}a_{i2}$ ... $a_{im})$ – число появлений m-граммы $a_{i1}a_{i2}...a_{im}$ в тексте T, а L – общее число подсчитанных m-грамм, то опыт показывает, что при достаточно больших L частоты L $(a_{i1}a_{i2}...$ $a_{im})/L$, для данной m-граммы мало отличаются друг от друга.

Поэтому, относительной частотой здесь считают приближением вероятности P $(a_{i1}a_{i2}...a_{im})$ появления данной m-граммы в случайно выбранном месте текста (такой подход принят при статистическом определении вероятности).

В таблице 1 приведены частоты букв некоторых европейских языков. Данные заимствованы из книги «Вероятность и информация» известных советских математиков братьев А. И. и И. М. Яглом [3].

ТАБЛИЦА 1. Частоты букв (в процентах) некоторых европейских языков

Буква алфавита	Французский язык	Немецкий язык	Английский язык	Испанский язык	Итальянский язык
A	7,68	5,52	7,96	12,90	11,12
B	0,80	1,56	1,60	1,03	1,07
C	3,32	2,94	2,84	4,42	4,11
D	3,60	4,91	4,01	4,67	3,54
E	17,76	19,18	12,86	14,15	11,63
F	1,06	1,96	2,62	0,70	1,15
G	1,10	3,60	1,99	1,00	1,73
H	0,64	5,02	5,39	0,91	0,83
I	7,23	8,21	7,77	7,01	12.04
J	0,19	0,16	0,16	0,24	–
K	–	1,33	0,41	–	–
L	5,89	3,48	3,51	5,52	5,95
M	2,72	1,69	2,43	2,55	2,65
N	7,61	10,20	7,51	6,20	7,68
O	5,34	2,14	6,62	8,84	8,92
P	3,24	0,54	1,81	3,26	2,66
R	6,81	7,01	6,83	6,95	6,56
S	8,23	7,07	6,62	7,64	4,81
T	7,30	5,86	9,72	4,36	7,07
U	6,05	4,22	2,48	4,00	3,09
V	1.27	0,84	1,15	0,67	1,67
W	–	1,38	1,80	–	–

Буква алфавита	Французский язык	Немецкий язык	Английский язык	Испанский язык	Итальянский язык
X	0,54	–	0,17	0,07	–
Y	0,21	–	1,52	1,05	–
Z	0,07	1,17	0,05	0,31	1,24

Разница в значениях частот в различных источниках, как говорилось выше, объясняется тем, что они существенно зависят не только от длины текста, но и от его характера.

Статистика частотности букв русского языка (на материале Национального корпуса русского языка) представлена в таблице 2, рис. 1.

ТАБЛИЦА 2. Частотность букв русского языка

Ранг	Буква	Употреблений	Частотность	Ранг	Буква	Употреблений	Частотность
1	о	55414481	10,97	**18**	ь	8784613	1,74
2	е	42691213	8,45	**19**	г	8564640	1,70
3	а	40487008	8,01	**20**	з	8329904	1,65
4	и	37153142	7,35	**21**	б	8051767	1,59
5	н	33838881	6,70	**22**	ч	7300193	1,44
6	т	31620970	6,26	**23**	й	6106262	1,21
7	с	27627040	5,47	**24**	х	4904176	0,97
8	р	23916825	4,73	**25**	ж	4746916	0,94
9	в	22930719	4,54	**26**	ш	3678738	0,73
10	л	22230174	4,40	**27**	ю	3220715	0,64
11	к	17653469	3,49	**28**	ц	2438807	0,48
12	м	16203060	3,21	**29**	щ	1822476	0,36
13	д	15052118	2,98	**30**	э	1610107	0,32
14	п	14201572	2,81	**31**	ф	1335747	0,26
15	у	13245712	2,62	**32**	ъ	185452	0,04
16	я	10139085	2,01	**33**	ё	184928	0,04
17	ы	9595941	1,90				

Стоит также упомянуть о *Частотных словарях*, который представляют набор слов языка вместе с информацией о частоте их встречаемости. Такой словарь может быть отсортирован по частоте, по алфавиту (тогда для каждого слова будет указана его частота), по группам слов (например, первая тысяча наиболее частотных слов, за ней вторая и т. п.), по типичности (слова, частотные для большинства текстов), и т. д.

Частотные списки используются для преподавания языка, создания новых словарей, приложений компьютерной лингвистики, исследований в области лингвистической типологии, и т. д.

Устойчивыми являются также частотные характеристики биграмм, триграмм и четырехграмм осмысленных текстов.

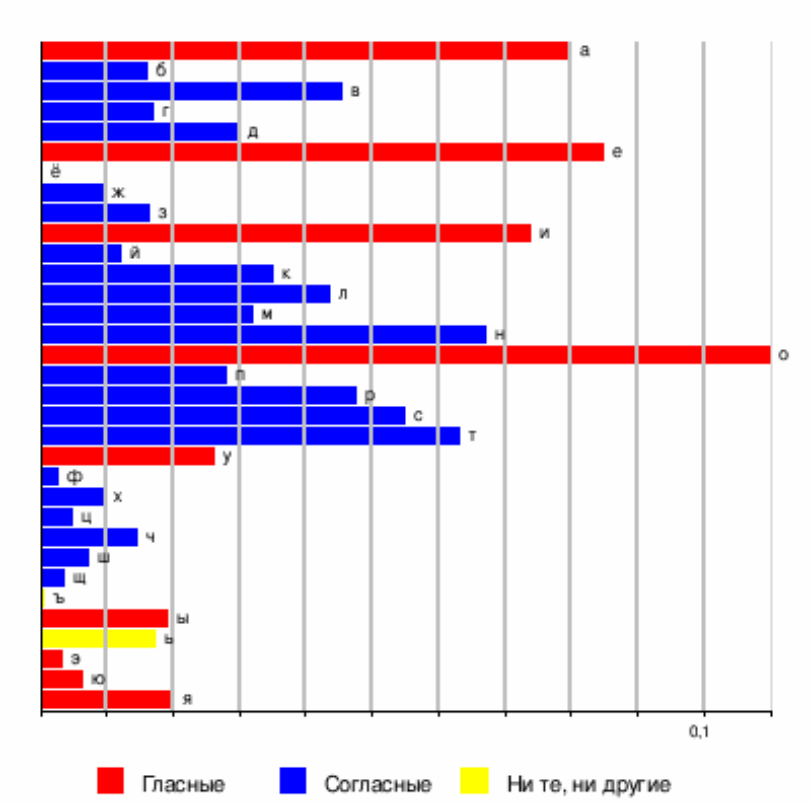


Рис. 1. Частотность букв русского языка

Ниже в таблицах 3.1. и 3.2. приведены частоты биграмм букв (от А до Я) русского алфавита относительно первой (от А до П включительно) и второй (от Р до Я) половин алфавита (от Р до Я) (таблицы заимствована из книги «*Military cryptanalysis*» *Friedman W. F., Callimahos D.*) [4].

ТАБЛИЦА 3.1. Частоты биграмм букв русского языка

б/б	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	5	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
Й	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2

б/б	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	8	1	7	1	2	25			6		40	13	3	9	27	11
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5
Ф	2					2			2						1	
Х	4	1	4	1	3	1		2	3		4	3	3	4	18	5
Ц	3					7			10		2				1	
Ч	12					23			13		2			6		
Ш	5					11			14		1	2		2	2	
Щ	3					8			6					1		
Ы		1	9	1	3	12		2	4	7	3	6	6	3	2	10
Ь		2	4	1	1	2		2	2		6		3	13	2	4
Э											1			1		
Ю		2	1	2	1			3	1		1		1	1	1	3
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6

ТАБЛИЦА 3.2. Частоты биграмм букв русского языка

б/б	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
А	26	31	27	3	1	10	6	7	10	1			2	6	9
Б	8	1		6						1	11				2
В	6	19	6	7		1	1	2	4	1	18	1	2		3
Г	7			2											
Д	6	8	1	10			1	1	1		5	1			1
Е	39	37	33	3	1	8	3	7	3	3			1	1	2
Ж		1													
З	3	1		2							4				4
И	11	29	29	3	1	17	3	11	1	1			1	3	17
Й	3	10	2				1	3	2						
К	10	3	7	10			1								
Л		3	1	6		4		1			3	20		4	9
М	2	5	3	9	1			2			5	1	1		3
Н	1	9	9	7	1		5	2			36	3			5
О	43	50	39	3	2	5	2	12	4	3			2	3	2
П	41	1		6							2				2
Р	1	5	9	16		1	1	1	2		8	3			5
С	4	11	82	6		1	1	2	2		1	8			17
Т	26	18	2	10				1			11	21			4
У	7	14	7			1		8	3	2				9	1
Ф	1	1													
Х	3	4	2	2	1			1							
Ц				1							1				
Ч			7	1					1			1			
Ш				1								1			
Щ				1											
Ы	3	9	4	1		16		1	2						
Ь	1	11	3					1	4				1	3	1
Э		1	9												
Ю	1	1	7				1	1		4					
Я	3	6	10			2	1	4	1	1			1	1	1

Неравномерность *k*-грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался А. А. Марковым (старшим). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (г, г), гласная-согласная (г, с), согласная-гласная (с, г), согласная-согласная (с, с) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

ТАБЛИЦА 4. Частоты чередования согласных и гласных букв

	Г	**С**	**Всего**
Г	6588	38310	44898
С	38296	16806	55102

Из этой таблицы видно, что для русского языка характерно чередование гласных и согласных, причем относительные частоты могут служить приближениями соответствующих условных и безусловных вероятностей:

$$p(г/с) \approx 0{,}663,\ \ p(с/г) \approx 0{,}872,$$

$$p(г) \approx 0{,}432,\ \ p(с) \approx 0{,}568.$$

После А. А. Маркова зависимость появления букв текста вслед за несколькими предыдущими исследовал методами теории информации К. Шеннон. Фактически им было показано, в частности, что такая зависимость ощутима на глубину приблизительно в 30 знаков, после чего она практически отсутствует.

На сегодняшний день для обработки текста существуют лингвоанализаторы, это т. н. программы-атрибуторы, представляющие собой систему для анализа единиц текста, которая автоматически сравнивает тексты по параметрам индивидуального авторского стиля. Первый такой лингвоанализатор принадлежит Д. Хмелеву и работает в сети Интернет с августа 1999 г. [5]. В эталонную выборку, на которой происходило обучение атрибутора, попали в основном романы и повести отечественных писателей XIX–XX веков.

Помимо криптографии частотные характеристики открытых сообщений применяются и в других сферах деятельности. Например, клавиатура компьютера, пишущей машинки – это воплощение идеи ускорения набора текста, связанное с оптимизацией расположения букв алфавита относительно друг друга в зависимости от частоты их применения.

Приведенные выше закономерности имеют место для открытых текстов, используемых при общении людей. Эти закономерности играют большую роль в теории криптоанализа. В частности, они используются при построении формализованных критериев на открытый текст, позволяющих применять методы математической статистики в задаче распознавания открытого текста в потоке сообщений. При использовании же специальных алфавитов требуются аналогичные исследования частотных характеристик «открытых текстов», возникающих, например, при межмашинном обмене информацией или в системах передачи данных. В этих случаях построение формализованных критериев на «открытый текст» – задача значительно более сложная.

В таком направлении будут проводиться дальнейшие исследования. Планируется произвести сравнительный анализ полученных результатов и выявить имеющиеся закономерности, благодаря чему авторы текстов могут быть определены с качественно более высокой достоверностью, реализовать алгоритм на языке программирования, который упростит взаимодействие человека с ресурсом посредством удобного интерфейса, за счет чего будет обладать рядом преимуществ по сравнению с программами-аналогам. В ближайшей перспективе рассматривается задача поиска алгоритмов и их оптимизация по совместному использованию при составлении частотных портретов комбинаций одно- и биграммных лингвистических матриц.

Список используемых источников

1. Марков А. А. Об одном применении статистического метода // Известия Имп. Акад. Наук. Серия VI. Т. X, N 4. 1916. С. 239.

2. Марков А. А. Пример статистического исследования над текстом «Евгения Онегина», иллюстрирующий связь испытаний в цепь // Известия Имп. Акад. Наук. Серия VI. Т. X, N 3. 1913. С. 153.

3. Яглом А. М., Яглом И. М. Вероятность и информация. Издание третье, переработанное и дополненное. М. : Наука, 1973. 512 с.

4. Friedman W. F., Callimahos D. Military cryptanalysis. Part I. Vol. 2. Aegean Park Press, Laguna Hills CA, 1985.

5. http://www.philol.msu.ru/~lex/khmelev/descrwin.html

УДК 004.056.55

ИССЛЕДОВАНИЕ ПРИНЦИПОВ ШИФРОВАНИЯ МУЛЬТИМЕДИА ИНФОРМАЦИИ В ГРАФИЧЕСКИХ ФАЙЛАХ

П. А. Волынкин, А. С. Севостьянова

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

В настоящее время вопросы по защите информации являются наиболее актуальными, так как несанкционированный доступ к данным активно развит. Для того чтобы уберечь информацию, существуют различные методы шифрования. В данной статье рассматривается принцип шифрования мультимедиа информации в графических файлах. Главной задачей такого способа является итоговое наличие в обычном изображении какого-либо голосового сообщения, музыкального сопровождения или звука. Возможно, при создании могут возникнуть сложности с размером мультимедиа файла, но реализация данного метода поможет уменьшить риск в уязвимости информации от злоумышленников.

защита информации, шифрование, мультимедиа, графические файлы, звуковая информация, стеганография.

В поисках решения проблемы защиты информации при ее передаче между абонентами человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от злоумышленников. На практике выработалось несколько групп методов защиты секретных посланий.

По форме представления послания могут быть текстовыми, графическими, видео и звуковыми. Хотя в конечном счете послание любого вида сводится к двоичному представлению.

Для шифрования текстовой информации известно более двух десятков элементарных методов, на основе которых строятся комплексные методы довольно высокого уровня сложности.

В данной работе поставлена задача исследовать методы шифрования мультимедиа информации. Причем, для шифрования выбрана технология стеганографии. Предлагается в качестве контейнера для хранения мультимедиа информации (в частности, звука) использовать графические файлы. Фактически, предлагается использовать обычную картинку, в которой в последующем будет зашифрован некий звук.

Известен принцип шифрования графического файла на основе метода замены цветовой палитры. Такой метод используется для скрытия текста

в картинке. Но по такому же принципу мы в дальнейшем сможем скрыть и звуковой файл.

В основном графические файлы используются в формате BMP, JPEG, GIF, PCX.

Палитра представляет из себя некоторое число триад байт, но не более 256, которые описывают цвет точки по тому же принципу, что и в файлах True color. После палитры следует массив байт, каждый из которых описывает одну точку изображения с содержанием в себе номера цвета в палитре [1, 2].

При использовании данного метода в качестве контейнера рекомендуется выбрать файлы, которые содержат тот или иной цвет в избытке. Это могут быть различные рисунки, схемы, черный текст на белом фоне. Сочетание черного и белого цвета считается оптимальным для реализации данного метода, но можно использовать и другие оттенки.

Вначале создается алфавит. Если сообщение написано на русском языке, значит используется русский алфавит, если же иностранный, то, соответственно, алфавит используемого языка. Берутся буквы от А до Я, цифры от 0 до 9, знаки пунктуации и специальные знаки. Общее количество символов составляет 51 символ. Эти данные заносятся в таблицу 1.

ТАБЛИЦА 1. Алфавит

Код	0	1	2	3	4	…	49	50
Символ	А	Б	В	Г	Д	…	%	;

Затем проводится замена цветов палитры. Для этого первому 51 цвету палитры назначается, в данном случае, цвет рисунка, который является цветом рисунка. Следующему 51 цвету палитры назначается белый цвет соответственно, т. к. это цвет нашего фона. В итоге измененная палитра цветов будет иметь в шестнадцатеричном представлении следующий вид для черного и белого цветов (табл. 2):

ТАБЛИЦА 2. Палитра для черного цвета

Код	0	1	2	…	49	50
Цвет	00 00 00	00 00 00	00 00 00	…	00 00 00	00 00 00

Палитра для белого цвета будет иметь следующий вид (табл. 3):

ТАБЛИЦА 3. Палитра для белого цвета

Код	51	52	53	…	100	101
Цвет	FF FF FF	FF FF FF	FF FF FF	…	FF FF FF	FF FF FF

Черный цвет в данном случае будет иметь нулевой уровень, что для одного байта соответствует ноль в десятичной системе счисления, в двоичной 00000000 и в шестнадцатеричной 00, а для белого цвета уровень 255, что соответствует в десятичной 255, в двоичной 11111111 и в шестнадцатеричной FF. Для скрытия информации берется первая точка изображения, анализируется её принадлежность к определенной цветовой группе, например, к группе белого цвета, затем этой точке из файла-сообщения присваивается код текущего символа с учетом выбранной цветовой группы. Например, для символа Б в белой точке будет предназначен цвет с кодом 52, а для белой точки цвет с кодом 1.

Рассмотрим на примере скрытие какого-либо мультимедиа файла внутри BMP-изображений с помощью рассмотренного метода (рис. 1) [3].

В BMP-файлах каждая точка (пиксель) кодируется с помощью 24 бит, по 8 бит на каждый из каналов (синий, красный, зеленый). Следовательно, компьютер различает огромное количество различных цветов, что невозможно для человеческого глаза. Это и позволяет незаметно манипулировать цветом любого изображения.

Если мы заменим младшие биты цвета каждого пикселя на те, что нам нужны либо вставим туда сигнал нашего аудиофайла, то изображение при этом практически не изменится. В конце такой процедуры мы и получим зашифрованный звук в изображении. Проблема может возникнуть лишь в размере. Если мы будем шифровать короткий звуковой файл, то качество изображение и его размер практически не изменится. При шифровке более большого файла могут уже пойти искажения в изображении.

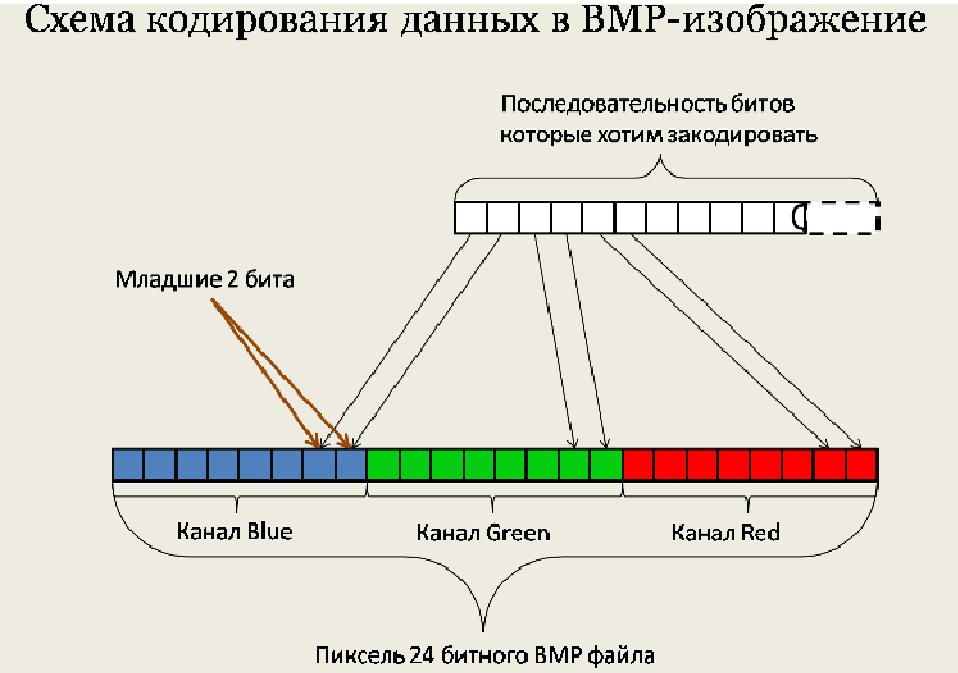


Рис 1. Схема кодирования данных

Пример оригинального изображения приведен на рис. 2 [4]. Пример зашифрованного звука в изображении приведён на рис. 3 [4].

Рис. 2. Оригинальное изображение

Рис. 3. Изображение с зашифрованным сообщением

В рамках данной задачи проводятся анализ и исследования различных алгоритмов шифрования звуковой информации в графических файлах, оптимизация размещения звуковой информации.

Список используемых источников

1. Алексеев А. П., Аленин А. А. Скрытая передача данных в звуковых файлах формата WAV// Инфокоммуникационные технологии. 2010. Т. 8. № 3. С. 101–106.

2. Аленин А. А., Алексеев А. П. Исследование методов обнаружения вложений в звуковых файлах формата WAV // Безопасность информационных технологий. 2011. Т. 9. № 1. С. 51–56.

3. Алефиренко В. М. Основы защиты информации: Практикум для студ. спец. «Техническое обеспечение безопасности» и «Моделирование и компьютерное проектирование радиоэлектронных средств». Мн. : БГУИР, 2004. 44 с.

4. https://www.bestfree.ru/soft/graph/coding.php

УДК 004.93

ПРИМЕНЕНИЕ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ В НЕЙРОННОЙ СЕТИ ДЛЯ РАСПОЗНАВАНИЯ ЖЕСТОВОГО ЯЗЫКА

В. И. Воронов, Л. И. Воронова, К. В. Генчель

Московский технический университет связи и информатики

В статье описываются особенности общения слабослышащих людей посредством жестового языка, разработка сверточной нейронной сети для распознавания дактилем, этапы создания обучающего набора для нейросети, а также целесообразность применения параллельных алгоритмов для оптимизации её обучения и работы.

ИАД, нейронные сети, жестовый язык, машинное обучение, параллельные вычисления.

Жестовый язык – самостоятельный язык, состоящий из комбинации жестов, каждый из которых производится руками в сочетании с мимикой, формой или движением рта и губ, а также в сочетании с положением корпуса тела. Использование этого языка является основным способом коммуникации людей с нарушением слуха и играет важную роль в их жизни, поскольку даёт возможность участия в жизни общества.

В жестовом языке имеется возможность воспроизведения слов с помощью дактильного алфавита, символы которого можно разделить на статические и динамические (рис. 1).

Рис. 1. Статические и динамические жесты русского дактильного алфавита

В сфере распознавания весьма активно развивается направление Kinect-устройств [1]. Бесконтактный сенсорный Kinect-контроллер, состоит из двух сенсоров глубины, цветной видеокамеры и микрофонной решетки. Существуют «обученные» камеры, частично распознающие жестовые языки (на данный момент только английский и китайского). В современных программных подходах основным методом распознавания образов является нейронная сеть.

Принцип работы нейронной сети основан на упрощенной модели работы биологического нейрона. Нейрон – это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше. В результате на основе векторов X и параметров на выходе получаем функцию гипотезы, которая показывает вероятность принадлежности изображения к одному из классов [2]. Здесь под классом понимается дактильный символ. Сеть – это совокупность слоев, содержащих нейроны (рис. 2).

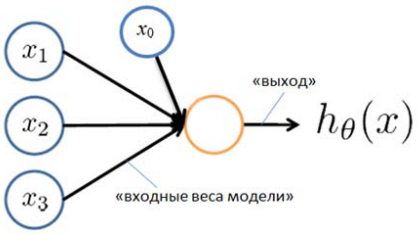


Рис. 2. Модель нейронной сети

Вычисления в каждом нейроне производятся по формулам (1) и (2). В них g – сигмоидная функция. Задачей вычислений нейросети является подобрать Θ, чтобы функция (3) стремилась к минимуму.

$$\begin{aligned} a_1^{(2)} &= g\left(\theta_{10}^{(1)}x_0 + \theta_{11}^{(1)}x_1 + .. + \theta_{1\,7361}^{(1)}x_{7361}\right), \\ &\dots \\ a_{486}^{(2)} &= g\left(\theta_{486\,0}^{(1)}x_0 + \theta_{486\,1}^{(1)}x_1 + .. + \theta_{486\,7361}^{(1)}x_{7361}\right), \end{aligned} \tag{1}$$

$$\begin{aligned} a_1^{(3)} &= g\left(\theta_{10}^{(2)}a_0 + \theta_{11}^{(2)}a_1 + .. + \theta_{1\,486}^{(2)}a_{486}\right) \\ &\dots \\ a_{32}^{(3)} &= g\left(\theta_{32\,0}^{(2)}a_0 + \theta_{32\,1}^{(2)}a_1 + .. + \theta_{32\,486}^{(2)}a_{486}\right) \end{aligned} \tag{2}$$

$$J(\theta) = -\frac{1}{m}\left[\sum_{i=1}^{m}\sum_{k=1}^{K} y_k^{(i)} \log\left(h_\theta\left(x^{(i)}\right)\right)_k + \left(1 - y_k^{(i)}\right)\log\left(1 - \left(h_\theta\left(x^{(i)}\right)\right)_k\right)\right] + \frac{\lambda}{2m}\sum_{l=1}^{L-1}\sum_{i=1}^{s_l}\sum_{j=1}^{s_l+1}\left(\theta_{ji}^{(l)}\right)^2. \tag{3}$$

На кафедре ИСУиА МТУСИ в рамках магистерских диссертаций [3, 4] разрабатывается проект по распознаванию жестового языка, первый этап которого – распознавание статических изображений [5]. Авторами создан обучающий набор данных. Для этого проведено порядка 100 видеозаписей каждого жеста с последующей сегментацией по 50–100 кадров. Полученные изображения сохранены в директории, порядковые номера которых – цифра, сопоставляемая дактилеме (рис. 3).

Рис. 3. Наборы данных для обучения нейронной сети

Изображения приведены к размеру 80 на 92 пикселя. На рис. 4 представлена полносвязная нейронная сеть из трех слоев, на вход которой подается 7360 значений (по количеству пикселей в одном изображении).

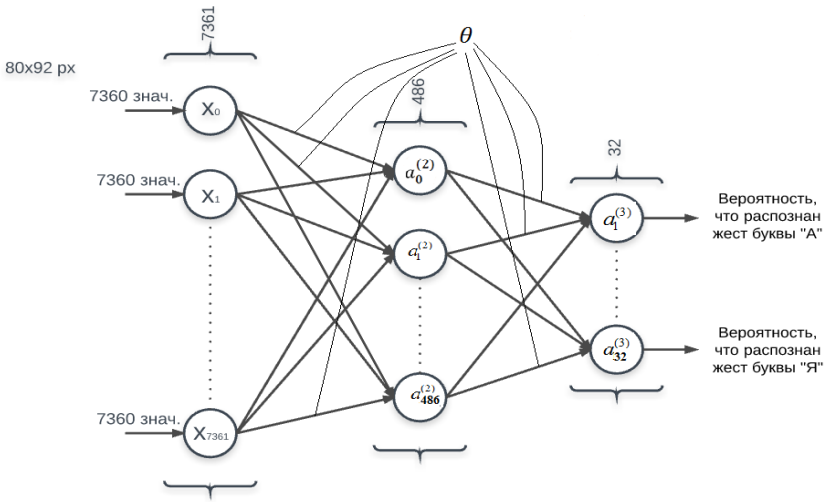


Рис. 4. Полносвязная нейронная сеть

К задаче вычисления этой сети можно применить декомпозицию. Тогда вычисления могут выглядеть следующим образом (рис. 5):

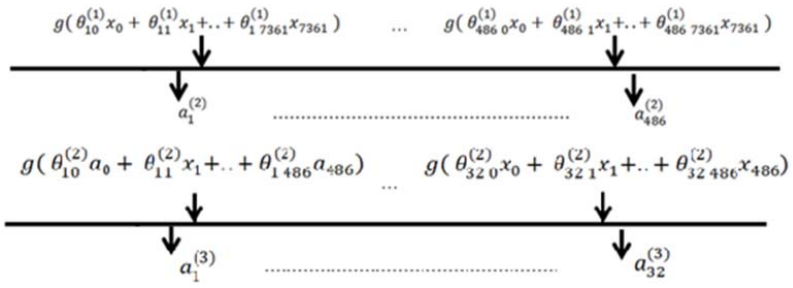


Рис. 5. Декомпозиция вычислений нейросети

При использовании полносвязной нейронной сети, даже при распараллеливании становится слишком много вычислений и потоков (в первом случае 32, а во втором – 486). В такой сети каждый нейрон связан со всеми последующими, и каждая связь имеет свой весовой коэффициент. Для уменьшения размерности и количества вычислений возможно использование свёрточной нейронной сети (рис. 6).

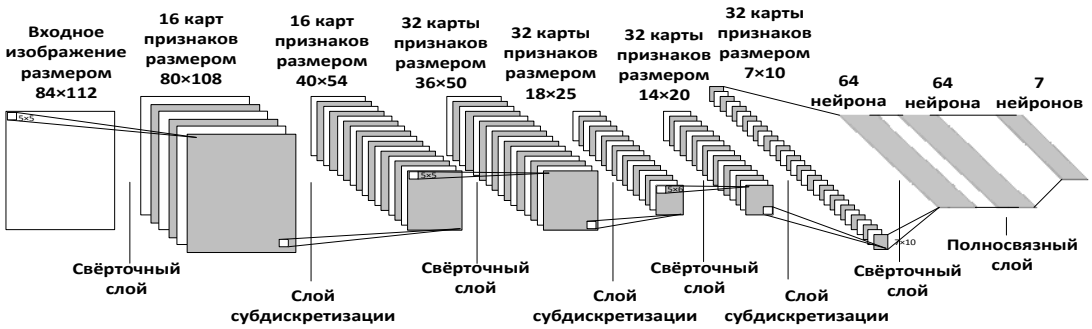


Рис. 6. Сверточная нейронная сеть

В свёрточной нейронной сети в операции свёртки используется матрица весов небольшого размера – фильтр/ядро свертки, которую «передвигают» по сверточному слою, формируя после каждого сдвига сигнал активации для нейрона следующего слоя на основе скалярного произведения интенсивностей пикселей рецептивного поля свертки и параметров фильтра. Операции свертки можно считать параллельно в своих потоках (рис. 7).

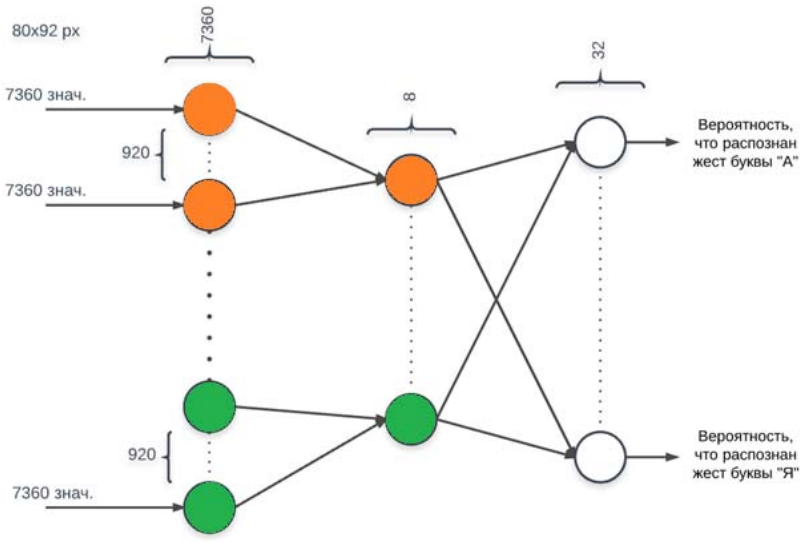


Рис. 7. Распараллеливание вычислений в нейронной сети, распознающей дактилемы жестового языка

В результате распараллеливания вычислений сеть будет обучаться быстрее, а значит, будет более эффективной.

Распараллеливание осуществлено на языке программирования Java с использованием средств MPI. Программный код, реализующий процесс распараллеливания вычислений нейронной сети изображен на рис. 8.

```
import mpi.*;
public class Network {
   private static double sigmoid(double x)
{
    return 1 / (1 + Math.exp(-x));
}
        public static void main(String args[]) throws Exception {
        MPI.Init(args);
        int rank = MPI.COMM_WORLD.Rank();

        if (rank == 0){
      int[] A = new A[486];
          for(int i=0; i<486; i++)
        {
  A[i]= (int) Math.round((Math.random() * 256));
        }
     MPI.COMM_WORLD.Send(A, i, 486, MPI.INT, i+1, 0);
                }
                else{
          double [] param = new double [32];
          double [] F = new double [486];
             for(int i=0; i<486; i++)
          {
         F[i]= (double) Math.round((Math.random()));
           }
       int [] A = new int [486]
       MPI.COMM_WORLD.Recv(A, rank, 486, MPI.INT, 0, 0);
             for (int i = 0; i < 32; i++)
             for (int j = 0; j < 486; j++) {
               param [i] =  sigmoid(F[j]*A[j]); }
            for (int i = 0; i < 32; i++)
       {
 if (A[rank] == i) MPI.COMM_WORLD.Send(param, rank-1, 32, MPI.DOUBLE, 0, 0);
                        }
                    }
if (rank == 0){
        String[]russian={"а","б","в","г","д","е","ж","з","и","й","к","л","м","н","о","п",
"р","с","т","у","ф","х","ц","ч","ш","щ","ы","ь","э","ю","я"};
         double [] param = new double[32];
         MPI.COMM_WORLD.Recv(param, i, 32, MPI.DOUBLE, 0);
              double max = param[0];
        for (int i = 1; i < param.length; i++) {
           if (param[i] > max) max = param[i];
           int k= i;
         }
       for (int i = 1; i < 32; i++)
    {if k = i
 (System.out.print (“Распознана буква - ” + russian [i]));}
                  }
          MPI.Finalize();
        }
}
```

Рис. 8. Программный код, реализующий распараллеливание в нейросети

MPI [6] – интерфейс передачи сообщений между процессами, выполняющими одну задачу. Под параллельной программой в рамках MPI понимается множество одновременно выполняемых процессов. Все процессы порождаются один раз, образуя параллельную часть программы. Базовым механизмом связи между MPI процессами является передача и приём сообщений. Сообщение несёт в себе передаваемые данные и информацию,

позволяющую принимающей стороне осуществлять их выборочный приём [7]:

– отправитель – ранг (номер в группе) отправителя сообщения;

– получатель – ранг получателя;

– признак – может использоваться для разделения различных видов сообщений;

– коммуникатор – код группы процессов.

Выводы: в статье описана разработанная сверточная нейронная сеть для распознавания дактилем, использующая параллельные вычисления. Следующим этапом разработки является проектирование нейросети для распознавания динамических жестов. Также планируется использование методов распределения для высокопроизводительных вычислений в рамках расширения проекта [8].

Список используемых источников

1. Михаеску С. В., Трунов А. С., Воронова Л. И. Анализ предметной области для разработки системы построения скелетной модели человека на основе массива опорных точек, получаемых совокупностью контроллеров Kinect // Международный студенческий научный вестник. 2015. № 3–4. С. 521–522.

2. Воронова Л. И., Воронов В. И. Machine Learning: регрессионные методы интеллектуального анализа данных: учебное пособие; МТУСИ. М., 2017. 81с.

3. Воронов В. И., Воронова Л. И. О повышении результативности магистерских программах в условиях инновационной экономики // Инновационные подходы в науке и образовании: теория, методология, практика : монография. Пенза : Наука и Просвещение, 2017. С. 35–44.

4. Voronov V. I., Voronova L. I. Features of realization master’s program "automation of technological processes and manufactures" // International Journal of Applied and Fundamental Research. 2016. № 2. URL: www.science-sd.com/464-25196

5. Genchel K. V., Voronov V. I., Voronova L. I. The sign language recognition project for disabled people with hearing violation about // International journal of applied and fundamental research. 2017. № 3.

6. Воронова Л. И., Трунов А. С. Оптимизация параллельного алгоритма подсистемы распределенного молекулярно-динамического моделирования // Межотраслевая информационная служба. 2011. № 3. С. 3–11.

7. Жалнин Р. В., Панюшкина Е. Н., Пескова Е. Е., Шаманаев П. А. Основы параллельного программирования с использованием технологий MPI и OpenMP: учебное пособие. Саранск: Изд-во СВМО, 2013. 78 с.

8. Трунов А. С., Воронова Л. И., Воронов В. И. Разработка методов распределения для высокопроизводительных вычислений в многочастичных системах // Международный журнал прикладных и фундаментальных исследований. 2013. № 10–2. С. 192–194.

УДК 004.94

КОМПОНЕНТЫ СПЕЦИАЛЬНОЙ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ПОСТРОЕНИЯ ОПТИМАЛЬНЫХ МАРШРУТОВ

А. В. Вострых, Д. Г. Шуракова

Главное управление МЧС России по Новгородской области
Санкт-Петербургский университет ГПС МЧС России

Рассматривается задача построения оптимальных маршрутов следования аварийно-спасательных формирований пожарно-спасательного гарнизона на примере города Кострома. В качестве инструментария для ее решения предлагается специальная информационная технология. Технология содержит 3 стратифицированные компоненты, каждая из которых включается в работу при невозможности решения задачи на предыдущем уровне (ступени), что обеспечивает гарантированную возможность решения задачи в реальном масштабе времени и в различной обстановке.

аварийно-спасательные формирования, маршруты следования, специальная информационная технология, имитационное моделирование, алгоритм Дейкстры, кластеризация.

В среднем за год на территории нашей страны происходит около 220 тыс. пожаров, 70 % которых приходится на непроизводственную сферу. Ежегодно во время пожаров погибает порядка 14 тыс. человек [1]. Величина потерь от пожаров превышает общий ущерб государства от чрезвычайных ситуаций (ЧС) техногенного характера и является безвозвратной: урон от пожаров не только невосполним, но и требует еще больших затрат для восстановления уничтоженных материальных ценностей.

С целью ликвидации и предотвращения пожаров, аварий и ЧС созданы аварийно-спасательные подразделения МЧС России, основной функцией которых является сохранение человеческих жизней и минимизация материального ущерба [2]. Вследствие, стремительного роста городов, увеличения количества автотранспорта и возросшей в разы нагрузки на автомобильные дороги всё чаще возникает вопрос о своевременной доставки сил и средств (СиС) подразделений МЧС России к месту происшествия, так как скорость реагирования на происшествия и время следования СиС к месту ликвидации ЧС играет ключевую роль в выполнении нормативов прибытия и сведения, тем самым, материального ущерба к миниму-

му (максимальное допустимое нормативное время прибытия согласно ФЗ-123 [3] – 10 минут).

На сегодняшний день решение задачи определения оптимального маршрута следования СиС подразделений МЧС к месту происшествия России возложено на командиров соответствующих расчетов. Задача ими решается, исходя из имеющихся технических возможностей и навыков по использованию геоинформационных технологий, знания городской обстановки личного опыта, т. е. в принципе достаточно индивидуально и уникально для каждого конкретного подразделения. И здесь необходимо иметь в виду ряд факторов, которые не позволяют гарантировать устойчивое и оптимальное решение этой важнейшей задачи.

Во-первых, это значительное влияние на решение человеческого фактора. Во-вторых, специфика используемых средств геоинформационных технологий, которые могут выйти из строя, или быть временно недоступны, или не покрывают район выезда (нет актуальных электронных карт). Не говоря уже о том, что в их работу могут вмешаться злоумышленники. Все это приводит к неустойчивости существующей и требует разработки специальной информационной технологии построения оптимальных маршрутов следования сил и средств МЧС России к месту происшествия. К традиционным технологическим требованиям (результативности, детерминированности и массовости) добавим требование устойчивости, под которым будет пониматься гарантированная возможность решения задачи в реальном масштабе времени в различной обстановке и в различных ситуациях, что является объективным фоном деятельности спасателей и пожарных. Это требование предполагается реализовать за счет многоуровневого использования известных информационных технологий.

Критерием оптимальности выбранного маршрута следования будем считать время на доставку СиС, а не протяженность этого пути. Задачу оптимизации решим для маршрутов следования аварийно-спасательных формирований конкретного пожарно-спасательного гарнизона среднестатистического, но конкретного города – Костромы. Анализ официальных статистических данных показывает, что, несмотря на наметившийся общий благоприятный вектор развития пожарной обстановки в городе Кострома (снижение количества пожаров и числа погибших), отмечается стабильный рост показателя пожарного риска для человека погибнуть при пожаре, который в ближайшее десятилетие, с учетом роста населения города, останется как минимум на прежнем уровне [1]. Поэтому решение поставленной задачи является крайне актуальным.

Разработанная для решения задачи специальная информационная технология содержит 3 стратифицированные компоненты, каждая из которых будет включаться в работу при невозможности решения задачи на предыдущем уровне (ступени). Этими компонентами являются:

1-й уровень – использование универсального картографического сервиса Яндекс.Карты для построения кратчайшего маршрута (дополнительно с имитационной моделью для уточнения районов выезда – только на этапе планирования);

2-й уровень – использование специального программного продукта для нахождения оптимального маршрута (дополнительно с алгоритмами кластеризации для уточнения районов выезда – только на этапе планирования);

3-й уровень – использование графической модели в виде схем-карты оптимальных маршрутов следования, индивидуальной для каждого подразделения МЧС.

Принцип применения специальной информационной технологии следующий: имитационная модель, разработанная коллективом под руководством проф. Буйневича М. В. [4] на основе инструмента Яндекс.Карты, устанавливается на электронно-вычислительное устройство вида планшет, смартфон или ноутбук и работает в режиме реального времени, составляя маршрут на основе данных Яндекс-сервиса «Навигатор» и введённых ранее в программу оператором.

Программный интерфейс модели позволяет включать/отключать демонстрацию зон прикрытия, что помогает визуально оценить зоны ответственности различных подразделений МЧС на этапе планирования. Зоны прикрытия отображаются в виде зелёных многоугольников с синей границей (рис. 1).

Указанная имитационная модель может также использоваться для решения задачи расчета численности и размещения пожарно-спасательных подразделений в городе Кострома. Принцип работы модели в этом случае заключается в разбиении города на множество квадратов со стороной примерно в 1 км; затем рассчитывается кратчайший маршрут от места дислокации пожарного подразделения до центра каждого квадрата (как очага пожара), и производится окрашивание квадрата в цвет согласно следующим правилам: время в пути менее 5 минут – зелёный; время в пути менее 10 минут – жёлтый; время в пути менее 18 минут – красный; иначе используется чёрный цвет. Из результатов моделирования видно (рис. 2), что в целом территория города прикрыта, за исключением «Заволжского округа», где около половины территории находится за пределами нормативного времени прибытия пожарных расчётов.

Минусом данного подхода является то, что для устойчивого функционирования 1-го уровня необходимо подключение к сети интернет и наличие исправной компьютерной техники и безотказного программного обеспечения.

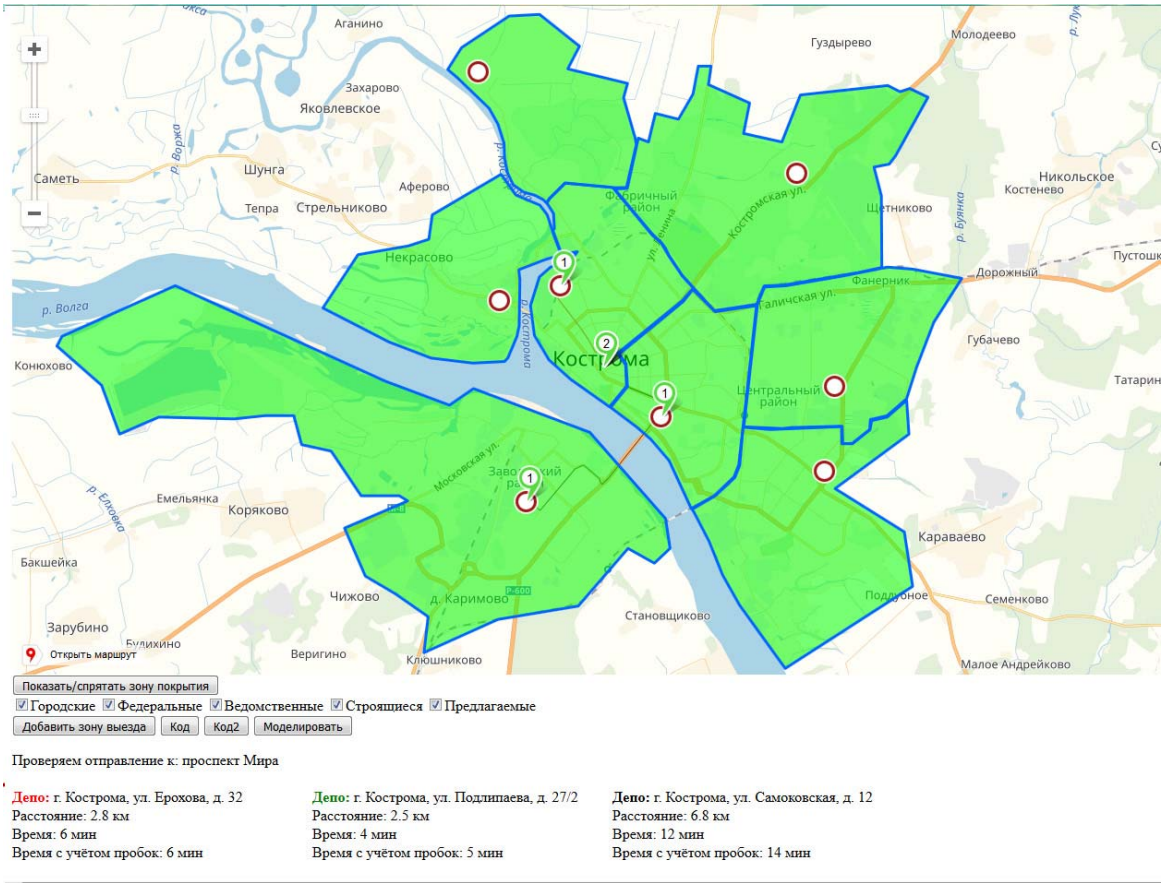


Рис. 1. Режим имитационной модели «Зоны прикрытия (выезда)»

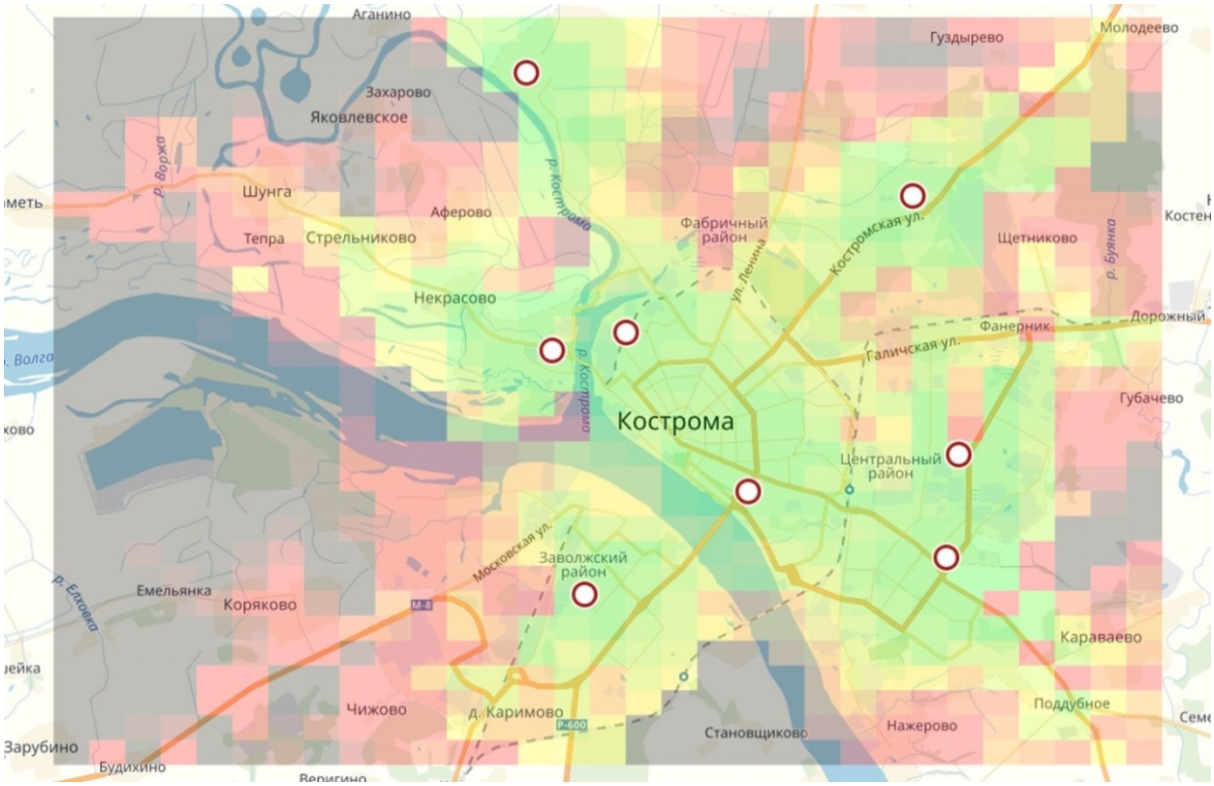


Рис. 2. Результат работы имитационной модели

В случае если интернет-соединение отсутствует в работу подключается 2-й уровень данной технологии – это off-linemодель на основе программного продукта, строящая кратчайший маршрут по электронным картам, основываясь на алгоритме Дейкстры [5].

Предварительно, на этапе планирования, целесообразно актуализировать районы выезда путем двухуровневой кластеризации субоптимальных зон прикрытия города Кострома подразделениями МЧС России при возникновении происшествий, для чего следует:

– на электронной карте были инициализировать точечные социально значимые и потенциально опасные объекты, а также подразделения МЧС;

– затем, используя алгоритм FOREL [6] произвести первоначальное разграничение зон с учётом проблем на дорогах, и получить точки-центроиды.

– и, наконец, для улучшения результата вычислений (сокращения количества зон выезда до количества подразделений МЧС) к множеству точек-центроидов применить метод кластеризации, например «Кратчайшего незамкнутого пути».

Если же у следующего к месту вызова подразделения по каким-либо причинам отсутствует компьютерная техника (или она неисправна или сбоит), в решение задачи построения маршрута вступает 3-й уровень вида схем-карты, обладающий наглядным отображением оптимальных путей следования и информацией об имеющихся маршрутах и известных уязвимых местах (таких как проблемные участки дорог с постоянными пробками) на основе статистических данных (см. рис. 3 ниже).

Гипотетически такая информационная технология будет обладать необходимой устойчивостью в условиях экстремальных ситуаций, при этом, будучи результативной, детерминированной (алгоритмичной) и обладая свойством массовости (за счет многократного использования, универсальности и возможности тиражирования). Прогнозируется, что разработка подобной технологии, как минимум обеспечит гарантированное решение задачи, а как максимум – сокращение времени прибытия подразделений на вызов и как следствие спасение большего количества человеческих жизней.

Список используемых источников

1. Официальный сайт МЧС России. Раздел: Чрезвычайные ситуации – Статистика чрезвычайных ситуаций за 2003–2018 гг. Подраздел «Пожары» [Электронный ресурс]. URL: http://www.mchs.gov.ru/activities/stats/Pozhari.

2. Федеральный закон от 22.07.2008 № 123-ФЗ «Технический регламент о требованиях пожарной безопасности».

3. Федеральный закон от 22.08.1995 № 151-ФЗ «Об аварийно-спасательных службах и статусе спасателя».

4. Буйневич М.В., Максимов А.В., Пелех М.Т. Принципы информационной поддержки системного проектирования развития сети пожарных депо на территории мегаполиса // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2017. № 3. С. 129–135.

5. Левитин А. В. Алгоритмы. Введение в разработку и анализ. М. : Вильямс, 2006. 576 с.

6. Загоруйко Н. Г. Прикладные методы анализа данных и знаний. Новосибирск : ИМ СО РАН, 1999. 270 с.

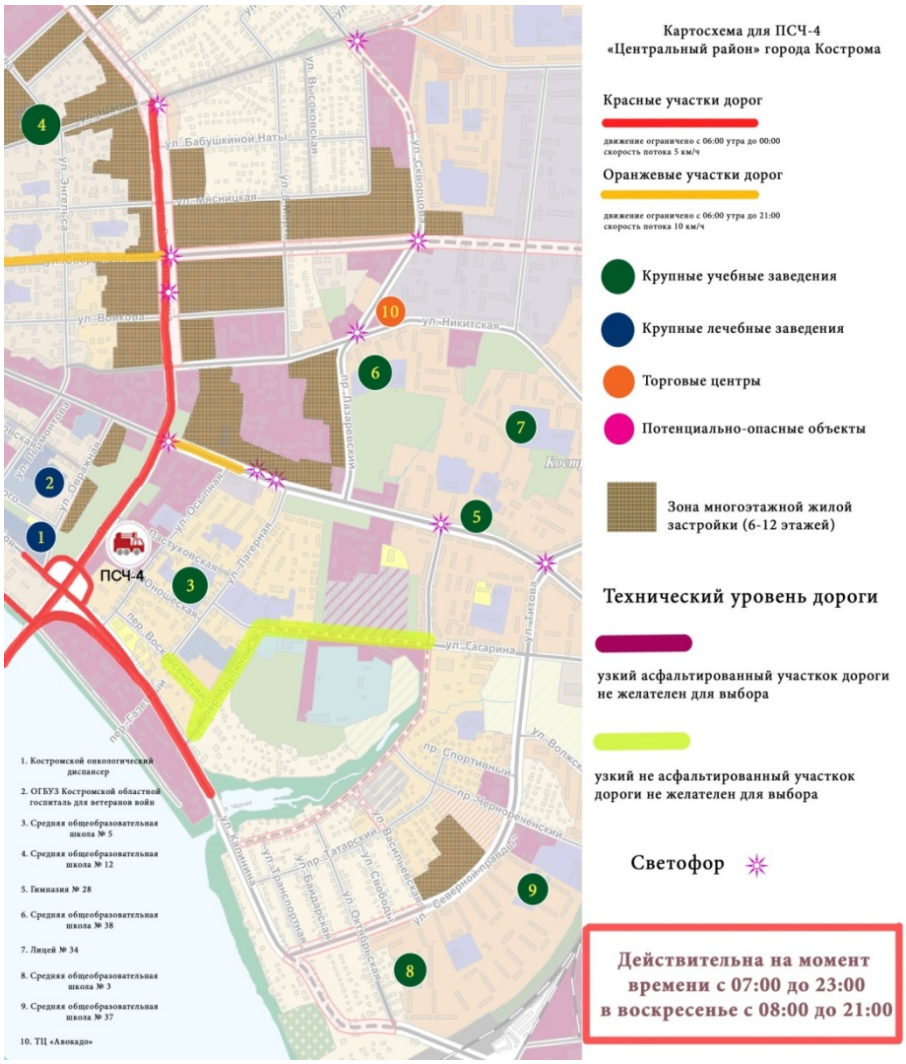


Рис. 3. Схем-карта для пожарно-спасательной части № 4 (ПСЧ-4)

Статья представлена профессором кафедры БИС СПбГУТ, доктором технических наук, профессором М. В. Буйневичем.

УДК 4.056

МЕЖРЕГИОНАЛЬНОЕ ВЗАИМОДЕЙСТВИЕ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. С. Гаврилов, М. Д. Глуховский, А. Д. Кузнецова, А. И. Пешков

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

В наши дни повышение уровня информационной безопасности является одним из важнейших аспектов национальной безопасности. В данной работе авторы рассматривают этапы импортозамещения иностранного ПО на российский аналог, а также некоторые другие решения, которые позволят обеспечить информационную безопасность исполнительных органов государственной власти. Информационные и коммуникационные технологии уже стали неотъемлемой частью современных управленческих систем во всех сферах государственного управления и безопасности государства.

импортозамещение, информационная безопасность, угрозы, уязвимости, распределенные сети, межрегиональное взаимодействие, информационные системы.

В современном мире информационная безопасность является одним из основополагающих факторов безопасности государств, отдельных ведомств, компаний и людей в частности. В правовом нормативном акте, впервые кибербезопасность была озвучена 23 ноября 2001 г. в международном документе «Конвенция по киберпреступлениям». Государства обозначили высокую значимость виртуального пространства, и приняли совместные базовые решения, обозначили правовые ограничения кибербезопасности, которые позволили бы предотвратить возможные киберпреступления [1].

В 2010 г. генеральный секретарь Интерпола Рональд Ноубл высказался на конференции в Гонконге, где выступали 300 председателей правоохранительных структур из 56 стран. Он заявил, что киберприступность главная угроза обществу, и при обсуждении масштабов проблемы его слова подтвердились. На тот момент было зафиксировано, что около 75 % процентов пользователей когда-либо подвергались кибератакам. При этом ущерб, нанесенный в денежном эквиваленте компаниям и отдельным лицам, шел уже на миллиарды долларов. Последний конгресс ООН, который прошел в 2015 г. в г. Дохе закрепил положение киберприступности, как основной угрозы обществу и человечеству в целом на ровне с терро-

ризмом так, как почти все люди на планете были подвержены к этому времени кибератакам, наносимый ущерб растет невероятно быстро [2, 3].

В России также, как и в многих других странах мира были предприняты меры по улучшению ситуации в области безопасности. 31 декабря 2015 г. был принят указ президента Российской Федерации, Владимира Владимировича Путина, о стратегии национальной безопасности Российской Федерации. В нем обозначены множественные угрозы национальной безопасности и цели, которые необходимо выполнить, чтобы соблюсти все меры защиты. В частности, были выделены угрозы и цели, относящиеся к информационной безопасности.

Важно понимать на каких уровнях и как могут быть организованы кибератаки, где может быть утечка информации, как этому противостоять, какие меры нужно предпринять, чтобы обезопасить информационной пространство. Все это можно представить, рассмотрев базовую иерархическая модель сети. В современных реалиях она строится на 3 уровнях: уровне доступа, уровне агрегации и уровне ядра (рис. 1).

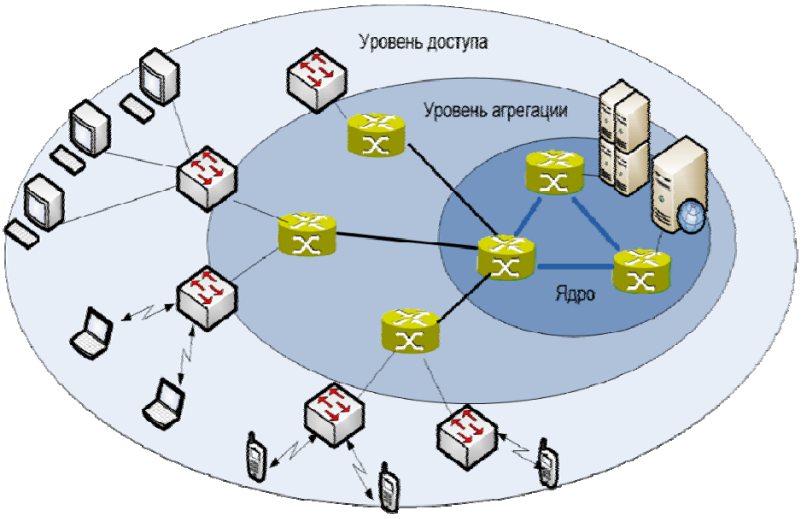


Рис. 1. Базовая иерархическая модель сети

Уровень доступа нужен для подключения станций и серверов к какой-либо сети. Уровень доступа представлен в сети L2-коммутаторами (коммутаторами второго уровня), в редких случаях используют L3-коммутаторы (коммутаторы третьего уровня). Сейчас в России органы государственной власти используют в своих сетях в основном L2-коммутаторы. Одним из шагов, который позволит защитить сети станет переход на L3-коммутаторы, это связано в первую очередь с тем, что на них легче осуществить защиту, и она будет состоять из нескольких уровней. Также стоит отметить, что переход на 3 уровень позволит использовать VPN соединения между филиалами отдельных органов, которое осуществлялось путем почты или выхода в глобальную есть, а это в свою очередь наруша-

ет информационную безопасность и является менее удобным в использовании.

Как правило для организации этого самого простого уровня иерархической модели устанавливаются наиболее оптимальные по цене устройства, не требующие сложной конфигурации. Это пользовалось спросом, пренебрегая защитой информации экономили на оборудовании, так как это было не нужно, сейчас этого нельзя допустить. Так же огромным минусом на этом уровне можно выделить использование иностранного ПО на конечных устройствах, что значительно увеличивает шансы взлома и утечки информации. В данный момент повсеместно это проблема решается путем замены иностранного ПО на российский аналог на базе ПО Linux, что существенно повысит безопасность [4].

Уровень распределения – этот уровень является самым «умным» в иерархической модели. На уровне распределения решаются задачи агрегации широковещательных доменов и доменов маршрутизации, фильтрации и настройки Qos, агрегации больших проводных сетей, обеспечение высокого уровня доступности ядра для конечных пользователей. Маршрутизаторы, использующиеся на уровне распределения также могут брать на себя функции обеспечения доступа в Интернет.

Ядро – это комплекс сетевых устройств (маршрутизаторов и коммутаторов), обеспечивающих резервирование каналов и высокоскоростную передачу данных между различными сегментами уровня распределения. На этом уровне важнейшим приоритетом является выход не в Интернет для взаимодействия органов власти, а в собственную защищенную сеть закрытого доступа для увеличения скорости и надежности выполняемой работы, а также безопасности, что является самым важным на данный момент [5].

Начало формированию новой системы взаимодействия государственных органов положил проект Ханты-Мансийского автономного округа еще на 2005–2007 гг. было создано постановление правительства округа и принято решение совместно с ФСО на базе округа создать сеть, которая станет прототипом в дальнейшем создания сети государственных органов России. Она имела свои определенные особенности и должна была стать в дальнейшем частью сети государственных органов обозначив главные проблемы и способы их решения. В последствии после довольно продолжительного тестирования таких сетей, потом уже на базе не одного субъекта, была создана концепция и метод постепенного внедрения сети RSNet и опубликован приказ ФСО (рис. 2) [6].

В дальнейшем все ведомства и государственные органы будут подключены к этой сети. В ней были учтены все аппаратные недостатки ранее описанные, создана защищенная архитектура сети и использованы все возможные методы защиты. Конечно это не гарантирует 100 % защиту,

но сильно уменьшит возможность угроз как снаружи, так и изнутри, ведь эта сеть изолирована от глобальной.

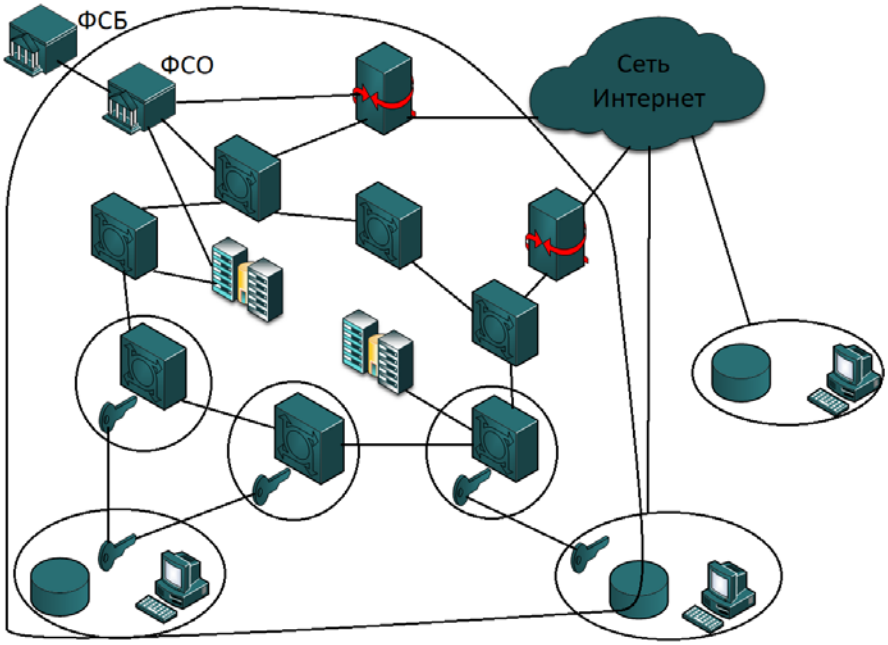


Рис. 2. Предположительная схема сети RSNet

Выводы

Таким образом, была создана и внедрена сеть, имеющая высокую степень защищенности информации. Она позволит взаимодействовать, как различным органам государственной власти для обеспечения более качественной быстрой и надежной работы между ними, так и между отдельными филиалами определенных государственных органов. При этом вся информация, которая является важной будет защищена и вовремя, а главное быстро обработана. Также на схеме можно видеть, что определенные органы смогут по-прежнему использовать глобальную сеть, при этом все данные из вне будут обрабатываться и проверяться ФСО совместно с ФСБ для обеспечения контроля и избежание утечек изнутри. Все эти меры позволят создать централизованную, высокоэффективную, безопасную систему передачи, обработки и хранения данных в органах государственной власти и не только.

Список используемых источников

1. Колганова Е. А., Давтян Д. В. Характеристика киберпреступлений и способы их предотвращения// Аллея науки. 2017. Т. 4, N 9. С. 755–760.

2. Иванов Д. В. Конгрессы ООН по предупреждению преступности и обращению с правонарушителями: глава в книге Европейское Международное Право. М., 2005. С. 485–489.

3. Пысина Л. М., Пыринов А. А., Бердюгин В. Ю. Фундаментальные проблемы защиты информационных объектов от кибератак // 68-я научная конференция «Наука ЮУРГУ», Челябинск, 2016. С. 618–622.

4. Андрианов В. И., Виткова Л. А., Сахаров Д. В. Исследование алгоритма защиты общедоступных персональных данных в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 т. 2015. С. 377–379.

5. Душин С. Е., Красов А. В., Кузьмин Н. Н. Моделирование систем управления : учебное пособие для студентов высших учебных заведений, обучающихся по направлению 220400 «Управление в технических системах» / Под ред. С. Е. Душина. М., 2012.

6. Фомин Д. А. Разработка методов повышения защищенности сегмента информационно-телекоммуникационной сети «интернет» для федеральных органов государственной власти и органов государственной власти субъектов федерации // Студенческая наука для развития информационного общества, Ставрополь, 2017 г. С. 480–483.

УДК 004.624

ОБЗОР ФОРМАТОВ ПРЕДСТАВЛЕНИЯ СЕТЕВОГО ТРАФИКА ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ КИБЕР-ФИЗИЧЕСКИХ СИСТЕМ

Д. А. Гайфулина[1,2], А. В. Федорченко[1,2]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Работа посвящена анализу форматов представления сетевого трафика в кибер-физических системах. Целью исследований является выявление достоинств и недостатков существующих способов представления информации о сетевой активности для задач сбора, передачи, хранения и последующей обработки. В результате работы проанализированы полуструктурированные и структурированные форматы, наиболее часто применяемые на практике. Приводится сравнение форматов по аспектам сложности, удобства восприятия, ресурсопотребления и др. Также рассматривается возможность нормализации исходной информации для обеспечения совместимости и корректной интерпретации данных сетевого трафика.

форматы сетевого трафика, анализ сетевого трафика, оценка защищенности.

В современном мире кибер-физические системы (КФС) являются все более востребованными из-за возможности интеграции информационных технологий и устройств взаимодействия с физическими процессами и объ-

ектами. Подобные системы подразумевают наличие вычислительной среды, программно-аппаратной инфраструктуры (платформы), а также среды передачи информации и межмодульного взаимодействия [1].

Для обеспечения безопасности КФС используются различные методы обнаружения (предупреждения) атак и оценки защищенности. Одним из подобных методов является анализ сетевой активности с целью обнаружения аномалий в данных сетевого трафика. В данном случае под аномалиями понимаются ситуации, в которых поведение инфраструктуры или ее отдельных элементов отличается от нормального (эталонного) поведения. Аномалии в КФС могут проявляться в виде отключения, отказа, некорректной работы ее элементов, перегрузки сетевого оборудования и сервисов, а также изменения сетевой активности [2].

Одной из особенностей КФС является неопределенность архитектуры, внутреннего функционирования модулей, среды передачи данных, в том числе протоколов сетевого обмена. По этой причине часть сетевого трафика (СТ) для проведения анализа сетевой активности инфраструктуры может быть синтаксически и семантически не определена. Анализ подобных снимков сетевого обмена является достаточно сложной вычислительной задачей, практически не реализованной в настоящее время.

Для обеспечения совместимости и корректной интерпретации данных СТ на этапах его сбора, передачи, хранения и последующей обработки в КФС могут использоваться определенные форматы представления информации. Данные форматы могут быть оценены с помощью различных характеристик, определяющих удобство использования конкретного формата как для машинной обработки и передачи данных, так и для восприятия человеком.

Работа посвящена анализу ряда форматов представления данных СТ. Цель проводимого исследования заключается в определении наиболее подходящего формата описания сетевой активности для оценки защищенности КФС. Задачами исследования являются: (1) определение характеристик форматов СТ и их значений; (2) рассмотрение особенностей форматов СТ; (3) сравнение форматов СТ и выявление наиболее подходящего из них.

В общих схемах анализа СТ первым шагом является захват пакетов, целью которого является получение объекта анализа с использованием различных подходов.

«Слайсинг» (*slicing*) – подход, при котором анализу подвергается не все содержимое сетевого пакета, а только заданный префикс из определенного количества данных, считая от начала пакета. В ряде исследований показано, что этот подход успешно использован для классификации пакетов трафика по протоколам [3]. «Сэмплинг» (*sampling*) – подход, при котором перехватывается часть пакетов, выбираемая по заданным условиям и стра-

тегиям отбора. Задача получения информации о полном состоянии сети по результатам «сэмплинга» известна как проблема инверсии (*inversion problem*) [4]. Для задач же, в которых необходим максимально точный анализ трафика, требуется перехватывать все данные без потерь с использованием подхода глубокого захвата пакетов (*deep packet capture,* DCP). Также может производиться агрегирование сетевых пакетов в потоки по адресным признакам (*flow generation*) для получения объекта анализа в виде сетевого потока. В работе [5] было предложено использовать «сэмплинг» для потоков.

Большинство анализаторов СТ используют библиотеки Libcap/WinPcap для записи поступающих пакетов в специальный бинарный формат PCAP (*Packet Capture*), который имеет следующую структуру [6]: глобальный заголовок файла, заголовки и содержание пакетов.

Среди текстовых форматов представления полуструктурированных данных выделены XML (*eXtensible Markup Language*) и JSON (*Java Script Object Notation*). ПО Wireshark позволяет экспортировать пакетные данные сетевого трафика в формат JSON и два следующих формата на основе XML:

1. PSML (*Provisioning Services Markup Language*) – формат, включающий сводку сетевого трафика: (1) номера пакетов; (2) время получения; (3) IP-адреса отправителей и получателей; (4) наименования протоколов и (5) дополнительная информация, зависящая от типа пакета.

2. PDML (*Packet Details Markup Language*) – формат, включающий сведения о принятых пакетах в виде элементов <packet>, которые имеют один или несколько элементов <proto>. Последний отражает содержание одного протокола за счет следующих атрибутов [7]: (1) имя поля (name); (2) имя для печати (*showname*); (3) размер (*size*); (4) начальная позиция заголовков текущего протокола (*pos*). Для каждого поля протокола элемент <proto> должен иметь один вложенный элемент <fields> со следующими атрибутами: (1) имя поля (name); (2) имя для печати (*showname*); (3) значение поля в виде шестнадцатеричной строки (value); (4) размер текущего поля (size); (5) начальная позиция текущего поля (pos); (6) связное значение поля (*showmap*); (7) объяснение ценности поля (*showdtl*).

В формате JSON структура данных СТ аналогична структуре PDML, однако каждый элемент представлен объектом JSON – неупорядоченным множеством пар «ключ: значение», заключенное в фигурные скобки. Информация о пакетах представлена следующими основными ключами [8]: (1) «_index» – базовое имя; (2) «_type» - тип документа; (3) «_source» - тело документа; (4) «layers» - слои протоколов пакета; (5) «eth» (*Ethernet*), «ip» (Internet Protocol), «tcp» (*Transmissioon Control Protocol*), «udp» (*User Datagram Protocol*) и другие протоколы.

В рамках данного исследования были выделены количественные и качественные характеристики форматов СТ для представления данных о сетевой активности. Количественные характеристики представлены следующими показателями:

1. Средний размер пакета N в байтах.

2. Коэффициент преобразования ΔN, выраженный отношением размера исследуемого файла к размеру файла в формате PCAP (бинарном формате с минимальными затратами памяти для хранения информации).

3. Среднее число символов в экземпляре пакета.

Качественные характеристики форматов СТ выражены следующими показателями:

1. Содержательность – присутствие в формате СТ детальной информации: заголовков протоколов, физических и сетевых адресов узла источника и узла назначения, номера портов, время создания и завершения сетевых сессий и другие.

2. Компактность – минимизированные затраты ресурсов на хранение данных о сетевой активности.

3. Расширяемость – возможность изменять (дополнять) данные внутри файла СТ.

4. Поддержка перечисляемых типов данных (списки, словари и т. п.).

5. Понятность – человеко-ориентированность представления данных.

6. Поддержка Юникода – стандарта кодирования символов.

Для сравнения форматов СТ по указанным характеристикам были использованы данные о сетевой активности в размере 1000 перехваченных пакетов: (1) PCAP (783 Кб); (2) PSML (290 Кб); (3) PDML (34 099 Кб); (4) JSON (13 003 Кб). Результаты анализа выбранных форматов представлены в таблице.

ТАБЛИЦА. Сравнительная характеристика форматов представления данных

Параметр	PCAP	PSML XML	PDML XML	JSON
Средний размер пакета (Кб), N	0,783	0,29	34	13
Коэффициент преобразования, ΔN	1	0,37	43,55	16,6
Среднее число символов в экземпляре пакета	1 212	509	13 372	3 530
Содержательность	+	–	+	+
Компактность	+	+	–	+
Расширяемость	–	+	+	+
Поддержка перечисляемых типов данных	–	–	+	+
Понятность	–	+	+	+
Поддержка Юникода	–	+	+	+

Формат PCAP является основным для приложений, использующих библиотеки Libcap/WinPcap. В связи с жесткой структурированностью данного формата, его недостатками являются: отсутствие возможности дополнения данных о СТ посредством вставки и невозможность описания синтаксиса пакетов СТ.

Представленные форматы XML и JSON являются удобочитаемыми, что хорошо сказывается на визуальном восприятии информации. Однако в данном аспекте формат JSON обладает преимуществом, так как имеет более лаконичное синтаксическое описание, в отличии от форматов XML.

С учетом размера и структуры пакетов исходного набора данных СТ формат PSML является наиболее компактным, но не обладает достаточной содержательностью. В свою очередь, формат PDML предоставляет более подробное описание полей протоколов сетевого трафика, однако является наиболее ресурсозатратным для хранения, обработки и передачи данных. Формат JSON содержит более подробную информацию о пакете, чем формат PSML, и является более компактным по сравнению с PDML без потери содержательности данных СТ.

Использование формата JSON обеспечит более высокую скорость обмена данными, а также приведет к снижению нагрузки на сетевые каналы. Можно увидеть, что данные в формате XML, содержащие тот же объем информации, приблизительно в 3 раза больше.

В результате проведенных исследований были оценены форматы представления СТ, наиболее часто применяемые на практике. Выявлены достоинства и недостатки существующих способов представления СТ на этапах сбора, передачи, хранения и последующей обработки информации для оценки защищенности КФС. В результате сравнительного анализа текстовый формат JSON был выбран в качестве наиболее подходящего для представления сетевого трафика в случае, когда его структура не определена.

Работа выполнена при поддержке РФФИ (16-29-09482, 18-07-01488), гранта президента РФ (МК-314.2017.9), стипендии президента РФ (СП-751.2018.5), при частичной поддержке бюджетных тем (№ АААА-А16-116033110102-5), и при государственной финансовой поддержке ведущих университетов РФ (субсидия 074-U01).

Список используемых источников

1. Henzinger T., Sifakis J. The Embedded Systems Design Challenge // Lecture Notes in Computer Science. 2006. Vol.4085. P. 1–15.

2. Десницкий В. А., Котенко И. В., Ногин С. Б. Обнаружение аномалий в данных для мониторинга компонентов защиты Интернета вещей // XVIII Международная конференция по мягким вычислениям и измерениям (SCM'2015). Сборник докладов. Том 2. СПб. : Издательство СПбГЭТУ «ЛЭТИ». 2015. С. 17–22.

3. Cascarano N, Ciminiera L, Risso F. Optimizing deep packet inspection for high-speed traffic analysis. Network System Manager. 2011. N 19 (1). P. 7–31.

4. Callado A., Kamienski C., Szabo G., Gero B., Kelner J., Fernandes S., Sadok D. A. Survey on Internet Traffic Identification; Communications Surveys & Tutorials, IEEE. 2009. Vol. 11 (3). P. 37–52.

5. Duffield N., Lund C., Thorup M. Learn more, sample less: control of volume and variance in network measurement // IEEE Transactions in Information Theory. 2005. N 5. P. 1756–1775.

6. Libpcap File Format [Электронный ресурс] // Wireshark Wiki. URL:: https://wiki.wireshark.org/Development/LibpcapFileFormat#File_Format (дата обращения 07.12.2017)

7. PDML Specification, [Электронный ресурс] // URL: http://ftp.tuwien.ac.at/.vhost/analyzer.polito.it/30alpha/NetPDL/PDMLSpec.htm (дата обращения 07.12.2017)

8. Bray, T. The JavaScript Object Notation (JSON) Data Interchange [Электронный ресурс] // Internet Engineering Task Force (IETF). 2014. URL:: https://tools.ietf.org/html/rfc7159 (дата обращения 07.12.2017)

9. Baldi M., Risso F. Using XML for Efficient and Modular Packet Processing, [Электронный ресурс] // URL: https://pdfs.semanticscholar.org/2d8b/43890f56399762c6e38995c28de116526f66.pdf (дата обращения 07.12.2017)

Статья представлена заведующим лабораторией проблем компьютерной безопасности СПИИРАН, доктором технических наук, профессором И. В. Котенко.

УДК: 004.7

ОСОБЕННОСТИ РАЗРАБОТКИ ПРИЛОЖЕНИЙ ДЛЯ ПРОВЕДЕНИЯ DOS-АТАК

И. Ю. Гатчин, П. Н. Чистяков

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Выделив модели DoS-атак и используемые уязвимости, можно понять, как снизить угрозы, т.е. какие меры и средства необходимо внедрить для защиты информации и информационной системы в открытой сети. Понимание разработки и реализации ПО для DoS-атак позволяет понимать их алгоритмы и структуру, что поможет в создании программных средств защиты. Это поможет в создании средств защиты от DoS-атак, как, например, разработка и реализация анализатора трафика (снифера), необходимого для выявления сетевых атак (в т. ч. DoS).

вычислительные сети, сетевые атаки, разработка программ.

Отказ в обслуживании (*Denial of Service*, DoS) делает вычислительную сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, ОС (операционной системы) или приложения.

При распределенной атаке типа «отказ в обслуживании» (DDoS) входящий трафик, наводняющий жертву, происходит из разных источников. Это фактически делает невозможным остановить атаку, просто заблокировав один источник [1].

Для проведения DDoS атак необходимо очень большое количество запросов. Поскольку использование значительного числа вычислительных машин очень дорого для злоумышленника, используют «зараженные» машины. Такие машины имеют ПО, осуществляющие DoS-атаки. Зачастую деятельность таких программ скрывается от пользователя системы, поэтому такие программы обычно являются rootkit-приложениями.

Существует следующая классификация DoS-атак:

– насыщение полосы пропускания;
– недостаток ресурсов;
– ошибки программирования;
– маршрутизация и атаки DNS.

Наиболее распространены DoS-атаки осуществляющие переполнение полосы пропускания. Эти атаки связанны с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания системных ресурсов – процессора, памяти или каналов связи. Такие атаки называются флудом (англ. *flood* – «наводнение», «переполнение») и имеют несколько разновидностей.

1. *HTTP-flood* и *ping-flood*. ICMP-сообщение (эхо-запрос) обрабатывается сетевым оборудованием третьего (и выше) уровня. В большинстве случаев это оборудование использует программные средства маршрутизации и обработки пакетов. При этом эхо-запрос требует от устройства принятия пакета, его обработки и формирования/отправки пакета с ответом на запрос. Объём выполняемых действий при этом многократно превышает объём работы по маршрутизации обычного пакета.

Размер ICMP-запроса обычно небольшой (около 64 байт, при максимальном размере пакета IP 64 кбайт). В результате, при формальном сохранении небольшого трафика, возникает перегрузка по количеству пакетов, и устройство начинает терять остальные пакеты (по другим интерфейсам или протоколам), что и является целью атаки.

Проведение таких атак не требует дополнительных программных средств, и осуществимо с помощью терминала или командной строки.

2. *Smurf*-атака (ICMP-*flood*). Атака smurf заключается в передаче в сеть широковещательных ICMP запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к значительному снижению пропускной способности канала связи и, в ряде случаев, к полной изоляции атакуемой сети. Атака smurf очень эффективна и широко распространена.

Проведение такой атаки требует подмены MAC-адреса и IP-адреса источника отправляемого пакета.

3. Атака Fraggle является полным аналогом Smurf-атаки, где вместо ICMP пакетов используются пакеты UDP, поэтому её ещё называют UDP-flood. Принцип действия этой атаки простой: на седьмой порт жертвы отправляются echo-команды по широковещательному запросу. Затем подменяется IP адрес злоумышленника на IP адрес жертвы, которая вскоре получает множество ответных сообщений. Их количество зависит от числа узлов в сети. Эта атака приводит к насыщению полосы пропускания и полному отказу в обслуживании жертвы. Если все же служба echo отключена, то будут сгенерированы ICMP сообщения, что также приведёт к насыщению полосы.

4. Атака Syn-flood посылает большое число запросов на установление TCP соединения. Согласно процессу «трёхкратного рукопожатия» TCP, клиент посылает пакет с установленным флагом SYN (*synchronize*). В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (*acknowledges*). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.

Принцип атаки заключается в том, что злоумышленник, посылая *SYN*-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес, как представлено на рис. В очереди подключений появляются так называемые полуоткрытые соединения (англ. *half-open connection*), ожидающие подтверждения от клиента. По истечении определенного времени эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся

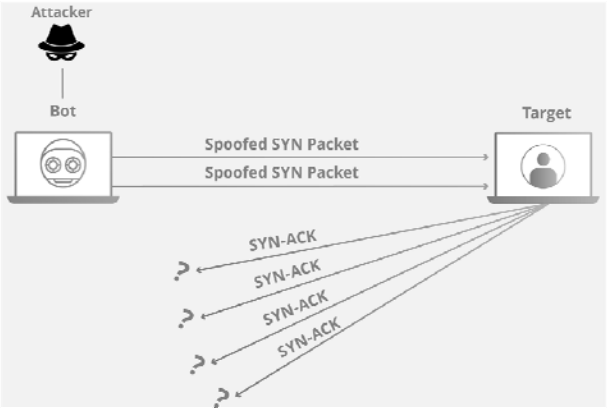


Рисунок. SYN-flood атака

злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.

Рассмотрим, как разрабатываются и реализуются приложения (программы) для DoS-атак.

При разработке обычных сетевых приложений в качестве интерфейса (API) для передачи данных в TCP/IP сетях используют сокеты (в UNIX среде это библиотека *socket*, для Windows используют адаптированный аналог *Winsock*).

Для реализации некоторых DoS-атак (например, SIN-*flood*) необходимо формировать заголовки TCP/IP пакетов вручную. Для этого используются так называемые «сырые» сокеты (*raw socket*). Но в Windows Winsock API не позволяет использовать такой тип сокетов. Приложение можно скомпилировать, но передавать или принимать данные оно не будет.

Выходом из такой ситуации является библиотека Pcap (*Packet Capture*), которая позволяет создавать программы анализа сетевых данных, поступающих на сетевую карту компьютера (т. е. в обход API операционной системы). Для Unix-подобных систем это библиотека libpcap, а для Microsoft Windows – WinPcap.

Программное обеспечение сетевого мониторинга может использовать libpcap или WinPcap, чтобы захватить пакеты, путешествующие по сети, и (в более новых версиях) для передачи пакетов в сети. Libpcap и WinPcap также поддерживают сохранение захваченных пакетов в файл и чтение файлов, содержащих сохранённые пакеты. Программы, написанные на основе libpcap или WinPcap, могут захватить сетевой трафик, анализировать его. Файл захваченного трафика сохраняется в формате, понятном для приложений, использующих Pcap.

Замаскировав действия такого ПО для DoS-атаки от обычного пользователя, по факту превратив приложение в руткит (*rootkit*) и найдя способ его распространения на вычислительные машины других пользователей в сети, злоумышленник получит огромную сеть, способную проводить успешные DDoS атаки.

Список используемых источников

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М. : ДМК Пресс, 2012. 593 с.

Статья представлена научным руководителем, доктором технических наук, профессором Ю. А. Гатчиным.

УДК 621.395

ОБСЛУЖИВАНИЕ МУЛЬТИМЕДИЙНЫХ ПОТОКОВ С ПРИОРИТЕТНЫМИ ОЧЕРЕДЯМИ

И. В. Гвоздков, Ю. Ф. Кожанов, А. И. Ликарь

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

В зависимости от вида услуги в IP-сети существуют нормированные значения доставки информации (пакета) «из конца в конец».

Производится расчет задержек для мультимедийных потоков на интерфейсе маршрутизатора при использовании механизма обслуживания очередей с абсолютными приоритетами.

маршрутизатор, приоритетное обслуживание, нагрузка, среднее время пребывания.

В зависимости от вида услуги в IP-сети существуют нормированные значения доставки информации (пакета) «из конца в конец». Рекомендация Y.1541 [1] определяет численные значения параметров, для различных услуг, существующих в настоящий момент. Численные значения рассмотренных параметров приведены в таблице.

ТАБЛИЦА. Численные значения параметров доставки

Параметр	Описание	Классы качества обслуживания					
		Класс 0	Класс 1	Класс 2	Класс 3	Класс 4	Класс 5
IPTD	Верхняя граница среднего значения (Прим. 1)	100 мс	400 мс	100 мс	400 мс	1 с	U
IPDV	Верхняя граница разности (IPTD – min IPTD) с квантилем 0,999 (Прим. 2)	50 мс	50 мс	U	U	U	U
IPLR	Верхняя граница	0,001	0,001	0,001	0,001	0,001	U
IPER	Верхняя граница	0,0001	0,0001	0,0001	0,0001	0,0001	U

Примечания: U – означает не специфицировано.

1. Определяется как среднее арифметическое совокупности пакетов. В некоторых случаях это значение для классов 0 и 2 не всегда достижимо. С другой стороны, не исключается возможность меньшего значения.

2. Суммарное значение задержки IPTD+IPDV в 99,9 % не должно превышать 150 мс в течение коротких интервалов времени (для класса 0). Для длинных интервалов времени в этом же случае используется квантиль 95 %.

Рекомендация Y.1541 устанавливает соответствие между классом качества обслуживания и наиболее соответствующими ему приложениями:

Класс 0 – приложения реального времени, чувствительные к джиттеру, характеризуемые высоким уровнем интерактивности (VoIP, видеоконференции через наземные каналы связи);

Класс 1 – приложения реального времени, чувствительные к джиттеру, характеризуемые невысоким уровнем интерактивности (VoIP, видеоконференции через спутниковые каналы связи);

Класс 2 – транзакции данных, характеризуемые высоким уровнем интерактивности (например, сигнализация);

Класс 3 –обмен данными с низким уровнем интерактивности (web-сайты, электронная почта);

Класс 4 – приложения, допускающие низкий уровень потерь (короткие транзакции, большие массивы данных, потоковое видео);

Класс 5 – традиционные применения сетей IP.

Выполнение этих требований достигается присвоением каждому потоку класса обслуживания и введением механизма обслуживания очередей для каждого класса.

Для обслуживания очередей используется один из ниже перечисленных механизмов: взвешенного справедливого обслуживания потока (*Weighted Fair Queuing*, WFQ), взвешенного справедливого обслуживания классов (*Class-Based Weighted Fair Queuing*, CBWFQ), с абсолютными приоритетами (*Priority Queue*, PQ).

В данной работе производится расчет задержек для мультимедийных потоков на интерфейсе маршрутизатора при использовании механизма обслуживания очередей с абсолютными приоритетами.

При использовании механизма с абсолютными приоритетами (***Priority Queue,*** **PQ**) с прерыванием обслуживания уже находящихся в обслуживании вызовов создаются четыре класса (очереди): high, medium, normal, low.

Планировщик очередей всегда начинает обслуживание очереди с класса high без прерывания обслуживания уже находящихся в обслуживании вызовов. Только после того, как все пакеты этого класса будут обслужены, начнется обслуживание класса medium. Соответственно, передача класса low окажется возможной только после того, как будут обслужены все более приоритетные классы. Вполне возможно, что в моменты перегрузки сети вся скорость передачи интерфейса будет занята высокоприоритетными пакетами, а передача пакетов класса low будет происходить с большими задержками.

Для системы ***M/M/1///PQ*** справедливы следующие предположения:

– на вход системы поступают четыре пуассоновских потока с интенсивностями вызовов $\lambda 1$, $\lambda 2$, $\lambda 3$, $\lambda 4$, соответственно;

– длительность занятия подчиняется экспоненциальному распределению с параметром μ;

– вызов, не принятый к обслуживанию в момент занятости линии пучка, поступает в свою бесконечную очередь. При освобождении линии поочередно обслуживаются все вызовы из первой очереди, затем – все вызовы из второй, третьей, четвертой очереди. Следовательно, вызовы четвертого потока обслуживаются только при отсутствии в очереди вызовов первого, второго и третьего потоков;

– пучок доступен, когда он свободен, для любого вызова;

– исходной для расчета является поступающая нагрузка;

– система находится в стационарном режиме.

Интенсивности нагрузок равны $a1 = \lambda 1/\mu$, $a2 = \lambda 2/\mu$, $a3 = \lambda 3/\mu$, $a4 = \lambda 4/\mu$, $a = a1 + a2 + a3 + a4 < 1$, при этом условии все потоки будут обслужены.

Поскольку потоки низших приоритетов не влияют на потоки высших приоритетов, то для первого потока в системе ***M/M/1/ / /PQ*** имеем [2]:
среднее число вызовов только первого потока в системе:

$$Q1 = Qe1 = \frac{a1}{1-a1};$$

среднее время пребывания вызова в системе:

$$te1 = \frac{Qe1}{\lambda 1} = \frac{1}{\mu}\frac{1}{1-a1}, \qquad a1<1.$$

Для второго потока в системе ***M/M/1/ / /PQ***:
среднее число вызовов только 1 и 2 потоков в системе:

$$Q2 = \frac{(a1 + a2)}{1 - a1 - a2},$$

среднее число вызовов второго потока в системе:

$$Qe2 = Q2 - Q1 = \frac{a2}{(1 - a1 - a2)(1 - a1)};$$

среднее время пребывания вызова в системе:

$$te2 = \frac{Qe2}{\lambda 2} = \frac{1}{\mu(1 - a1 - a2)(1 - a1)}, \qquad a1+a2<1.$$

Для третьего потока в системе ***M/M/1/ / /PQ***:
среднее число вызовов только 1, 2 и 3 потоков в системе:

$$Q3 = \frac{(a1 + a2 + a3)}{1 - a1 - a2 - a3},$$

среднее число вызовов третьего потока в системе:

$$Qe3 = Q3 - Q2 = \frac{a3}{(1 - a1 - a2 - a3)(1 - a1 - a2)};$$

среднее время пребывания вызова в системе:

$$te3 = \frac{Qe3}{\lambda 3} = \frac{1}{\mu(1 - a1 - a2 - a3)(1 - a1 - a2)}, a1+a2+a3<1.$$

Для четвертого потока в системе ***M/M/1/ / /PQ***:
среднее число вызовов 1, 2, 3 и 4 потоков в системе:

$$Q4 = \frac{(a1 + a2 + a3 + a4)}{1 - a1 - a2 - a3 - a4},$$

среднее число вызовов четвертого потока в системе:

$$Qe4 = Q4 - Q3 = \frac{a4}{(1 - a1 - a2 - a3 - a4)(1 - a1 - a2 - a3)};$$

среднее время пребывания вызова в системе:

$$te4 = \frac{Qe4}{\lambda 4} = \frac{1}{\mu(1 - a1 - a2 - a3 - a4)(1 - a1 - a2 - a3)}, a1 + a2 + a3 + a4 < 1.$$

Пример расчета

На систему *M/M/1/ / /PQ* поступает четыре потока с параметрами $\lambda 1 = 2{,}5$ с$^{-1}$, $\lambda 2 = 2{,}5$ с$^{-1}$, $\lambda 3 = 2{,}5$ с$^{-1}$, $\lambda 4 = 2{,}5$ с$^{-1}$, $\mu = 11$ с$^{-1}$. Определить среднее время ожидания конца обслуживания для каждого потока.

Решение.

$$\lambda = \lambda 1 + \lambda 2 + \lambda 3 + \lambda 4 = 10 \text{ с}^{-1},$$

$$a1 = 0{,}227 \text{ Эрл}, a2 = 0{,}227 \text{ Эрл}, a3 = 0{,}227 \text{ Эрл},$$

$$a4 = 0{,}227 \text{ Эрл}, a = 0{,}909 \text{ Эрл}.$$

Среднее время ожидания конца обслуживания первого потока:

$$te1 = \frac{1}{\mu}\frac{1}{1 - a1} = 0{,}117 \text{ с};$$

среднее время ожидания конца обслуживания второго потока:

$$te2 = \frac{1}{\mu(1 - a1 - a2)(1 - a1)} = 0{,}215 \text{ с};$$

среднее время ожидания конца обслуживания третьего потока:

$$te3 = \frac{1}{\mu(1-a1-a2-a3)(1-a1-a2)} = 0{,}524 \text{ с};$$

среднее время ожидания конца обслуживания четвертого потока:

$$te4 = \frac{1}{\mu(1-a1-a2-a3-a4)(1-a1-a2-a3)} = 3{,}142 \text{ с}.$$

В системе без приоритетов:

$$te1 = te2 = te3 = te4 = \frac{1}{\mu}\frac{1}{1-a} = 1 \text{ с}.$$

Список используемых источников

1. ITU-T Recommendation Y.1541. Network performance objectives for IP-based Services.

2. Кожанов Ю. Ф. Качество обслуживания в сетях связи; СПбГУТ. СПб., 2014. 160 с.

УДК 004.7:004.422.8

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ОБМЕНА В МУЛЬТИАГЕНТНОЙ СИСТЕМЕ ИНТЕГРАЦИИ СЕРВИС-ОРИЕНТИРОВАННЫХ КОМПЛЕКСОВ

Ю. А. Голутвина, Л. К. Птицына

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

Описаны объективные причины актуальности применения онтологического подхода к организации информационного обмена в мультиагентной системе интеграции сервис-ориентированных комплексов. Проанализированы известные парадигмы построения онтологий. Приведены формализации описания онтологий для интеллектуальных информационных систем. Предложена парадигма онтологии для организации информационного обмена в мультиагентной системе интеграции сервис-ориентированных комплексов. Детализированы ключевые элементы формального описания генерируемой онтологии. Раскрыты приёмы инвариантной организации информационного обмена.

онтология, интеллектуальная информационная система, сервис-ориентированные системы, мультиагентные системы.

Информационный обмен является образующей составляющей взаимодействия субъектов и объектов любой сферы социально-экономической деятельности. Стратегическое направление повышения экономического роста и национального суверенитета позиционируется с созданием экосистемы цифровой экономики, в которой осуществляется эффективное взаимодействие трансграничных систем, бизнеса, научно-образовательного сообщества, государства и граждан, погружаемое в информационную инфраструктуру с обеспечиваемой информационной безопасностью. Повышение эффективности взаимодействия ассоциируется с внедрением технологий искусственного интеллекта. В связи с этим актуализируется интеллектуализация информационного обмена. Наряду с этим, интенсивно расширяются магистральные направления развития технологий искусственного интеллекта, связанные с агентными технологиями и онтологическими технологиями [1]. Каждый из указанных технологических сегментов, имеющий высочайший собственный потенциал, наполняется новыми компонентами, повышающими их значимость в профессиональной деятельности и расширяющими области применения. Одновременно с указанными тенденциями проявляются и другие характерные особенности рассматриваемого взаимодействия. При погружении взаимодействия трансграничных систем, бизнеса, научно-образовательного сообщества, государства и граждан в информационную инфраструктуру разрастаются масштабы применения сервис-ориентированных систем (СОС), группируемых в соответствующие комплексы в соответствии с характером предметных областей. Для каждого подобного комплекса предлагаются инновационные наукоёмкие интегральные интеллектуальные решения для объединения составляющих сервисов, основанные на включении в их архитектуру интеллектуальных информационных агентов с планируемыми действиями и модельно-аналитического интеллекта, оценивающего и контролирующего качество функционирования сервис-ориентированной системы [2].

На уровне взаимного согласования и объединения предметных областей образующих элементов экосистемы цифровой экономики образуются множества сервис-ориентированных комплексов, нуждающихся в интеграции. С позиций системного подхода и технологической однородности для интеграции сервис-ориентированных комплексов с агентным управлением предлагается мультиагентная система, информационный обмен интеллектуальных агентов в которой организуется на основе онтологического подхода. В предлагаемом решении проблемы преодоления априорной неопределённостей различного характера решаются не только за счёт введения в архитектуру каждого артефакта искусственного интеллекта (комплекса сервис-ориентированных систем) интеллектуального информационного агента с планируемыми действиями и модельно-аналитического

интеллекта, но и с помощью построения мультиагентной системы, информационный обмен в которой организуется на основе онтологического подхода.

Для поиска решений научно-технических задач интеллектуальной интеграции сервис-ориентированных систем проводятся исследования, в ходе которых формируются методики создания и интеграции сервис-ориентированных систем [3]. В исследованиях используются математическое моделирование, нотации моделирования бизнес-процессов для их формального описания и среды программирования для автоматизации формирования программного продукта. Однако вопросы интеллектуального информационного обмена в мультиагентной системе интеграции интеллектуальных сервис-ориентированных комплексов на основе онтологического подхода остаются открытыми.

В настоящее время применяется ряд известных парадигм построения онтологий, разделяемых на три группы: группа математических парадигм, группа компьютерных парадигм и группа парадигм «Эсперанто», представляющая компромиссный подход.

Для группы математических парадигм свойственна формальная непротиворечивость. Для обработки онтологий, формируемых с помощью подобных парадигм, рекомендуются дедуктивный метод, логика первого порядка и вычислительно прослеживаемые подмножества логики. В парадигме выделяется предпочтительность использования онтологий высшего порядка, поскольку в них используются фундаментальные термины такие как «объект», «свойство», «реляция», которые актуальны для любых предметных областей. Наиболее известные реализации такой группы парадигм – Basic Formal Ontology (BFO), SUMO, BORO.

Группа компьютерных парадигм опирается на натурализацию окружающего мира. Основным критерием построения онтологии является полезность. Для конструирования новых онтологий не придерживаются строгих методологий. Распространяется множество эвристических решений, компьютерных программ и языков компьютерной онтологии. В связи с этим парадигма подобного рода формулируется следующим образом: онтология для информационных систем есть компьютерный артефакт [4]. Самыми известными примерами реализации парадигм второй группы считаются RDF-онтологии, OWL-онтологии.

Группа парадигм «Эсперанто» характеризуется как компромисс между первыми двумя группами парадигм. В данном случае поддерживается создание онтологий любой формы. Главным принципом считается ее полезность и эффективность в контексте специфических проблем. В подобной группе парадигм определяются социологические цели концентрации информации. Этому способствует их намеренная политика облегчения коммуникации между различными сообществами.

Из вышеперечисленных групп парадигм онтологий для интеллектуализации информационного обмена в мультиагентной системе интеграции интеллектуальных сервис-ориентированных комплексов выбирается группа компьютерных парадигм, потому как для построения сервис-ориентированных систем преимущественно используются компьютерные технологии и web-сервисы, которые взаимодействуют между собой по протоколу SOAP.

Наиболее распространённым из известного множества видов онтологий, соответствующих компьютерной парадигме, является OWL-онтология. Описание формальной модели онтологии информационного обмена между сервисами сервис-ориентированной системы определяется следующим кортежем:

$$\mathbf{Out} = <\mathbf{T}, \mathbf{R}, \mathbf{F}>,$$

где **T** – конечное множество понятий (концептов) предметной области, **R** – конечное множество отношений между понятиями, **F** – конечное множество функций интерпретации, заданных на концептах и/или отношениях.

Ниже описываются ключевые элементы для каждого из элементов OWL-онтологии, составленной для интеграции сервисов и предназначенной для определения ее качества (рис.).

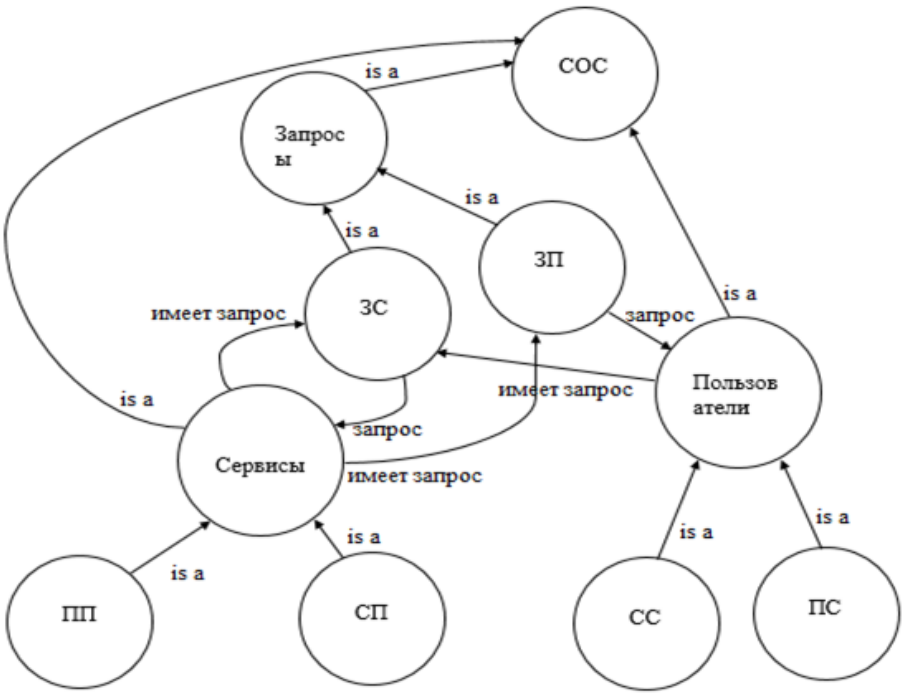


Рисунок. Онтология информационного обмена в сервис-ориентированной системе

T = {СОС, Сервисы, Запросы, Пользователи, Пакетные приложения, Собственные приложения, Запросы к пользователю, Запросы к сервису, Сотрудники сервиса, Потребители сервиса};

R = {Сервисы *is a* СОС; Пользователи *is a* СОС; Запросы *is a* СОС; Пакетные приложения (ПП) *is a* Сервисы; Собственные приложения (СП) *is a* Сервисы; Запросы к пользователю (ЗП) *is a* Запросы; Запросы к сервису (ЗС) *is a* Запросы; Сотрудники сервиса (СС) *is a* Пользователи; Потребители сервиса (ПС) is a Пользователи};

F – множество функций интерпретации, задается индивидуально в зависимости от предметной области сервис-ориентированной системы.

Отношения между индивидами классов имеют вид свойство-значение [5]. Ключевые свойства: имеет запрос к пользователю, имеет запрос к сервису.

Сервис в данном случае – это видимый ресурс, выполняющий повторяющуюся задачу и описанный внешней инструкцией [6]. Представленный тип онтологии относится к нижнему уровню онтологий, соответствующих информационному обмену в мультиагентной системе интеграции интеллектуальных сервис-ориентированных комплексов.

Для организации информационного обмена в сервис-ориентированных системах используется протокол обмена структурированными сообщениями SOAP. Данный протокол используется не только для вызова процедур, но и для обмена произвольными сообщениями в формате XML. Чаще всего протокол SOAP используется поверх протокола HTTP. Ограничений на использование с другими протоколами прикладного уровня не имеется, но каждый процесс характеризуется своими особенности. Правильно собранные SOAP-запросы становятся удобными в использовании и понятными даже обычному пользователю. Однако у них есть один недостаток, связанный со снижением скорости обработки запросов из-за увеличения объема самих сообщений. Если в системе скорость обработки запросов является критичным критерием, то целесообразно пользоваться пересылкой XML-документов через HTTP напрямую. В таком случае параметры запроса будут передаваться через HTTP параметры.

При предлагаемом подходе повышается степень интеллектуализации процессов информационного обмена при взаимодействии трансграничных систем, бизнеса, научно-образовательного сообщества, государства и граждан в информационной инфраструктуре, что является неоспоримым преимуществом для расширения возможностей преодоления неопределённостей различного характера, присущих развитию жизнедеятельности социума.

Список используемых источников

1. Птицына Л. К. Методологическое профилирование интеллектуализации информационных инфраструктур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; 2016. Т. 1. С. 31–35.

2. Кондратьев Д. А., Птицына Л. К., 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.; 2016. Т. 2. С. 108–113.

3. Птицына Л. К., Веселов В. О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоёмкие технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 42–47.

4. Целищев В. В. Парадигмы онтологий в информационных системах // Вестник Новосибирского государственного университета. Серия: философия, 2013. Т. 1. № 1. С. 5–11.

5. OWL. Язык веб онтологий. Руководство. URL: http://sherdim.ru/pts/semantic_web/REC-owl-guide-20040210_ru.html (дата обращения: 25.01.2018).

6. Сервис-ориентированное моделирование и архитектура. URL: https://www.ibm.com/developerworks/ru/library/ws-soa-design1/index.htm (дата обращения: 20.12.2018).

УДК 621.39.001.63, 621.391.1.037.37

МОДЕЛИРОВАНИЕ УСТРОЙСТВА ЗАЩИЩЕННОГО ШИРОКОПОЛОСНОГО ОБМЕНА СООБЩЕНИЯМИ

А. Ю. Гришенцев[1], А. И. Елсуков[1,2], А. Г. Коробейников[1,3]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Научно-производственное объединение «Аврора»
[3]Институт земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук, Санкт-Петербургский филиал

Публикация посвящена моделированию приемо-передающей системы широкополосной радиосвязи скрытой подшумовой передачи сообщений. Реализация математической модели была осуществлена в среде Simulink (Matlab). Широкополосные сигналы формировались при помощи комплексных матриц с особой формой автокорреляционной функции. В приемопередающей системе была применена адаптивная синхронизация методом смещенного окна, которая позволила в разы сократить вычислительные затраты на прием сообщений. Также было произведено исследование модели на устойчивость передачи данных при искажении передаваемого сигнала аддитивным белым гауссовым шумом. При искажении сигнала мультипликативной помехой и помехой многолучевого распространения сигнала устойчивость передачи определяется методом синхронизации, применяемой в приемо-передающей системе.

широкополосная радиосвязь, подшумовая радиопередача, обработка сигналов, радиостеганография, математическое моделирование.

Снижение вероятности обнаружения сигнала в радиоэфире при передаче данных является актуальной задачей, решение которой может применяться в различных целях. Методы скрытой передачи в большинстве, случаев базируются на распределении энергии сигнала в достаточно большой области частотно-временного пространства при передаче данных. Задачей принимающего устройства в таком случае является концентрация энергии из данной области, которая ему известна, в точку.

В работе представлены результаты математического моделирования, при помощи Simulink (MatLab) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12], приемо-передающей системы (ППС) широкополосной связи скрытой подшумовой передачи сообщений.

По определению широкополосный сигнал (ШС) [13, 14, 15] имеет $WT > 1$, где W – ширина полосы частот занимаемой сигналом, T – длительность сигналов. ШС в данной работе формировались при помощи комплексных матриц с особой формой автокорреляционной функции (АКФ) [16, 17, 18, 19, 20, 21, 22]. Особенностью таких матриц является то, что форма их АКФ имеет вещественный максимум в центре при относительно малых значениях боковых лепестков, имеющих комплексные значения. ШС сформированные на основе таких матриц, используются в системах с поляризационным разделением сигналов [23], в системах с временным или частотным разделением автокорреляционных гармонических составляющих [24].

Для комплексной матрицы A с особой формой АКФ размером $N_A \times M_A$, можно сформировать ШС при помощи выражение:

$$s(t) = \sum_{i=1}^{M_A} \left[\mathrm{Re}(A_{ix}) \cos\left(\frac{2\pi f_0 it}{N_A}\right) + \mathrm{Im}(A_{xi}) \sin\left(\frac{2\pi f_0 it}{N_A}\right) \right],$$

где f_0 – опорная частота, $x = \left\lceil \frac{t \cdot M_A}{T} \right\rceil$. Значение f_0 выбирается так, чтобы каждому элементу матрицы A соответствовала сумма гармонических функций, число периодов каждой из которых кратно $\frac{T}{N_A}$.

На рис. 1 представлена блок схема моделируемой ППС.

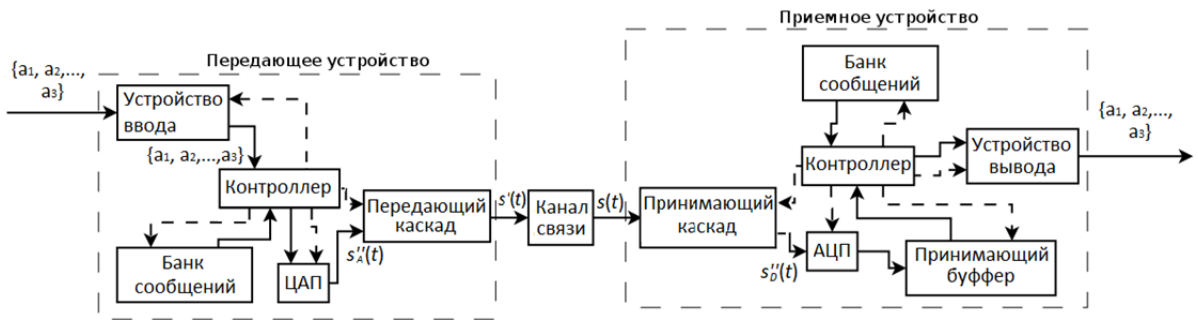


Рис. 1. Блок схема ППС. Сплошными стрелками показано направление движения данных. Пунктирными стрелками показаны управляющие воздействия

Основной задачей передающего устройства является сопоставление кодовых последовательностей из множества $C = \{a_1, a_2, \dots, a_n\}$ некоторым ШС из множества $B = \{s_1, s_2, \dots, s_n\}$. Элементы множества C поступают на вход устройства ввода, откуда дальше к контроллеру. Контроллер сопоставляет поступившие последовательности с сигналами из банка сообщений, в котором хранятся элементы B. После сопоставления в цифроаналоговом преобразователе (ЦАП) осуществляется преобразование сигнала из цифрового в аналоговый вид. Затем аналоговый сигнал, через передающий каскад, передается в радиоэфир. Передающий каскад содержит усилитель и антенну.

Также передающее устройство перед началом передачи данных формирует и передает последовательность сигналов синхронизации, реализованной в данной модели методом смещенного окна [25]. Сигнал при передаче проходит через канал связи, в котором он искажается различными типами помех: аддитивный белый гауссов шум (АБГШ), мультипликативная помеха [26] и помеха, связанная с многолучевым распространением сигнала. Математически канал связи возможно представить, как:

$$s(t) = \sum_{i=1}^{D} \left[g_i(t) \left(h_i(t) * s'(t) \right) \right] + w(t),$$

где t – время, $h_i(t) * s'(t)$ – свертка с импульсной характеристикой $h_i(t)$, характеризующей линейные искажения вносимые каналом связи в сигнал, распространяющийся по i-му лучу, $g_i(t)$ – мультипликативная составляющая помехи i-го луча распространения сигнала, $w(t)$ – АБГШ, D – число путей распространения сигнала.

Принимающее устройства осуществляет получение радиосигнала из канала связи принимающим каскадом, который содержит антенну и усилитель. Далее он оцифровывается ЦАП с сохранением в принимающем буфере. Основной задачей контроллера приёмного модуля является осуществление адаптивной синхронизации методом смещенного окна [25, 27] и распознавание принятых сигнальных образов, с помощью вычисления взаимно-корреляционной функции (ВКФ) [15, 22]:

$$R_{fm_k}[l] = f \bullet m_k = \sum_{i=0}^{N-1} f[i] m_k[i - l],$$

где f – принятый сигнал, m_k – сигнальный образ, с которым производится сравнение.

Процесс синхронизации разделен на синхронизацию в начале сеанса связи, к которой приемник готов в режиме ожидания сеанса связи, и синхронизацию, осуществляемую в процессе передачи данных, возникающую

при отслеживании пика ВКФ, и адаптируемой к изменениям фазы сигнала в канале связи. На рис. 2 представлена диаграмма принятых сигналов, искаженных гауссовым шумом. Отображение сигналов осуществлялось с использованием скалярного произведения [27] принятых сигналов с известными. После распознавания сигнальных символов, в приемном устройстве, осуществляется вывод полученных элементов сообщения через устройство вывода.

В данном исследовании было произведено моделирование канала связи и приемопередающей системы широкополосной связи скрытой подшумовой передачи сообщений. При реализации приёмного устройства была применена адаптивная синхронизация методом смещенного окна. Исследование модели показали, что система способна успешно осуществлять передачу сигналов скрытых подшумом радиоэфира. Устойчивость системы к мультипликативным помехам и помехами связанным с многолучевым распространением сигнала определяется методом синхронизации. Также были проведены исследования на устойчивость передачи данных при искажении сигнала АБГШ.

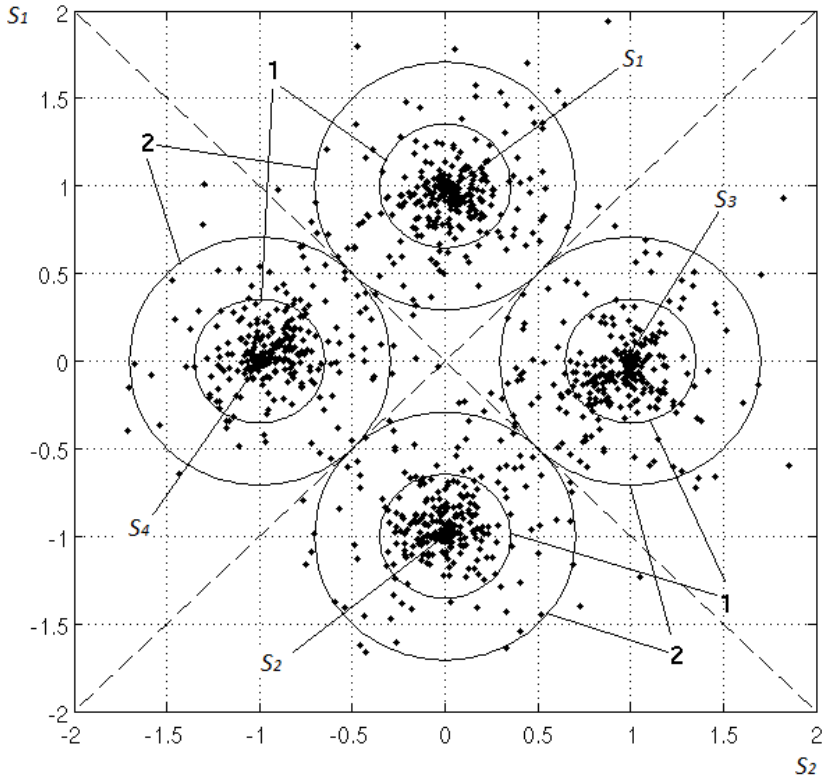


Рис. 2. Отображение принятых приемником сигналов на сигнальной плоскости.
– известные сигнальные образы

Список используемых источников

1. Солонина А. И. Цифровая обработка сигналов. Моделирование в Simulink // СПб. : БХВ-Петербург, 2012. 432 с.: ил.

2. MatLab, Simulink. URL: https://www.mathworks.com/products/simulink.html

3. Donald C. Electronics Engeneers' Handbook, 4th ed. // McGraw-Hill, 1996. 350 p.

4. Кобейников А. Г. Разработка и анализ математических моделей с использованием MATLAB и Maple : учебное пособие. СПб. : СПбГУ ИТМО, 2010. 144 с.

5. Коробейников А. Г. Проектирование и исследование математических моделей в средах MATLAB и Maple. СПб. : СПбГУ ИТМО, 2012. 160 с.

6. Коробейников А. Г., Гришенцев А. Ю. Разработка и исследование многомерных математических моделей с использованием систем компьютерной алгебры. СПб. : НИУ ИТМО, 2014. 100 с. https://elibrary.ru/download/elibrary_26121279_54604165.pdf

7. Коробейников А. Г., Кутузов И. М., Колесников П. Ю. Анализ методов обфускации // Кибернетика и программирование. 2012. № 1. С. 31–37.

8. Коробейников А. Г., Кутузов И. М. Алгоритм обфускации // Кибернетика и программирование. 2013. № 3. С. 1–8.

9. Коробейников А. Г, Гатчин Ю. А. Математические основы криптологии : учебное пособие. СПб. : СПб ГУ ИТМО, 2004. 106 с, илл.

10. Гришенцев А. Ю., Коробейников А. Г. Средства интероперабельности в распределенных геоинформационных системах // Журнал радиоэлектроники. 2015. № 3. С. 19.

11. Гришенцев А. Ю., Коробейников А. Г., Дукельский К. В. Метод численной оценки технической интероперабельности // Кибернетика и программирование. 2017. № 3. С. 23–38.

12. Гришенцев А. Ю., Коробейников А. Г., Гурьянов А. В., Шукалов А. В. Автоматизация проектирования распределенных геоинформационных систем : учебное пособие. СПб. : Университет ИТМО, 2017. 96 с.

13. Семёнов А. М., Сикарев А. А. Широкополосная радиосвязь. М .: Воениздат, 1970. 280 с.: ил.

14. Ipatov P. Spread Spectrum and CDMA. Principles and Applications. Wiley, 2004. 373 p.

15. Ипатов В. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М. : Техносфера, 2007. 488с.

16. Гришенцев А. Ю., Коробейников А. Г. Алгоритм поиска, некоторые свойства и применение матриц с комплексными значениями элементов для стеганографии и синтеза широкополосных сигналов // Журнал радиоэлектроники. 2016. № 5. URL: http://jre.cplire.ru/jre/may16/11/text.pdf

17. Гришенцев А. Ю., Коробейников А. Г. Понижение размерности пространства при корреляции и свертке цифровых сигналов // Изв. вузов. Приборостроение. 2016. Т. 59, № 3. С. 211–218. DOI 10.17586/0021-3454-2016-59-3-211-218.

18. Гришенцев А. Ю., Коробейников А. Г. Теоремы об уменьшении размерности пространства при корреляции и свертке // Журнал радиоэлектроники. 2015. № 1. URL: http://jre.cplire.ru/jan15/19/text.pdf

19. Гришенцев А. Ю., Коробейников А. Г., Величко Е. Н., Непомнящая Э. К., Розов С. В. Синтез бинарных матриц для формирования сигналов широкополосной связи // Радиотехника. 2015. № 9. С. 51–58.

20. Стивен С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных сотрудников; пер. с англ. М. : Додэка-XXI, 2012. 720 с.

21. Гришенцев А. Ю., Гурьянов А. В., Тушканов Е. В., Шукалов А. В., Коробейников А. Г. Виртуализация и программное обеспечение в системах автоматизированного проектирования : учебное пособие. СПб. : Университет ИТМО, 2017. 60 с.

22. Гришенцев А. Ю., Гурьянов А. В., Кузнецова О. В., Шукалов А. В., Коробейников А. Г. Математическое обеспечение в системах автоматизированного проектирования. СПб. : Университет ИТМО, 2017. 88 с.

23. Дятлов А. П., Кульбикаян Б. Х. Корреляционная обработка широкополосных сигналов в автоматизированных комплексах радиомониторинга. М. : Горячая линия – Телеком, 2013. 333 с.

24. Гришенцев А. Ю. О методе разделения во времени автокорреляционных гармонических составляющих широкополосных сигналов // Журнал радиоэлектроники. 2016. № 9. URL: http://jre.cplire.ru/jre/sep16/2/text.pdf

25. Гришенцев А. Ю., Елсуков А. И. Адаптивная синхронизация в системах скрытой широкополосной связи // Научно-технический вестник информационных технологий, механики и оптики. 2017.Т. 17, № 4. С. 640–650.

26. Freeman R. L. Radio System Design for Telecommunications. Third Edition, IEEE, Wiley-Interscience, 2007. 880 p

27. Гришенцев А. Ю., Елсуков А. И., Коробейников А. Г., Сидоркина И. Г. Разработка и модельная реализация приёмопередающего устройства скрытого подшумового обмена радиосообщениями // Вестник ЧГУ. 2017. № 3. С. 195–206.

28. Тактаров Н. Г. Справочник по высшей математике для студентов вузов // Изд. Стереотип. М. : Книжный дом «ЛИБРОКОМ», 2014. 880 с.

УДК 004.891.2

ЭКСПЕРТНАЯ СИСТЕМА ДЛЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАНОСТИ НА ПРЕДПРИЯТИИ

А. Ю. Гришенцев[1], К. Д. Житков[1], А. Г. Коробейников[1,2]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

[2]Институт земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук, Санкт-Петербургский филиал

В современном мире сложно представить себе организацию, в которой информационные технологии не были бы тесно интегрированы в бизнес-процессы. Для обеспечения эффективной защиты информации на предприятии необходимо своевременное проведение аудита информационной безопасности. Одним из инструментов для проведения аудита являются экспертные системы. В данной статье описывается авторская реализация подобной системы, приводится структурная схема и алгоритм работы.

экспертная система, нечеткая логика, аудит информационной безопасности.

Проведение экспертного аудита информационной безопасности (ИБ) на предприятии необходимо для принятия эффективных управленческих решений в области защиты информации. Аудит состояния ИБ представляет собой независимое экспертное обследование основных аспектов ИБ, а также их проверку на соответствие определенным требованиям.

Аудит принято разделять на внешний и внутренний, при этом в качестве отдельного вида внутреннего аудита выделяют самооценку ИБ. Самооценка ИБ проводится, как правило, сотрудниками службы безопасности (СБ) для установления степени соответствия установленным критериям защищенности информационных ресурсов. Результат самооценки ИБ может быть использован при подготовке к проведению полноценного аудита ИБ [1, 2].

Существующие решения в области ЭС для аудита ИБ [3, 4], как правило, предполагают два режима работы [5, 6, 7, 8]: приобретение знаний и консультация. В первом случае осуществляется наполнение базы знаний инженером по знаниям. Во втором – диалог конечного пользователя с системой через соответствующий интерфейс: аудитор вводит в ЭС известные ему сведения о текущем состоянии ИБ, получая в результате список обнаруженных уязвимостей, а также рекомендации по их устранению. Такой принцип работы не позволяет проводить опрос нескольких сотрудников одновременно, предполагая присутствие аудитора при каждом опросе для ввода данных в систему.

Предлагается разделить режим консультации на две составляющие, отвечающие за ввод и вывод информации соответственно. В режиме ввода данных осуществляется сбор информации о предприятии посредством опроса сотрудников, а в режиме вывода – отображение отчета о проведенном аудите.

Таким образом, разработанная система предполагает использование тремя типами пользователей: инженер по знаниям, аудитор и сотрудник предприятия.

В обязанности инженера по знаниям входит организация знаний: сбор, структуризация и ввод в систему. В качестве источников знаний выступают общепризнанные стандарты в области информационной безопасности. Структурированные знания хранятся в базе данных в виде нечетких правил и используются для сравнения введенной пользователем информации с некими эталонными значениями. В результате, система может не только формировать советы по исправлению недочетов, но и объяснять логику принятия тех или иных решений.

Аудитор ИБ отвечает за запуск очередного аудита и выбор сотрудников предприятия для проведения опроса. В случае проведения самооценки ИБ организации, в роли аудитора может выступать сотрудник СБ. Резуль-

таты проведенных аудитов сохраняются в системе и доступны аудитору для дальнейшего анализа.

Сотрудники предприятия, на котором проводится аудит ИБ, имеют доступ только к опросным листам, разработанным инженером по знаниям.

Использование теории нечетких множеств при создании экспертной системы обеспечивает возможность математического представления качественных оценок, выражаемых людьми в форме лингвистических значений и нечетких чисел.

Нечеткие ЭС преобразуют значения входных переменных в выходные с помощью использования нечетких правил продукций. Используемый в разработанной экспертной системе механизм нечетких выводов в своей основе имеет базу знаний в виде совокупности нечетких предикатных правил вида:

$$\text{ЕСЛИ «}\beta_1 \text{ ЕСТЬ } \mathbf{P}\ \alpha_1\text{», ТО «}\beta_2 \text{ есть } \mathbf{P}\ \alpha_2\text{» } (F_i),$$

где β_1 и β_2 – это входная и выходная лингвистические переменные, α_2 и α_2 – это соответствующие нечеткие переменные, **P** – лингвистический модификатор, а F_i – коэффициент неопределенности правила ($i \in \{1, 2, ..., n\}$). Конструкцию вида β *ЕСТЬ* **P** α называют нечетким высказыванием.

Коэффициент неопределенности является экспертной оценкой достоверности правила, определяет значимость правила и может принимать значения в интервале [0, 1].

В формальном виде нечеткую переменную можно задать через набор:

$$<\alpha, X, A>,$$

где: α – название нечеткой переменной; X – универсальное множество, на котором заданы значения α (область рассуждений); A – нечеткое подмножество универсального множества X.

Лингвистической переменной будем называть переменную с лингвистическими значениями, выражающими качественные оценки. Она может либо быть входной, либо выходной и представляет из себя кортеж вида:

$$<\beta, T, X, G, M>,$$

где: β – название лингвистической переменной; T – базисное лингвистическое множество (конечное терм-множество, элементами которого являются названия нечетких переменных); X – универсальное множество; G – синтаксическое правило, позволяющее генерировать новые термы с применением слов естественного или формального языка; M – семантическое правило, которое каждому значению лингвистической переменной ставит в соответствие нечеткое подмножество множества X.

Основные этапы нечеткого вывода реализованы согласно алгоритму Мамдани-Заде.

Использование качественных (нечетких) оценок при проведении аудита ИБ позволяет обобщить большие объемы данных, помогая аудитору увидеть более полную картину [9]. Экспертные системы могут использоваться в качестве вспомогательного инструмента при осуществлении внешнего или внутреннего аудита ИБ. Кроме того, подобные системы могут быть использованы сотрудниками служб безопасности предприятий при проведении самооценки ИБ как самостоятельные инструменты, позволяющие проводить опрос сотрудников в короткие сроки, проверять степень соответствия текущего состояния системы рекомендуемому стандартами, предлагать рекомендации по исправлению недочетов, а также документировать результаты проверок.

Список используемых источников

1. Иванова Н. В., Коробулина О. Ю. Экспертная система аудита информационной безопасности // Программные продукты и системы. 2010. N 4. С. 89–91.

2. Atymtayeva L., Kozhakhmet K. Development of Expert System for Iinformation Security Audit // International Journal of Computer Research. 2015. N 4. С. 399.

3. Коробейников А. Г., Гришенцев А. Ю., Кутузов И. М., Пирожникова О. И., Соколов К. О., Литвинов Д. Ю. Разработка математической и имитационной моделей для расчета оценки защищенности объекта информатизации от несанкционированного физического проникновения // NB: Кибернетика и программирование. 2014. № 5. С. 14–25.

4. Коробейников А. Г., Федосовский М. Е., Гришенцев А. Ю., Поляков В. И. Метод инфологического моделирования в инженерии знаний для решения задач автоматизированного проектирования // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 10. С. 925–931.

5. Korobeynikov A. G., Fedosovsky M. E., Maltseva N. K., Baranova O. V., Zharinov I. O., Gurjanov A. V., Zharinov O. O. Use of information technologies in design and production activities of instrument-making plants // Indian Journal of Science and Technology. 2016. Т. 9. № 44. С. 104708.

6. Бондаренко И. Б., Коробейников А. Г., Прохожев Н. Н., Михайличенко О. В. Принятие технических решений с помощью многоагентных систем // Кибернетика и программирование. 2013. № 1. С. 16–20.

7. Гришенцев А. Ю., Гурьянов А. В., Тушканов Е. В., Шукалов А. В., Коробейников А. Г. Виртуализация и программное обеспечение в системах автоматизированного проектирования : учебное пособие. СПб. : Университет ИТМО, 2017. 60 с.

8. Гришенцев А. Ю., Гурьянов А. В., Кузнецова О. В., Шукалов А. В., Коробейников А. Г. Математическое обеспечение в системах автоматизированного проектирования. СПб. : Университет ИТМО, 2017. 88 с.

9. Теплов Э. П., Гатчин Ю. А., Нырков А. П., Коробейников А. Г., Сухостат В. В. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции. СПб. : Университет ИТМО, 2016. 120 с.

УДК 004.75

МИКРОКОМПЬЮТЕРЫ В ГОСАВТОИНСПЕКЦИИ РОССИИ

В. В. Громов

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

В настоящее время создание систем удаленного доступа приняло массовый характер для практически любой организации, которая создала свой интернет сайт. Многие компании пытаются создать сложные глобальные системы используя сложные, дорогостоящие технологии, не обращая внимания на основополагающие технологии построения простейших клиент-серверных приложений на основе off-line запросов. Данная статья раскрывает некоторые секреты формирования корпоративных вычислительных сетей.

связь компьютеров, локальные сети, распределенные системы обработки данных.

Выбор темы «Микрокомпьютеры в Госавтоинспекции России» связан представлением поколению 2000-х разработок, которые легли в основу современных информационных систем. Первое применение микрокомпьютеров в Госавтоинспекции России связано с созданием Федеральной информационной системы Госавтоинспекции России (Далее ФИС ГИБДД).

ФИС ГИБДД – уникальный проект реализации распределенной базы данных для МВД России, который был начат в1995 г. в Москве в ГУ ГАИ МВД РФ (в Главном Управлении Госавтоинспекции России) [1].

Середина 90-х гг. XX века – «время перемен» в Российском государстве, которое затронуло не только политическое устройство нашей страны, но и устройство всех исполнительных ветвей власти, к которым относится и МВД России. В период с 1992–2005 г. время активных изменений информационных системах в МВД России и в частности в Госавтоинспекции. С учётом плюрализма мнений создавались локальные и глобальные информационные системы ГИБДД регионального, межрегионального и федерального уровня [1].

В основу всех систем закладывались параметры:

- минимальная стоимость;
- надежность системы;
- длительный срок эксплуатации;
- простота использования;
- мобильность;
- оперативность;

– защита данных и системы от «взлома»;
– соблюдение режима конфиденциальности;
– удаленный доступ к системе.

Каждый региональный отдел информационного обеспечения ГИБДД старался создать универсальную систему для своей службы и попытаться её внедрить на федеральном уровне. Различные фирмы и отделы информационного обеспечения соревновались между собой в условиях «демократической» конкуренции для создания единого информационного пространства. Это было «золотое время»! Руководители невзирая на чины, прислушивались к мнению сотрудников как «высшего руководящего состава», так и низового уровня МВД России. Результатом данного плюрализма стало создание ФИС ГИБДД, системы которая проработала без обслуживания более 7 лет.

С одной стороны, данные факты негативно говорят об отношении к информационной системе, но с другой стороны данный факт показывает, что была создана практически «идеальная информационная система» в которую не требовалось внесение глобальных изменений.

Так оно и было! В основу системы вошла группа межрегиональных серверов с базами данных соединенных в единую корпоративную сеть. Для создания системы использовались сервера Sun Fire V890 под управлением, ОС Solaris 8-10 ver.

Ещё до ввода в опытную эксплуатацию ФИС ГИБДД был определен транспортный формат взаимодействия создаваемой системы и порядок обращения к ней. Для доступа к информационным массивам предлагалось использовать «on-line» доступ по средствам корпоративной вычислительной сети, и «off-line» доступ по средствам коммутируемых каналов связи или GPRS-каналов.

Если вопрос по коммутируемым каналам и средствам вычислительной техники был разрешен моментально, а именно:

1. Рабочее место на базе ПК-компьютера.
2. Принтер.
3. Модем для двухпроводных линий со скоростью от 2400bps.

Для мобильного доступа вопрос оставался открытым, т.к. на момент создания прототипа системы, зарубежные корпорации не выпускали GPRS модемы для стационарных компьютеров, не было планшетов и смартфонов, а был только PALM (рис. 1) и Apple Newton (рис. 2).

Оба этих карманных планшетных компьютера (как их ещё называли «наладошники» или КПК) работали с внешними устройствами – телефон, компьютер, а PALM работал ещё с GPS приёмниками.

Стоимость такого компьютера составляла порядка 400$ USD. Огромные деньги по тем временам для государственных учреждений. Поэтому,

работы по данному проекту были поручены коммерческому предприятию – ООО «Росби Информ К».

Рис. 1. КПК PALM

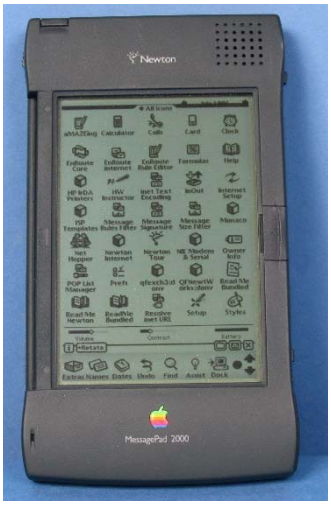


Рис. 2. КПК Apple Newton

Был приобретен один комплект – КПК Palm Tungsten 3, который был соединен по «blue tooth» каналу с сотовым телефоном для возможности доступа к «всемирной паутине». Далее использовались коммерческие сети и сети с крипто маршрутизаторами ФАПСИ (Федеральное Агентство правительственной связи и информации), для обеспечения транспорта от КПК до сервера ФИС ГИБДД.

Результат был потрясающий! Сотрудник МВД, мог формировать запрос на КПК Palm Tungsten 3, с помощью специального приложения. Затем запрос по средствам специального почтового агента отправлялся в виде файла в межрегиональный центр. Затем происходила обработка запроса и тем же путем пересылался ответ на КПК Palm Tungsten 3. С момента отправки запроса, до момента обработки ответа на КПК Palm Tungsten 3 проходило не более 40–50 секунд! Это был потрясающий результат для 2004 г.!

Данный эксперимент позволил определить приоритетное направление развития систем удаленного доступа – КПК, а в дальнейшем бортовые компьютеры и планшетные компьютеры.

В 2005 г. вместе с закупленными серверами Sun Fire V890 на вооружение поступили первые КПК компьютеры на базе Windows Mobile (см. рис. 3 ниже), которые были переданы в строевые подразделения и другие ведомства.

Первые 30 штук подобных карманных персональных компьютеров были введены в эксплуатацию в 2005 г. Началась эра мобильных устройств на службе МВД России, а в частности в Госавтоинспекции [2].

В заключение, хотелось отметить, что планы оснастить практически всех сотрудников Госавтоинспекции подобными устройствами «испарились как утренний туман» по мере сокращения финансирования подразделений. Учитывая, что современный смартфон на базе ОС Android стоит от 2000 рублей, не возникало проектов подобных описанному выше для комплексного оснащения сотрудников МВД, но это уже другая история [3].

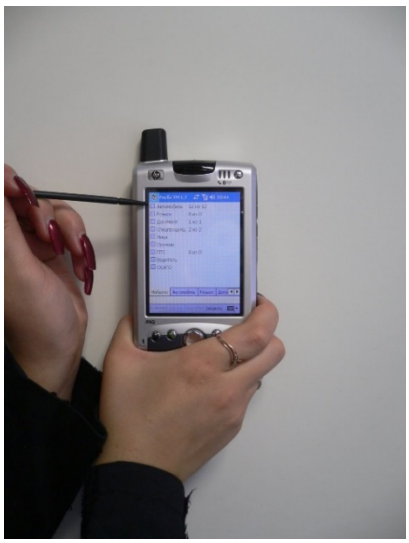


Рис. 3. КПК HP iPAQ h5450

Список используемых источников

1. Громов В. В. Организация информационного взаимодействия разнородных региональных сетей ГИБДД (на примере Межрегионального центра «Северо-Запад»). : дис ... канд. техн. наук : 05.13.13 / В. В. Громов. – М.: МИЭМ, 2004. – 144 с. Библиогр.: с. 115–122.

2. Приказ МВД России от 5 февраля 2016 г. N 60 «О порядке эксплуатации специального программного обеспечения Федеральной информационной системы Госавтоинспекции». URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=653703;fld=134;from=11184-139;rnd=203280.015356685686837457;;ts=020328045606727063938 47

3. Громов В. В. Информационные системы Госавтоинспекции России // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб. : СПбГУТ, 2017. С. 230–232.

УДК 004.5, 004.8

АНАЛИЗ МЕТОДОВ ПРОЕКТИРОВАНИЯ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ НА БАЗЕ ОНТОЛОГИИ ПРЕДМЕТНОЙ ОБЛАСТИ

А. Н. Губин, В. Л. Литвинов, Д. В. Литвинов, Ф. В. Филиппов

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

Развитие технологий и появление новых требований к разработке информационных систем приводит к частичному усложнению интерфейсов, связанному не только с увеличением набора функций информационных систем, но и с различными изменяющимися условиями их эксплуатации. В данной работе рассмотрены концепции расши-

ряемости инструментария для проектирования и реализации пользовательского интерфейса в рамках онтологического подхода.

пользовательский интерфейс, онтология предметной области.

Разработка пользовательского интерфейса (ПИ) является трудоемкой задачей. По подсчетам различных специалистов, в среднем она занимает не менее половины времени разработки программного продукта. При этом, с развитием технологий и появлением новых требований к разработке информационных систем, происходит частичное усложнение интерфейсов, связанное не только с увеличением набора функций информационных систем, но и с различными изменяющимися условиями их эксплуатации.

Для снижения трудоемкости разработки и сопровождения ПИ в настоящее время существуют различные средства автоматизации проектирования и реализации: построители WIMP-интерфейсов, моделеориентированные средства и средства, основанные на онтологическом подходе [1].

Отметим, что все перечисленные средства ориентированы на автоматизацию разработки пользовательских интерфейсов со статическими данными, для которых сценарий диалога и визуальное представление полностью определяется на этапе проектирования интерфейса. В то же время для редакторов, программ, в которых наборы входных/выходных данных генерируются логикой приложения, а также гибко конфигурируемых приложений наборы входных/выходных данных, структуру каждого набора, а также сценарий диалога невозможно определить на этапе проектирования интерфейса. Такие интерфейсы называют интерфейсами с динамическими данными [2].

Целью данной работы является исследование концепций расширяемости инструментария для проектирования и реализации пользовательского интерфейса в рамках онтологического подхода.

Определение интерфейса в рамках онтологического подхода предполагает наличие только той информации, которая может измениться в жизненном цикле информационной системы. Разработчики приложений используют эти знания для создания подходящих интерфейсов для представления данных: разумный набор данных, группирование и последовательность элементов ввода, отображение/скрытие разделов или навигация между страницами. Это знание неявно используется разработчиком и основано на его опыте или других правилах, которые являются неявным знанием. Основная идея данного подхода включить эти семантические знания в модель, ориентированную на данные, вместе с обработанными данными приложения.

Открытость, являясь важным требованием к архитектуре инструментальных комплексов для автоматической генерации программного кода,

достигается явным представлением систем понятий в виде онтологий. Разработчику предоставляются сторонние структурные и графические редакторы для формирования компонент пользовательского интерфейса, управляемых онтологиями. Такой подход позволяет изменять компоненты без модификации кода, однако, если модифицирование инструментария требует изменение кода интерфейса, то разработчик может работать с моделью генерации кода, которая описывает соответствия между алгоритмами бизнес-логики и компонентами модели интерфейса. Архитектура программного комплекса представлена на рис. 1.

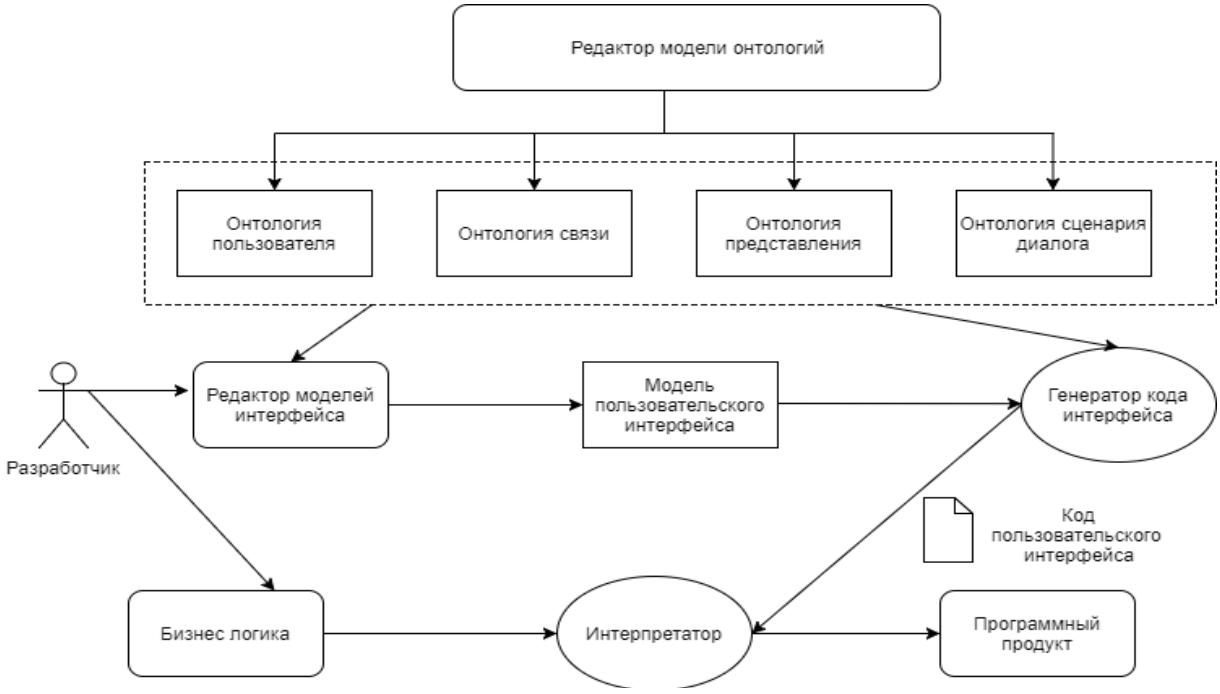


Рис. 1. Архитектура инструментального комплекса

Разработка программного комплекса может быть проведена с помощью библиотеки EasyRdf [3]. EasyRdf – это PHP-библиотека, предназначенная для упрощения работой с RDF файлами. После разбора EasyRdf создает граф объектов PHP, который затем можно найти, чтобы разместить данные на странице. Имеются методы дампа, позволяющие проверить, какие данные доступны во время разработки. Данные обычно загружаются в объект EasyRdf / Graph из исходных RDF-документов, загружаемых из Интернета через HTTP. Класс EasyRdf / GraphStore упрощает загрузку и сохранение данных, а также дальнейшую работу с использованием SPARQL. Пример показан на рис. 2.

Для описания элементов данных (т. е. типов и ограничений вида диапазонов или допустимых значений) необходима типовая и структурная информация, а также значимая временная последовательность экранов.

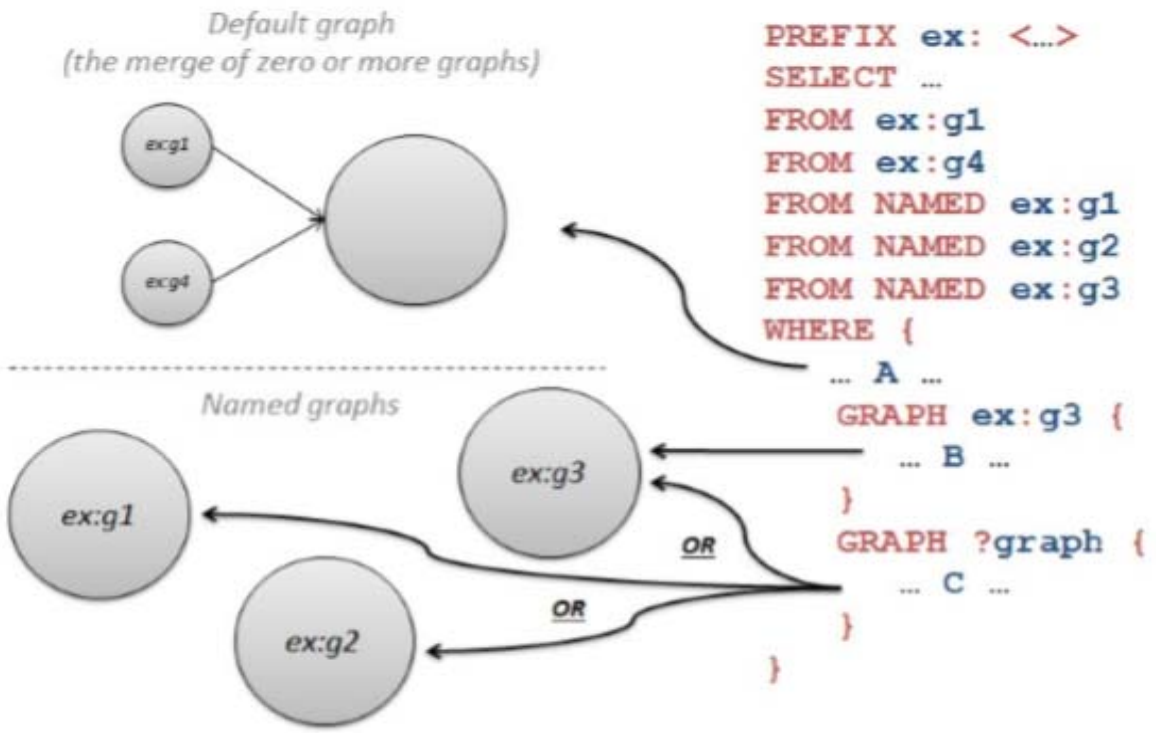


Рис. 2. Пример SPARQL запроса к дереву RDF

Поведенческая информация необходима для моделирования динамических, связанных с данными аспектов пользовательского интерфейса для проверки во время выполнения (условия существования, активации элементов / групп, связанных с содержанием других элементов данных в модели, указание для комплексной проверки, операции, связанные с элементами данных и группами, вызванными изменениями входных данных (реакций) или вызванными действиями пользователя.

Эта совокупность информации была сочтена адекватной для получения различных аспектов пользовательского интерфейса.

На основе полученных данных была разработана метамодель, которая включает идентифицированную информацию и послужила основой для разработки описаний данных для генерации пользовательского интерфейса (см. рис. 3 ниже).

Таким образом, в статье описана методология автоматической генерации программного кода пользовательского интерфейса по его проекту, представлен анализ онтологического подхода к автоматизации проектирования пользовательского интерфейса.

Список используемых источников

1. Грибова В. В., Клещев А. С. Управление проектированием и реализацией пользовательского интерфейса на основе онтологий // Проблемы управления. 2006. № 2. С. 58–62.

2. Грибова В. В., Черкезишвили Н. Н. Автоматизация разработки пользовательских интерфейсов с динамическими данными // Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): материалы междунар. науч.-техн. конф., Минск, 10–12 февраля 2011 г. / редкол. : В. В. Голенков (отв. ред.) [и др.]. – Минск : БГУИР, 2011. С. 287–293.

3. EasyRdf Documentation [электронный ресурс]. Режим доступа: https://github.com/njh/easyrdf (дата обращения 25.03.2017).

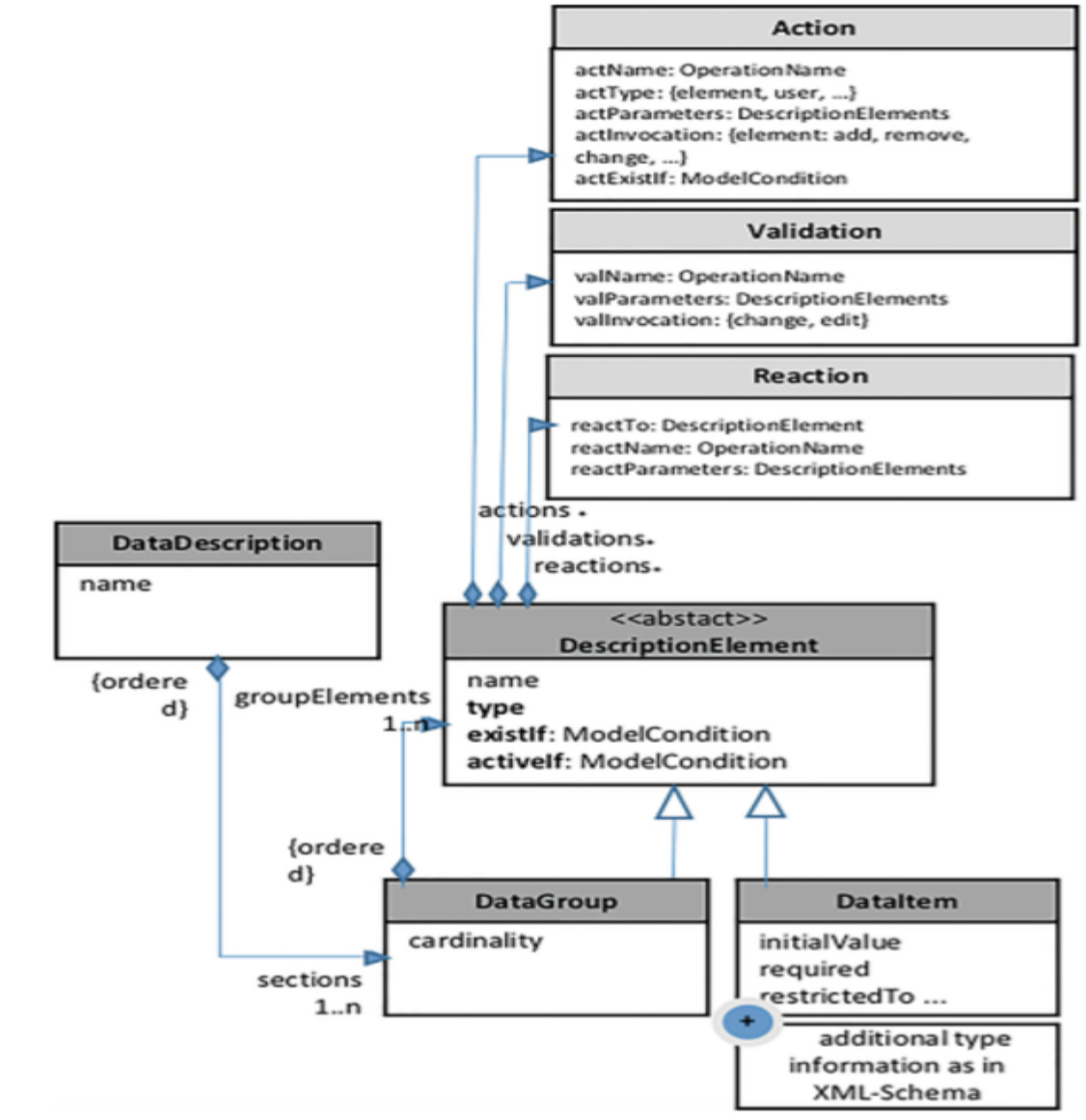


Рис. 3. Метамодель, описанная с помощью UML нотации

УДК 621.3

ВЫБОР ПАРАМЕТРОВ ПРИ РАЗРАБОТКЕ РЕКУРСИВНЫХ ЦИФРОВЫХ СГЛАЖИВАЮЩИХ ФИЛЬТРОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Вопрос о расположении нулей характеристического полинома рекурсивных цифровых сглаживающих фильтров внутри заданной области остается открытым, хотя их положение оказывает существенное влияние на величину дисперсии случайной ошибки на выходе фильтра. В данной статье рассматривается решение задачи выбора значений нулей характеристического полинома цифровых фильтров в процессе их оптимизации.

цифровые фильтры, дисперсия случайной ошибки, время наблюдения, характеристический полином.

При разработке рекурсивных цифровых сглаживающих фильтров искомый оператор обычно представляют в виде передаточной функции

$$\Phi(z) = \frac{K(z)}{Q(z)},$$

где z – аргумент Z-преобразования.

Оптимизация таких операторов цифровой фильтрации предполагает определение параметров многочлена $K(z)$, минимизирующего дисперсию случайной ошибки на выходе фильтра [1].

При этом предполагается, что характеристический полином фильтра $Q(z) = (z - j_1)\,(z - j_2)\,\ldots\,(z - j_m)$ задан.

Это означает, что прежде, чем приступить к оптимизации параметров фильтра необходимо произвести выбор значений $j_1, j_2, \ldots j_m$, который осуществляется с учетом ограничений, налагаемых требованиями обеспечения устойчивости:

$$|j_i| < 1,\ i = 1, 2, \ldots, m$$

и обеспечения заданного времени переходного процесса (времени наблюдения входного сигнала) [2]:

$$n_{\text{наб}} \approx \lg \delta_{\text{доп}} / \lg |j_{\max}|,$$

где $\delta_{доп}$ – допустимое значение ошибки при воспроизведении полезного сигнала, j_{max} – наибольший по модулю нуль характеристического полинома фильтра.

Однако вопрос о расположении нулей характеристического полинома внутри заданной области остается открытым, хотя их положение оказывает существенное влияние на величину дисперсии случайной ошибки на выходе фильтра.

В связи с этим возникает задача исследования поведения дисперсии случайной ошибки как функции нулей характеристического полинома фильтра с целью разработки практических рекомендаций по выбору оптимальных, с точки зрения минимума дисперсии σ^2, значений $j_1, j_2, \ldots j_m$ при проектировании операторов цифровой фильтрации.

Для решения поставленной задачи рассмотрим случай подавления стационарной некоррелированной помехи цифровыми фильтрами со следующей передаточной функцией:

$$\Phi(z) = \frac{b_0 + 0,5b_0(z-1)}{Q(z)},$$

где $b_0 = Q(z)\big|_{z=1}$.

Величина дисперсии случайной ошибки на выходе фильтра определяется контурным интегралом:

$$\sigma^2 = \oint_{|z=1|} \Phi(z)\Phi(z^{-1})\frac{dz}{z},$$

который может быть вычислен с помощью теоремы о вычетах. Однако это обычно связано с довольно громоздкими преобразованиями и большим объемом вычислений. Поэтому для определения значений дисперсии воспользуемся следующим методом [3]. Если представить оператор цифрового фильтра в виде дробно-рационального выражения:

$$\Phi(z) = \frac{b_0 z^n + b_1 z^{n-1} + \ldots + b_n}{c_0 z^n + c_1 z^{n-1} + \ldots + c_n},$$

то значение дисперсии можно определить, как частное от деления двух детерминантов:

$$\sigma^2 = \frac{\det E}{\det F},$$

где

$$F = \begin{bmatrix} c_0 & c_1 & \dots & c_n \\ c_1 & c_0 + c_1 & \dots & c_{n-1} \\ \dots & \dots & \dots & \dots \\ c_n & 0 & \dots & c_0 \end{bmatrix},$$

а матрица E получается путем замены в F первого столбца вектором B:

$$B = \begin{bmatrix} \sum_{i=0}^{n} b_i^2 \\ 2\sum_{i=0}^{n-1} b_i\, b_{i+1} \\ \dots \\ 2b_0 b_n \end{bmatrix}.$$

В дальнейшем ограничимся рассмотрением цифровых фильтров с характеристическим полиномом:

$$Q(z) = (z - j_1)(z - j_2).$$

В этом случае, с учетом последних выражений, величина дисперсии случайной ошибки на выходе фильтра определится следующим соотношением:

$$\sigma^2 = \frac{1}{2}\frac{(1 - j_1)(1 - j_2)}{1 - j_1 j_2}.$$

Анализ полученного выражения показывает, что областью наименьших значений дисперсии являются значения, которые принимает σ^2 при положительных вещественных j_1 и j_2. Причем, при прочих равных условиях, наилучшие результаты подавления помех достигается при $j_1 = j_2$, то есть при кратных положительных нулях характеристического полинома.

Действительно, при j_1 и j_2=c, где c – любое вещественное число из области допустимых значений, величина дисперсии определяется следующим выражением:

$$\sigma^2(c) = \frac{1}{2}\frac{(1 - c)}{1 + c}.$$

При $j_1=c$ и любых значениях $j_2<c$, величина дисперсии определяется соотношением:

$$\sigma^2(c, j_2) = \frac{1}{2}\frac{(1-c)(1-j_2)}{1-cj_2},$$

которое легко преобразуется к виду:

$$\sigma^2(c, j_2) = \frac{1}{2}\frac{(1-c)}{1+c}\left[1+\frac{c-j_2}{1-cj_2}\right].$$

Очевидно, что слагаемое:

$$\frac{c-j_2}{1-cj_2} > 0$$

при любых $j_2 < c$ и, следовательно, при принятых условиях:

$$\sigma^2(c, j_2) > \sigma^2(c).$$

В случаях, когда j_1 и j_2 – комплексно-сопряженные числа, то есть $j_1 = a + ib$, $j_2 = a - ib$, где $(a^2 + b^2) < 1$, выражение для σ^2 приобретает следующий вид:

$$\sigma^2 = \frac{1}{2}\frac{(1-a)^2+b^2}{(1-a^2)-b^2}.$$

После преобразований это равенство можно записать как:

$$\sigma^2 = \frac{1}{2}\frac{(1-a)}{1+a}\left[1+\frac{2b^2}{[1-(a^2+b^2)](1-a)}\right].$$

Слагаемое

$$\frac{2b^2}{[1-(a^2+b^2)](1-a)} > 0$$

при любых $b \neq 0$, откуда следует, что при любых $j_1 = a + ib$, $j_2 = a - ib$ величина дисперсии случайной ошибки на выходе фильтра будет превышать значении дисперсии при $j_1 = j_2 = a$.

Исследование цифровых фильтров более сложной структуры показывает, что и для них сохраняется тенденция поведения σ^2, аналогичная поведению дисперсии для рассматриваемого класса фильтров.

Таким образом, результаты проведенных исследований позволяют рекомендовать при проектировании оптимальных цифровых фильтров производить выбор значений нулей характеристического полинома фильтра из области положительных значений, причем наилучшие условия подавления помех обеспечиваются при кратных значениях нулей.

Список используемых источников

1. Губин А. Н., Литвинов В. Л. Особенности совместного использования цифровых рекурсивных и нерекурсивных фильтров // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. 2015. С. 479–482.

2. Хемминг Р. В. Цифровые фильтры; пер. с англ. / Под ред. А. М. Трахтмана. М. : Сов. Радио, 1980. 224 с.

3. Schneider F. Geschlossene Formeln zur Berechnung der quadratischen und zeitbeschwerten quadratischen Regelfflache continuerliche und diskret Sistem // Regelungstechnik. 14. № 4. P. 41–53.

УДК 004.62

ТЕОРЕТИКО-МНОЖЕСТВЕННЫЙ ПОДХОД К ПОИСКУ ИНФОРМАЦИИ В RDF-ХРАНИЛИЩАХ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Предлагается способ формализованного описания триплетов RDF-хранилищ, основанный на использовании теории множеств и позволяющий существенно сократить время поиска информации за счет замены процедур SPARQL на операции над множествами, доступными в языке программирования.

поиск данных, теория множеств, хранилище данных, RDF.

На концептуальном уровне набор данных RDF представляет собой набор троек $t = \langle s, p, o\rangle \in (U \cup B)\times U\times(U \cup B \cup L)$, где s – субъект, p – предикат, а o – объект. Счетно-бесконечные множества U, B и L являются обозначениями унифицированных идентификаторов ресурсов URI, пустых узлов и литералов, соответственно. Пустые узлы – это анонимные иденти-

фикаторы ресурсов, определенные в области набора данных. Литералы представляют собой константы, такие как числа, символьные строки и даты. Поскольку набор данных RDF может быть естественным образом представлен в виде помеченного графа, где субъекты и объекты являются узлами, а предикаты обозначены ребрами, набор данных часто называют графом RDF [1].

Базы знаний на основе RDF формируются в форме хранилищ наборов троек (триплетов), которые как правило записываются в текстовом виде в одном из форматов: RDF/XML, N-Triples, Turtle или JSON-LD. Для сокращения объема хранилища используются такие приемы, как введение префиксов для URI, опускание повторяющихся субъектов (с заменой точки в конце триплета на точку с запятой), опускание повторяющихся субъектов с предикатом (с заменой точки в конце триплета на запятую), описание пустых узлов внутри квадратных скобок, замена *rdf:type* на *a*, запись коллекций в круглых скобках. Аналогичные приемы используются для упрощения написания SPARQL запросов при поиске информации в хранилищах.

При описании больших объемов триплетов подобные приемы не оказывают существенного влияния на результирующий объем хранилища, а, главное, упрощая только написание запросов никоим образом не уменьшают время их исполнения.

Ниже предлагается подход формализованного описания больших объемов триплетов, основанный на использовании множеств U, B и L, позволяющий существенно сократить время поиска информации за счет замены ряда процедур SPARQL на операции над множествами доступными в языке программирования. В таблице 1 (см. ниже) приведен пример описания хранилища с помощью множеств, эквивалентный сериализации Turtle, а также запрос на языке R, эквивалентный языку SPARQL.

Существенным моментом в представленном примере является использование пакета data.table, который позволяет выполнять необходимую агрегацию данных хранилища с большой скоростью [2].

Хранилище данных естественным образом может быть отображено в трехмерном пространстве с координатами, представленными множествами всех значений субъектов, объектов и предикатов, используемых в триплетах. Подобное представление использовалось в [3, 4]. Каждый отдельный триплет будет представлять точку в этом пространстве. Положим, ось x соответствует субъектам из множества $s \in U \cup B$, ось y – объектам из множества $o \in U \cup B \cup L$ и ось z – предикатам из $p \in U$. Тогда наиболее естественной формой представления всех наборов хранилища будет три упорядоченных множества X_s, Y_o и Z_p, включающих соответственно все субъекты, объекты и предикаты в той последовательности, в которой они встречаются в триплетах. Более компактный способ наглядного представ-

ления этих данных предполагает рассмотрение плоскостей параллельных координатным плоскостям, включающий все точки, соответствующие ординате плоскости. Так плоскость, параллельная координатной плоскости *x*0*y* с ординатой *z = "subclass"*, будет включать точки определяющие координаты пар субъект – объект, связанные отношением подкласс. Реализация возможности такого компактного способа представления предполагает обеспечить независимую группировку и упорядочивание триплетов. Основной вопрос, с точки зрения сокращения времени выполнения запросов, состоит в скорости упорядочивания триплетов в соответствии с логикой запроса.

ТАБЛИЦА 1. Теоретико-множественное описание

Turtle описание хранилища	Описание с помощью множеств
:a dc10:title "SPARQL QueryLanguageTutorial" . *:a dc10:creator "Alice" .* *_:b dc11:title "SPARQL ProtocolTutorial" .* *_:b dc11:creator "Bob" .* *_:c dc10:title "SPARQL" .* *_:c dc11:title "SPARQL (updated)" .*	*Y = (("SPARQL QueryLanguageTutorial","Alice"), ("SPARQL ProtocolTutorial","Bob"), ("SPARQL ProtocolTutorial","Bob"))* *Z = (("dc10:title","dc10:creator"), ("dc11:title","dc11:creator"),("dc10:title","dc 11:title"))*
Запрос на SPARQL	**Запрос на языке R**
SELECT ?title *WHERE {* *{?book dc10:title ?title }* *UNION* *{?book dc11:title ?title } }*	*DT <- data.table(y = Y, z = Z)* *DT[z == ("dc10:title"),.(title = y)]* *DT[z == ("dc11:title"),.(title = y)]*

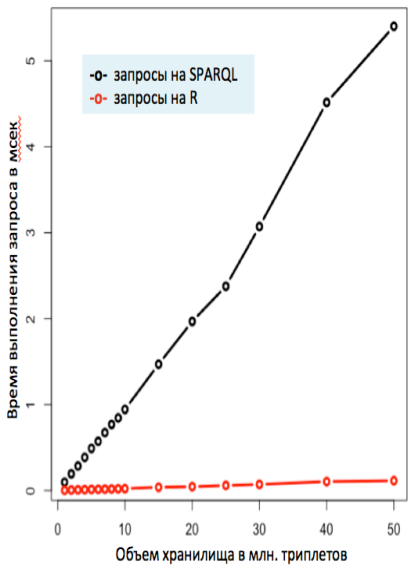
Известно много эффективных алгоритмов обработки больших массивов и, в частности, ассоциативных массивов. Наибольший выигрыш по скорости получается с использованием процедур бинарного поиска и сортировки с использованием ключей, аналогичных ключам ассоциативных массивов. Именно такие возможности предоставляет пакет data.table.

Множества X_s, Y_o и Z_p в этом пакете представляются в виде таблицы, которая может быть сформирована автоматически из фрейма хранилища. Назначение ключей осуществляется в соответствии со структурой и логикой запросов.

Рассмотрим простой пример, показывающий эффективность использования возможностей пакета data.table. В таблице 2 приведен пример кода моделирования запросов. Сначала формируются хранилища данных, включающие от одного до пятидесяти миллионов триплетов. Использование операции key() позволяет выполнять независимую группировку и упорядочивание триплетов. Так с помощью *key = c("y","z")* формируются

плоскости параллельные *x*0*y*, позволяющие мгновенно находить любые сочетания субъект-объект.

ТАБЛИЦА 2. Пример кода моделирования запроса

Код моделирования запросов	Время выполнения
WORDS1 = c("byte","cycle","global","name","planet") *WORDS2 = c("type","class","subclass","trend","is")* *WORDS3 = c("word","time","local","nick","earth")* *N = 1000000:50000000* *DT = data.table(x = sample(WORDS1, N, TRUE),* *y = sample(WORDS2, N, TRUE),* *z = sample(WORDS3, N, TRUE),* *key = c("y","z"))* *key(DT)* *(t1 <- system.time(DT[y == "class" & z == "time"]))* *(t2 <- system.time(DT[.("class", "time")]))*	

Для сформированных хранилищ производится сравнение времени выполнения запроса, отыскивающего все субъекты, для которых значение предиката *class = "time"*. Использование традиционных процедур, реализованных в стандарте SPARQL, затрачивает время t_1 = 0,097 мс, против t_2 = 0,003 мс на базе процедур пакета data.table языка *R*. Для хранилищ объемом вплоть до пятидесяти миллионов триплетов полученные временные оценки приведены на графике, представленном в таблице 2.

Кроме простейших операций сортировки и быстрого условного поиска пакет предоставляет большие возможности по быстрой группировке и агрегированию данных RDF-хранилища. Это в полной мере позволяет использовать теоретико-множественный подход для значительного повышения эффективности использования хранилищ большого объема в системах поиска информации в реальном времени.

Список используемых источников

1. Губин А. Н., Литвинов, В. Л., Турушева В. А., Филиппов Ф. В. Обеспечение заданного уровня доступа к данным в RDF-хранилищах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2017. С. 183–187.

2. Package ‘data.table’ [Электронный ресурс]. URL: https://cran.r-project.org/web/packages/data.table/ data.table.pdf (дата обращения: 25.03.2017).

3. A. Matono, S. M. Pahlevi, and I. Kojima. RDFCube: A P2P-based Three-dimensional Index for Structural Joins on Distributed Triple Stores [Электронный ресурс]. URL:

https://link.springer.com/chapter/10.1007/978-3-540-71661-7_31 (дата обращения: 25.03.2017).

4. M. Atre and J. A. Hendler. BitMat: A Main-memory Bit-Matrix of RDF Triples. In SSWS workshop at ISWC, 2009 [Электронный ресурс]. URL: http://www.cs.rpi.edu/~zaki/PaperDir/WWW10.pdf (дата обращения: 25.03.2017).

УДК 004.75

ПРОБЛЕМЫ ВНЕДРЕНИЯ ОБЛАЧНЫХ СЕРВИСОВ В КОРПОРАТИВНОЙ СТРУКТУРЕ

А. Н. Губин, А. С. Матвеев

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

В статье дается обзор по облачным информационным технологиям. Рассмотрены основные модели предоставления услуг облачных вычислений. Проводится оценка преимуществ внедрения облачных сервисов в различных корпоративных инфраструктурах. Приведены нормативные документы, регламентирующие методы и средства защиты конфиденциальной информации.

облачные сервисы, информационная инфраструктура, защита информации.

Облачные вычисления – это новый подход, позволяющий снизить сложность информационной инфраструктуры, благодаря применению широкого ряда эффективных технологий. Предприятия, используя облачные сервисы, могут получить множество преимуществ, среди которых снижение расходов, повышение качества предоставления сервиса и динамичности бизнеса. Такой подход помогает сотрудникам сосредоточиться на стратегических проектах компании, сэкономить время и средства на управлении и обслуживании собственных информационных сервисов. Все проблемы почти полностью перекладываются на провайдера услуг.

Однако решение о переносе информационной инфраструктуры в облачную среду предполагает тщательное планирование и анализ требований предприятия, оценку экономических затрат на модернизацию и обоснования целесообразности модернизации существующей корпоративной информационной модели в целом.

В настоящее время практически в любой корпоративной среде активно используются несколько сервисов: телефония, ERP и CRM-системы, электронная почта, реализуется совместный доступ к файлам и информа-

ционным системам, базам данных. Набор этих сервисов способ доступа к ним и определяет модель развертывания облачных технологий [1].

По модели развертывания облачные сервисы можно разделить на публичные, частные и гибридные. Публичные сервисы используются для обеспечения доступа к ресурсам широкого круга лиц вне корпоративной сети, они могут использоваться для подкрепления возможностей собственной инфраструктуры в ситуации пиковых нагрузок. Главным минусом публичного облака является отсутствие возможностей для контроля со стороны организации: работоспособность услуг полностью зависит от провайдера. Частные же сервисы ориентированы на использование защищенных каналов связи, они могут разграничивать доступ к ресурсам и оберегать конфиденциальную информацию [2, 3].

Также возможна классификация облачных сервисов по модели предоставления услуг: программное обеспечение как сервис (SaaS), платформа как сервис (PaaS), инфраструктура как сервис (IaaS). Использование той или иной модели традиционно зависит от размера предприятия: Модели SaaS и PaaS используются преимущественно малыми и средними организациями, где требуется организовать работу одного или нескольких приложения. Для этого могут использоваться относительно доступные и недорогие выделенные виртуальные серверы – VDS (*Virtual Dedicated Server*). В то же время IaaS используется в крупных корпорациях. Обусловлено это тем, что в крупных организациях, как правило, требуется большая гибкость инфраструктуры, возможность расширения и переноса ресурсов.

В облачных средах особенно важным качеством является управляемость. По сравнению с традиционными системами, достижение высокого уровня управляемости в облачных средах осложняется тремя факторами: ограниченным человеческим вмешательством, значительным разбросом диапазона рабочих нагрузок и разнообразием совместно используемых инфраструктур [4].

Экономическая целесообразность переноса рабочих процессов в облачную среду очень сильно зависит от используемые сервисов. Например, при использовании сервера «1С: Предприятие» выгода от его переноса в облако зависит в первую очередь от количества баз данных, их размера, а также совокупного количества пользователей. При большом количестве пользователей (от 100 сотрудников) облачный сервер «1С» обойдется в десятки раз дешевле чем организация аналогичного отказоустойчивого решения на площадке заказчика. При этом еще необходимо учесть расходы на штатного специалиста для обслуживания и настройки, стоимость лицензирования программного обеспечения, стоимость самого серверного оборудования. В облаке все затраты включены в стоимость обслуживания по модели «за пользователя в месяц». В настоящий момент существуют организации, предлагающие основной набор сервисов «1С» (Бухгалтерия,

зарплата и управление персоналом, управление торговлей) за тысячу рублей в месяц на одного пользователя. При этом обеспечивается ежедневное резервное копирование и предоставляется внушительный объем дискового пространства для каждого пользователя. При использовании же более мелких сервисов, например, облачной телефонии (виртуальной АТС) затраты и трудоемкость обслуживания также можно свести к минимуму. Однако не все руководители готовы перенести свою конфиденциальную информацию в «облако», особенно, когда речь заходит о крупных корпорациях.

Отдельно стоит рассмотреть необходимость защиты корпоративной информации. Для частных компаний основную ценность составляют коммерческая тайна и персональная информация [5, 6], а для предприятий, занимающихся государственными закупками или производством засекреченного оборудования, а также выполнением государственных оборонных заказов, вопрос защиты информации и, особенно, государственной тайны стоит намного более остро.

К органам защиты государственной тайны относится Федеральная служба по техническому и экспортному контролю (ФСТЭК), которая и осуществляет контроль за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации.

Согласно федеральному закону 149-ФЗ [7], все программное обеспечение в государственных, правоохранительных, финансовых и других структурах, обрабатывающих служебную информацию, подлежит сертификации ФСТЭК [8, 9]. Это накладывает определенные ограничения, так как не все используемые на рынке решения имеют такую сертификацию.

Сам процесс лицензирования по нормативам ФСТЭК является довольно продолжительным и затратным. Проведение таких мероприятий не могут позволить себе небольшие участники рынка или участники, заинтересованные в сиюминутной выгоде от проекта. В этой связи наиболее предпочтительным для них является выбор либо из уже сертифицированных аппаратно-программных комплексов (Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00), либо использование объектов уже аттестованной информационной инфраструктуры, таким как Центры Обработки Данных (ЦОД).

Однако, обязательной аттестации подлежат лишь объекты, предназначенные для обработки информации, содержащей сведения, составляющие государственную тайну, а также объекты, предназначенные для обработки информации ограниченного доступа (не государственной тайны), являющейся государственным информационным ресурсом. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации [10].

Такая ситуация негативно влияет на потребителей услуг ЦОД, ведь в настоящее время повсеместно используются технологии виртуализации, которые также должны быть сертифицированы. Наиболее используемые гипервизоры (*Microsoft Hyper-V* и *VMware vSphere*) уже достаточно давно имеют сертификаты ФСТЭК, но технологии виртуализации развиваются гораздо быстрее, чем происходит аттестация. Например, межсетевые экраны Cisco ASA и Juniper SRX имеют актуальные сертификаты ФСТЭК, а их аналоги на основе виртуальных машин Cisco ASA 1000V Cloud Firewall и Juniper vSRX сертификатов на данный момент не имеют. Это приводит к определенным трудностям, так как поставщики облачных услуг вынуждены отказаться от своевременной модернизации собственной инфраструктуры, чтобы не потерять возможность удовлетворять требованиям заказчиков.

Как было сказано выше, при обработке сведений, содержащих государственную тайну, предъявляются гораздо более суровые требования к информационной безопасности. Однако государственный сектор чаще опирается на собственную, некоммерческую информационную структуру, внедряя аппаратно-программные продукты российской разработки и возводя для государственных целей собственные центры обработки данных. Тем не менее, не все АПК российских разработчиков на данный момент прошли требуемую сертификацию и аттестацию, а, значит, пока не могут быть полноценной заменой зарубежному оборудованию в перспективе импортозамещения.

При планировании внедрения облачных сервисов следует учитывать множество факторов: бюджет, человеческие ресурсы, степень защищенности и расширяемость. Вложения в ИТ-инфраструктуру помимо прочего являются еще и капиталовложением, в случае использования публичного облака инвестирование с заделом на будущее просто невозможно, материальные активы не приобретаются. Для предприятий малого и среднего уровня вариант использования частных облачных сервисов становится рентабельным в большинстве случаев [дома]. При этом можно часть некритических сервисов перенести в облако, разгрузив ресурсы и персонал от выполнения рутинных задач, позволив сфокусироваться не обслуживании критически важных сервисов. В случае же возведение собственной инфраструктуры для государственных целей и предприятий затраты просто огромны: создание ЦОД категорий Tier 3 и Tier 4 согласно стандарту TIA-942 (с резервированием всех систем по схеме N+1 и 2N соответственно) и их оснащение может стоить миллионы долларов.

Список используемых источников

1. Медведев А. Облачные технологии: тенденции развития, примеры исполнения // Современные технологии автоматизации. 2013. № 2. С. 6–9.

2. Довгаль В. А. Особенности реализации безопасного подключения к облачным сервисам // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2015. Вып. 1 (154). С. 128–135.

3. Amrhein D., Quint S. Cloud computing for the enterprise: Part 1: Capturing the cloud. URL:http://www.ibm.com/developer-works/websphere/techjournal/0904_amrhein/ /0904_amrhein.html. (дата обращения 29.02.2018).

4. Никулин С. Настоящее и будущее отечественных ИКТ-технологий / CONNECT. Мир информационных технологий. 2017. № 1–2. С. 74–78.

5. Дорофеев А. В., Марков А. С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41–53.

6. Федеральный закон Российской Федерации «О персональных данных» от 27 июля 2006 года № 152-ФЗ // Собрание законодательства Российской Федерации, 2006, № 31 (1 часть), ст. 3451. 20.

7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 2006.

8. Барабанов А. В., Марков А. С., Цирлов В. Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264–270.

9. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

10. Приказ ФСТЭК от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

УДК 004.7

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ И СПОСОБЫ ВОЗДЕЙСТВИЯ НА НИХ

М. А. Гудков, М. А. Коцыняк, А. П. Нечепуренко, А. И. Суетин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматривается подход, позволяющий определить вероятностно-временные характеристики таргетированной компьютерной атаки, направленной на киберфизические системы. Для это в статье предлагается использовать метод топологического преобразования стохастических сетей и построить профильную модель таргетированной компьютерной атаки.

модель вероятностно-временные характеристики, таргетированные кибернетические атаки, метод топологического преобразования стохастических сетей.

Основной тенденцией последних лет называют смещение акцента с массовых атак на таргетированные, или целевые, которые заранее спланируют действия противник конкретной государственной или негосударственной структуры. Целевая атака всегда строится под объект воздействия, являясь продуманной операцией, а не простым техническим действием [1].

Таргетированная (целевая) кибернетическая атака (ТКА) на элемент киберфизических систем (КФС) реализуется в виде проведения комплекса мероприятий по изучению информационной системы и программного обеспечения. На основе этого выявляются слабые места в структуре КФС. Разрабатывается техника скрытого внедрения и обхода стандартных средств защиты информации, осуществляется закрепление внутри инфраструктуры, распространяется и выполняется вредоносное действие.

Таргетированная кибернетическая атака обладает вероятностно-временными характеристиками (ВВХ), определение их позволит оценить степень их опасности, выбрать и реализовать меры защиты. Для исследования и определения ВВХ ТКА необходимы модели. С этой целью предлагается использовать профильные модели ТКА и метод топологического преобразования стохастических сетей (ТПСС) [2, 3].

Сущность метода ТПСС состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации, т. е. реализации анализируемого процесса.

С целью определения ВВХ с использованием ТПСС на первом этапе необходимо произвести четкое разложение процесса функционирования на несколько физических процессов, т. е. построить профильную модель.

Профильная модель ТКА

Модель разрабатывается для условий, когда нарушитель реализует атаку в первый раз. Сеть содержит n элементов. Для выявления потенциально слабых мест осуществляется сбор информации за среднее время $\overline{t_{\text{сбор}}}$ при функции распределения времени $O(t)$ с помощью следующих приемов: социальная инженерия – прием, при котороmза среднее время $\overline{t_{\text{с.и.}}}$ с функцией распределения времени $Q(t)$; инсайд – прием, при котороmза среднее время $\overline{t_{\text{инс}}}$ с функцией распределения времени $W(t)$ от людей получают достаточно большой объем информации для подготовки и выбора вектора атаки; несанкционированный доступ коткрытым источникаминформации за среднее время $\overline{t_{\text{ист}}}$ с функцией распределения времени $R(t)$.

Затем нарушитель разрабатывает набор инструментов воздействия за среднее время $\overline{t_{\text{инст}}}$ с функцией распределения времени $A(t)$, который определяется следующим образом.

1. Набор новых инструментов за среднее время $\overline{t_{\text{нов}}}$ с функцией распределения времени $X(t)$.

2. Выбор из готовых инструментов (видов воздействия) за среднее время $\overline{t_{\text{пов}}}$ с функцией распределения времени $Y(t)$ трех компонентов: командный центр, обеспечивающий передачу команд подконтрольным, вредоносным модулям за среднее время $\overline{t_{\text{ком}}}$ с функцией распределения времени $Y1(t)$; выбор вариантов проникновения за среднее время $\overline{t_{\text{пов}}}$ с функцией распределения времени $Y2(t)$; вредоносная модель тело вируса Payload в целевой атаке за среднее время $\overline{t_{\text{загр}}}$ с функцией распределения времени $Y3(t)$ загружается на инфицированный устройство, состоящий из нескольких функциональных допмодулей.

Опираясь на собранную информацию, нарушитель приступает к созданию стенда воздействия ТКА за среднее время $\overline{t_{\text{стенд}}}$ с функцией распределения времени $U(t)$, применяя идентичные версии эксплуатируемого программного обеспечения. Отрабатываются следующие этапы: выбор способов воздействия скрытого внедрения за среднее время $\overline{t_{\text{внед}}}$ с функцией распределения времени $U1(t)$; обход стандартных средств защиты информации за среднее время $\overline{t_{\text{обход}}}$ с функцией распределения времени $U2(t)$. Далее разрабатывает стратегия воздействия за среднее время $\overline{t_{\text{страт}}}$ с функцией распределения времени $A1(t)$.

После выбора способа воздействия решается задача позволяющая осуществить обход стандартных средств защиты за среднее время $\overline{t_{\text{станд}}}$ с функцией распределения времени $I(t)$. Применяет следующие приемы: обфускация кода за среднее время $\overline{t_{\text{обфус}}}$ с функцией распределения времени $D(t)$, шифрование части кода от детектирующих механизмов за среднее время $\overline{t_{\text{шиф}}}$ с функцией распределения времени $G(t)$; инжектирование процесса динамическое внедрение собственного кода в чужой процесс за среднее время $\overline{t_{\text{инж}}}$ с функцией распределения времени $R(t)$; Mimikatz извлечение аунтификационных данных в систему пользователя в открытом виде за среднее время $\overline{t_{mim}}$ с функцией распределения времени Z(t).

Далее нарушитель приводит изменение штатной логики работы ПО, используя эксплуатационные уязвимости за среднее время $\overline{t_{\text{уязв}}}$ с функцией распределения времени $X1(t)$ по средствам внедрения кода в уже запущенную ОС или программу, с помощью: известных уязвимостей за среднее время $\overline{t_{\text{изв}}}$ с функцией распределения времени $C(t)$; неизвестных или уязвимостей нулевого за среднее время $\overline{t_{\text{неизв}}}$ с функцией распределения времени $D1(t)$. Для гарантированных воздействий применяется комбини-

рование техники атаки за среднее время $\overline{t_{\text{комб}}}$ с функцией распределения времени $B(t)$, такие как: утилиты за среднее время $\overline{t_{\text{утилит}}}$ с функцией распределения времени $N(t)$; механизмы эксплуатации уязвимостей нулевого дня за среднее время $\overline{t_{\text{экс}}}$ с функцией распределения времени $M(t)$; вредоносное программное обеспечение специально созданную под конкретную цель за среднее время $\overline{t_{\text{вред}}}$ с функцией распределения времени $O1(t)$.

После изменения штатной логики работы ПО нарушитель принимает решение по инвентаризации сети за среднее время $\overline{t_{\text{инв}}}$ с функцией распределения времени $Q1(t)$, а также осуществляет закрепление внутри инфраструктуры за среднее время $\overline{t_{\text{закр}}}$ с функцией распределения времени $W1(t)$ и распространение вредоносного модуля за среднее время $\overline{t_{\text{расп}}}$ с функцией распределения времени $A2(t)$. Закрепление осуществляется по следующим этапом: Duqu2.0 за среднее время $\overline{t_{duqu}}$ с функцией распределения времени $R2(t)$ и Carbanakза среднее время $\overline{t_{carb}}$ с функцией распределения времени $W2(t))$.

В заключении нарушитель производит поиск ключевой информациииза среднее время $\overline{t_{\text{поиск}}}$ с функцией распределения времени $C1(t)$ и выполняет вредоносное действие за среднее время $\overline{t_{\text{вред}}}$ с функцией распределения времени I1(t), такие атаки как: хищениеключевой информации за среднее время $\overline{t_{\text{хищ}}}$ с функцией распределения времени D2(t); получение информации, содержащей конфиденциальные данные за среднее время $\overline{t_{\text{получ}}}$ с функцией распределения времени $G1(t)$; изменение данных за среднее время $\overline{t_{\text{измен}}}$ с функцией распределения времени $J1(t)$.

После первой успешной реализации для уменьшения времени ТКА нарушитель оставляет файл возврата за среднее время $\overline{t_{\text{возвр}}}$ с функцией распределения времени $B2(t)$ для дальнейшей реализации атак с этапа выполнения вредоносного действия [2, 4].

Математическая модель

В результате представления анализируемого процесса в виде стохастической сети получилось сложная стохастическая сеть. Для определения ВВХ необходимо разбить её на простые сети. Каждая простая стохастическая сеть будет соответствовать каждому этапу ТКА. Порядок определения ВВХ простых сетей подробно описан в [5, 6].

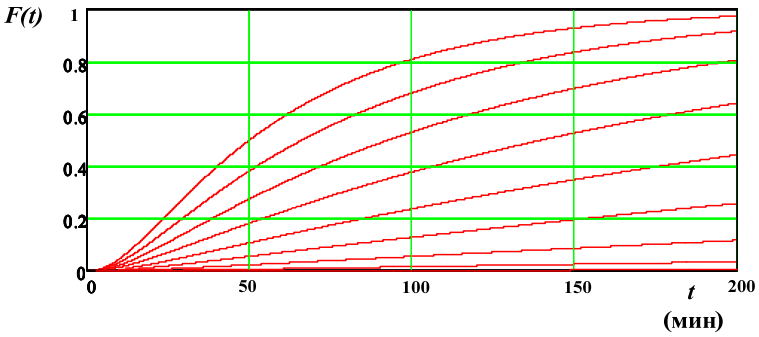
После определения ВВХ каждого этапа определяется ВВХ всей ТКА, профильная модель которой имеет следующий вид: с вероятностью P_{I} осуществляется подготовительный этап за среднее время $t_{\text{подг}}$ с функцией распределения $O(t)$; с вероятностью P_{II} осуществляется этап проникновенияза среднее время $t_{\text{проник}}$ с функцией распределения $A(t)$; с вероятностью P_{III} осуществляется этап распространения за среднее время $t_{\text{расп}}$

с функцией распределения $U(t)$; с вероятностью P_{IV} осуществляется этап достижения цели за среднее время $t_{д.ц.}$ с функцией распределения $A1(t)$. Результаты расчетов ВВХ представлены на рис. В качестве исходных данных используются следующие значения:

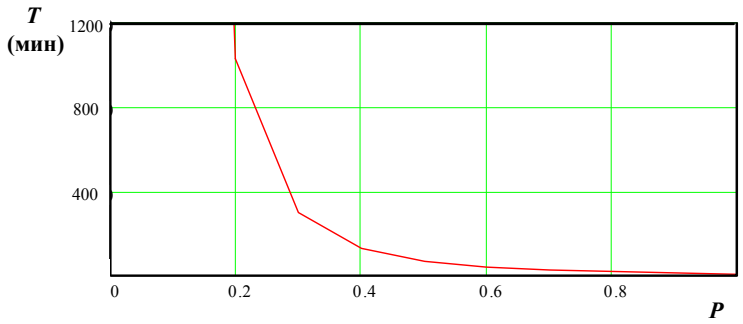
$\overline{t_{под}}$ =30 мин; $\overline{t_{проник}}$ = 48 мин; $\overline{t_{расп}}$ =8 мин; $\overline{t_{д.ц.}}$ =25 мин; $\overline{t_{пов}}$ =1 мин;

$$P_I = 0{,}1 \ldots 0{,}9;\ P_{II} = 0{,}1 \ldots 0{,}9;\ P_{III} = 0{,}1 \ldots 0{,}9;\ P_{IX} = 0{,}1 \ldots 0{,}9$$

Представление ТКА в виде профильной модели и использование метода ТПСС позволяет определить ВВХ ТКА, что, в свою очередь, позволило обосновать исходные данные для разработанной методики. Предполагаемая методика оценки устойчивости КФС позволяет оценивать устойчивость КФС в условиях информационного противоборства (в мирное время и в период непосредственной угрозы начала агрессии) при воздействии ТКА на КФС. Результаты оценки позволят обосновать требования к топологии КФС.



а)



б)

Рисунок. Вероятностно-временные характеристики реализации ТКА: а) зависимость интегральной функции распределения вероятности от времени реализации ТКА; б) зависимость среднего времени реализации ТКА

Список используемых источников

1. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-

телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. 2017. С. 420–425.

2. Баранов В. В., Гудков М. А., Крибель А. М., Лаута О. С., Нечепуренко А. П. Защита канала управления роботизированных систем // Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 32–37.

3. Баранов В. В., Иванов Д. А., Коцыняк М. А., Московченко В. М., Нечепуренко А. П. Применение метода топологического преобразования стохастической сети для моделирования системы воздействия / Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 38–43.

4. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Модель таргетированной кибернетической атаки // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х т. 2017. С. 90–98.

5. Елисеев А. И., Долгов А. А., Хорохорин М. А., Лаута О. С., Набатов К. А. Обеспечение живучести информационных систем (Часть 3. Методы обеспечения и повышения живучести) // Вестник Воронежского института ФСИН России. 2013. № 1. С. 91–94.

6. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 83–89.

УДК 004.921

РАЗРАБОТКА АЛГОРИТМА ДЛЯ ОПТИМИЗАЦИИ СИНТЕЗА ГРАФИЧЕСКИХ ЭЛЕМЕНТОВ

Е. В. Гунина, А. А. Степанов

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

Статья посвящена современной проблеме оптимизации создания графических элементов векторной графики в дизайне. Дизайнеры при создании векторных графических элементов таких, как иконки, пиктограммы, узоры и т.д. сталкиваются с невозможностью оперативно внести изменения в созданный векторный рисунок. Затронут вопрос поиска новых решений для упрощения работы с графическими элементами. Предложен вариант оптимизации с помощью разработки алгоритма в программе Симплекс.

оптимизация, графические элементы, дизайн, векторная графика, новые решения, разработка алгоритма, Симплекс, интерфейс, процесс.

В настоящее время вопросу оптимизации уделяется большое внимание во всех областях деятельности [1]. Он является одним из ключевых из года в год. При увеличении загруженности производства все задаются вопросом: «Как упростить или ускорить производственный процесс?». Ответом на этот вопрос является оптимизация. Оптимизация – это поиск наилучшего варианта для достижения максимальной эффективности какого-либо процесса [2].

Вопрос оптимизации актуален и для дизайна, в частности для создания и работы с элементами векторной графики. Очень часто дизайнеры при создании векторных графических элементов таких, как иконки, пиктограммы, узоры и т. д. сталкиваются с невозможностью оперативно внести изменения в созданный векторный рисунок [3]. И порой, чтобы изменить часть, приходится перерисовывать не только отдельные элементы-узоры, но и все изображение целиком. Такая работа затрачивает много сил и времени. Чтобы решить данную проблему нужно найти способ для оптимизации процесса создания и изменения векторных графических элементов.

Для решения проблемы оптимизации предложен вариант по созданию алгоритма в системе Симплекс.

Система Симплекс является инструментальным средством для автоматизации решения задач конструктивного геометрического моделирования, также позволяет автоматизировать выполнение многих графических операций, которые трудно или почти невозможно выполнить в векторных графических редакторах таких, как Adobe Illustrator, CorelDRAW и Inkscape [4].

Для создания алгоритма и его вывода необходимо построить основу будущего рисунка и указать опорные точки. Последовательность действий показана на рис. 1–4.

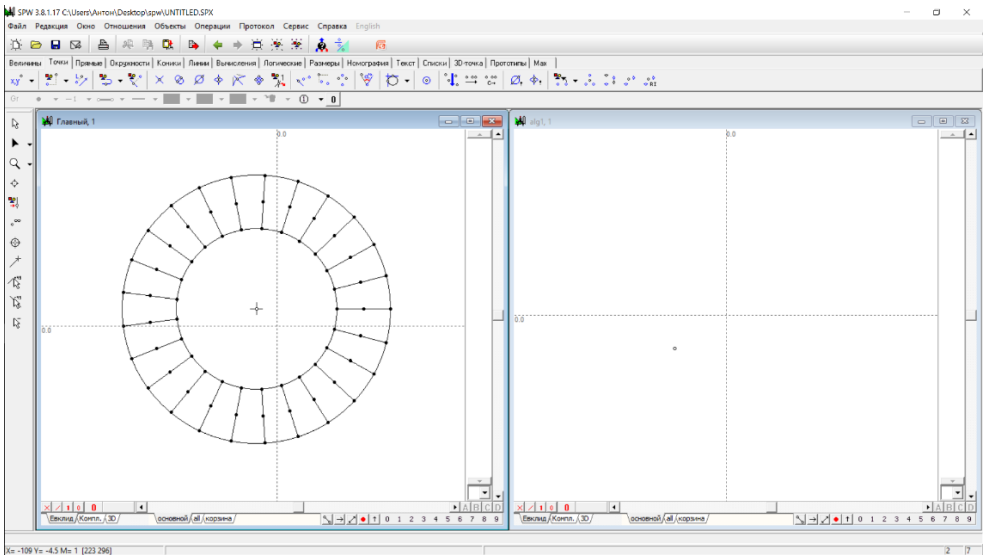


Рис. 1. Создание основы для рисунка

На рис. 1 изображена основа будущего рисунка. Справой стороны открыто окно, в котором создаем алгоритм для узора.

Созданный алгоритм будет представлять собой некий узор, который представлен на рис. 2 справа. В левом окне можно увидеть раскрытую структуру алгоритма.

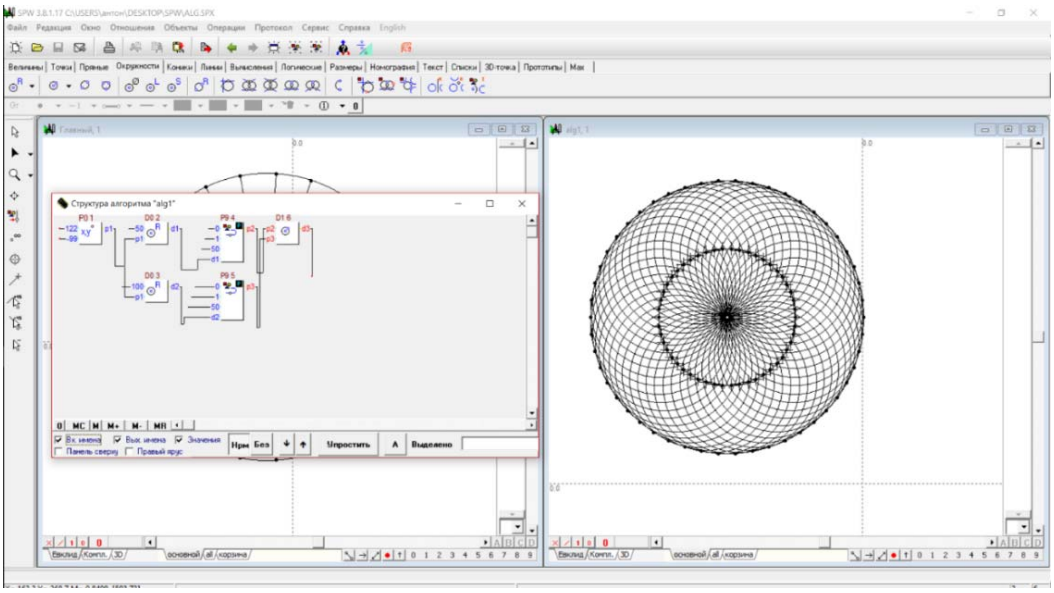


Рис. 2. Структура алгоритма

Используя опорные точки рисунка выводим алгоритм. Полученный результат виден на рис. 3.

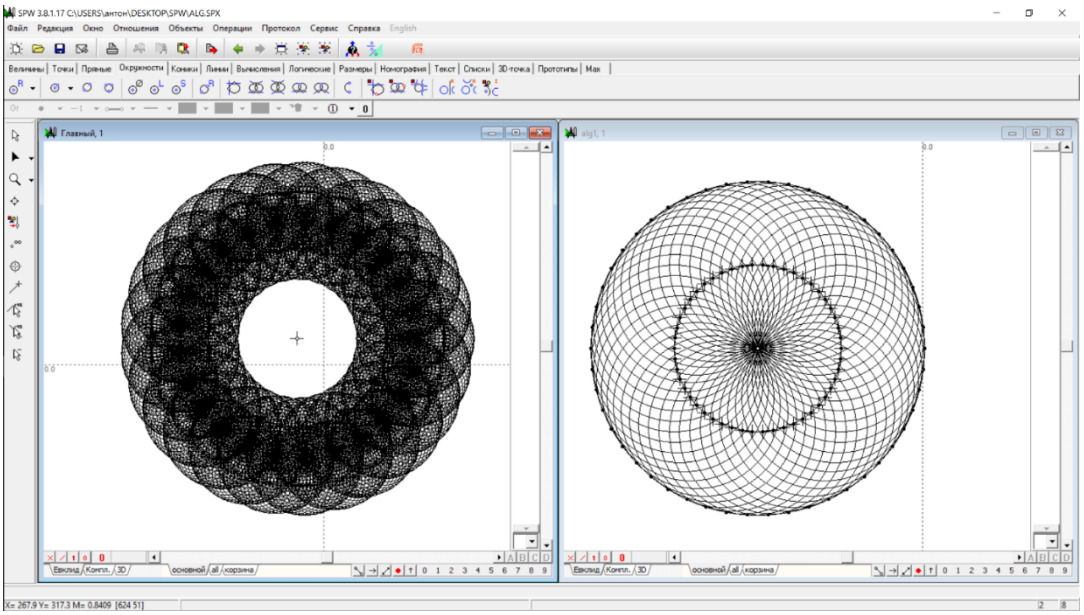


Рис. 3. Вывод алгоритма

Сделав небольшие изменения в алгоритме расположенного в правой части рабочего окна получаем измененный узор. Результат изменений показан на рис. 4.

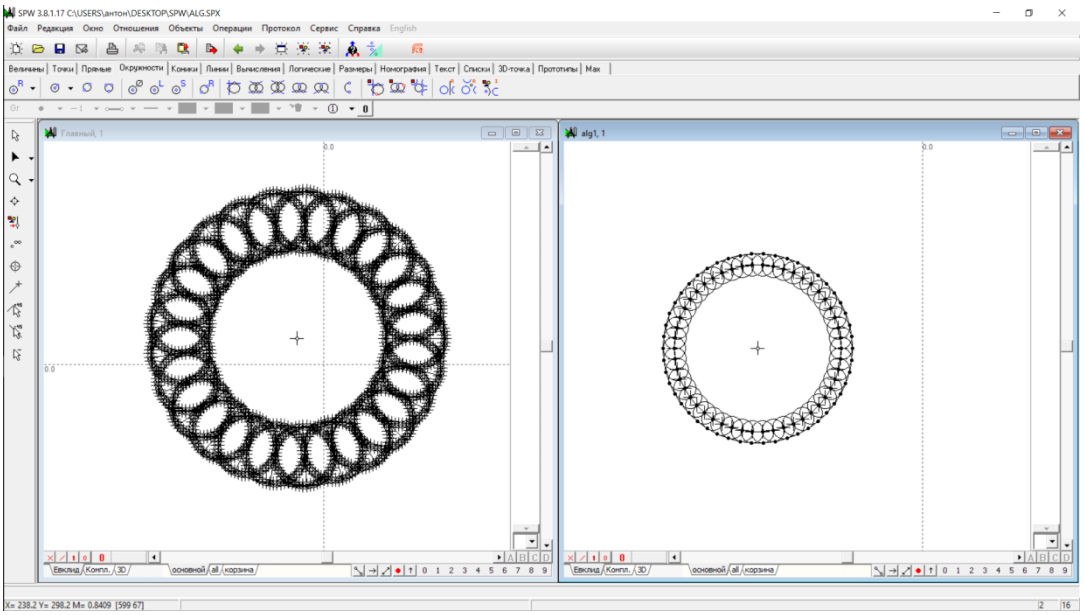


Рис. 4. Результат изменений алгоритма узора

Симплекс позволяет создать алгоритм любого узора и элемента, который может быть частью или основой для векторного изображения. Получившийся алгоритм можно изменять и моментально менять узор рисунка, при этом ненужно перерисовывать что-то заново, достаточно внести соответствующие изменения в алгоритм. Работа с алгоритмом значительно снижает временные затраты на любые действия с графическими элементами.

Список используемых источников

1. Колоколов А. А., Артемова А. В. Проектирование сложных изделий на основе моделей и алгоритмов дискретной оптимизации // Омский научный вестник. 2016. № 5. С. 131–135.

2. Оптимизация [Электронный ресурс] // Википедия. URL: https://ru.wikipedia.org/wiki/Оптимизация (дата обращения 16.01.2018).

3. Калимуллина О. В., Курбанова Е. С. Правила разработки пользовательского графического интерфейса в сфере информационных технологий [Электронный ресурс] // NovaInfo. Технические науки. 2016. № 42-1. Режим доступа: https://novainfo.ru/article/4645 (дата обращения 17.01.2018).

4. Волошинов Д. В. Основные сведения о системе Симплекс и ее интерфейс [Электронный ресурс]. URL: http://dww.no-ip.org/simplex/INTERFACE/index.htm (дата обращения 17.01.2018).

УДК 004.921

МЕТОДЫ АВТОМАТИЗАЦИИ СИНТЕЗА МОДУЛЬНОЙ СЕТКИ ДЛЯ ДИЗАЙН-ПРОЕКТИРОВАНИЯ

Е. В. Гунина, С. В. Яковлев

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

В статье рассматриваются вопросы автоматизации процессов создания модульных сеток. Описаны некоторые возможные способы создания сеток с использованием различного программного обеспечения и систем автоматизаций труда дизайнеров, представленные на рынке и имеющие положительный опыт использования в среде специалистов отрасли. Представлен вариант проектирования, при котором с помощью заданного алгоритма процесс создания и редактирования сетки становится динамическим и способным порождать многовариантные решения.

дизайн, модуль, модульная сетка, алгоритм, автоматизация, программное обеспечение.

На протяжении многих лет, дизайнеры используют модульную сетку как невидимый каркас, состоящий из системы вертикалей и горизонталей, а то и диагоналей, при составлении различных планов строительства, конструировании многополосных изданий и журналов, построении логотипов, верстке веб-страниц и т. д. Сетка стала неотъемлемой частью работы дизайнера. В графическом дизайне сетка сродни магии – то видима, то невидима, но, как правило, сетку, кроме дизайнера, больше никто не видит.

У сетки множество преимуществ, вот некоторые из них:

1) Сетка задает стандарт расположения элементов: это облегчает выравнивание элементов, добавление новых и поддержку страницы в дальнейшем.

2) Сетка позволяет работать быстрее.

3) Сетка снижает вероятность ошибок при переносе элементов с одной страницы на другую, помогает странице выглядеть более эстетично за счет того, что элементы пропорциональны и структурированы. Также сетка помогает пользователю быстрее считывать информацию.

4) Сетка создает визуальный порядок, и ориентироваться становится легче [1].

В настоящем времени дизайнеры используют множество различных программных обеспечений для создания модульных сеток, такие как Adobe «Photoshop», Adobe «Illustrator», «CorelDraw» и т. д. В качестве примера создания модульной сетки в одной этих программ, можно привести сетку,

созданную в программном обеспечении от компании Adobe – «Illustrator» (рис. 1).

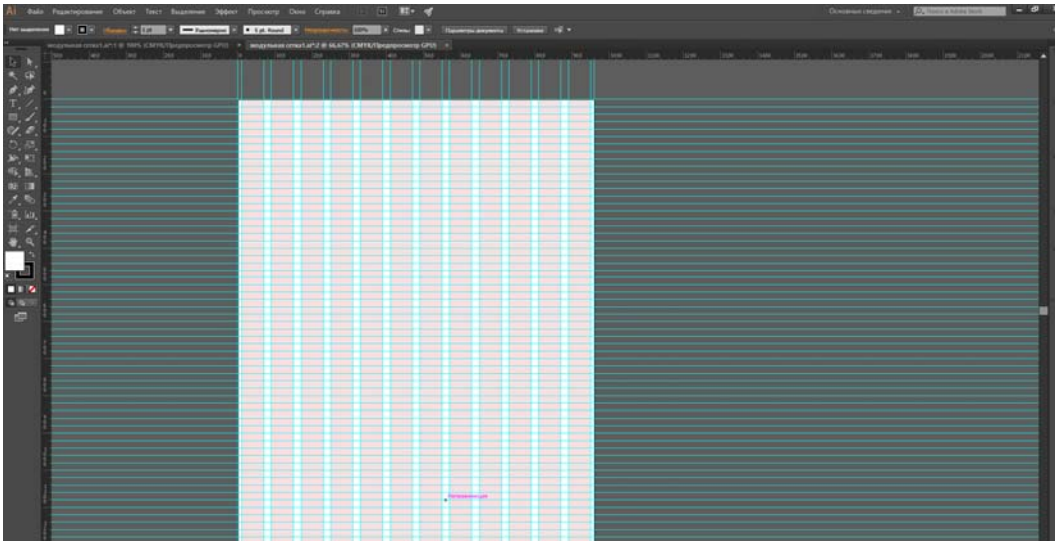


Рис. 1. Пример модульной сетки в Adobe «Illustrator»

Создание такой сетки занимает немало времени. И если нужно что-то поменять, придется потратить время на переделывание вручную.

Плагин «GuideGuide» позволяет за несколько щелчков мышью построить горизонтальную и вертикальную сетки с требуемым количеством колонок и расстоянием между ними, а также устанавливать границы и центральные точки для документа или выделенной области (рис. 2). Плагин работает с Adobe «Photoshop» начиная с версии CS4 и выше [2].

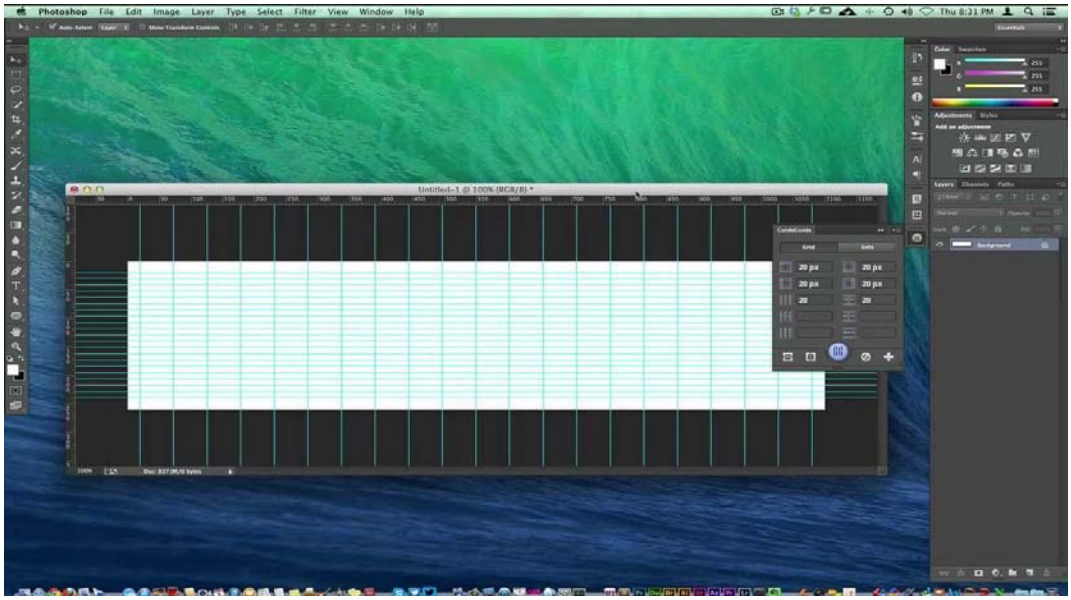


Рис. 2. Пример модульной сетки в плагине GuideGuide для Adobe «Photoshop»

«Modular Grid Pattern» (рис. 3) – это веб-приложение для веб-дизайнеров, которое поможет быстро и легко создать модульную сетку в Adobe «Photoshop», Adobe «Fireworks», «GIMP», «Microsoft» Expression Design и др. [2]

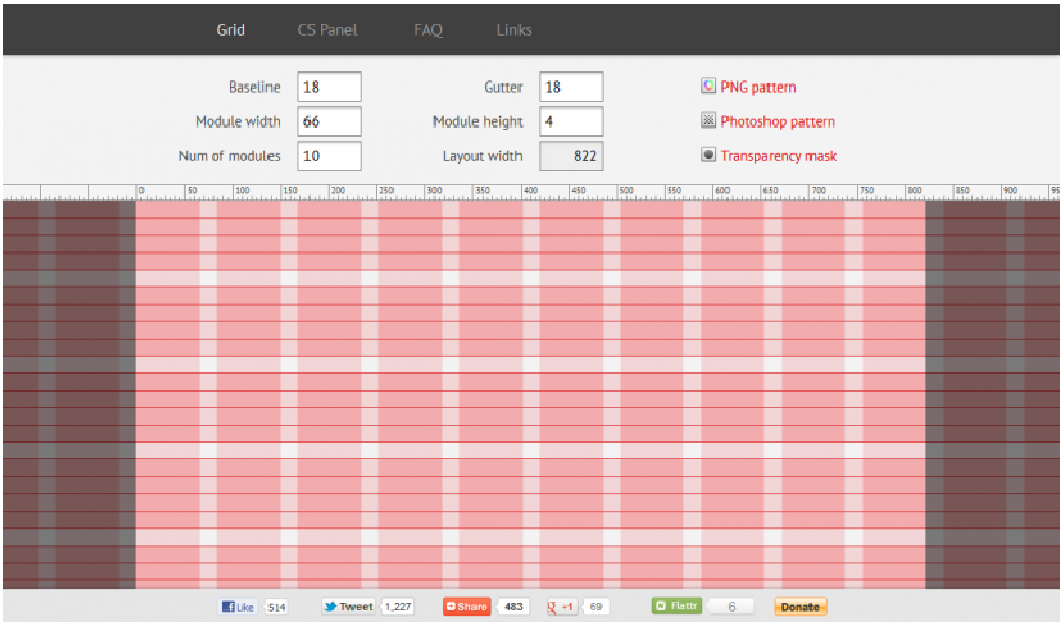


Рис. 3. Пример модульной сетки в веб-приложении «Modular Grid Pattern»

Разнообразие программных методов построения модульных сеток и различных интернет ресурсов, позволяют создать сетку за несколько кликов мышью, но им не всегда хватает необходимого инструментария для ускорения процесса создания. Существует еще один способ автоматизирования процесса построения различных сеток с помощью заданных алгоритмов: программное обеспечение Симплекс, за авторством Волошинова Д. В., доктора технических наук, профессора, заведующего кафедрой информатики и компьютерного дизайна Санкт-Петербургского Государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.

С помощью его программного обеспечения, на примере следующей задачи предоставляется возможность создания сетки с различными модулями и изменение их в реальном времени (рис. 4–6) [3].

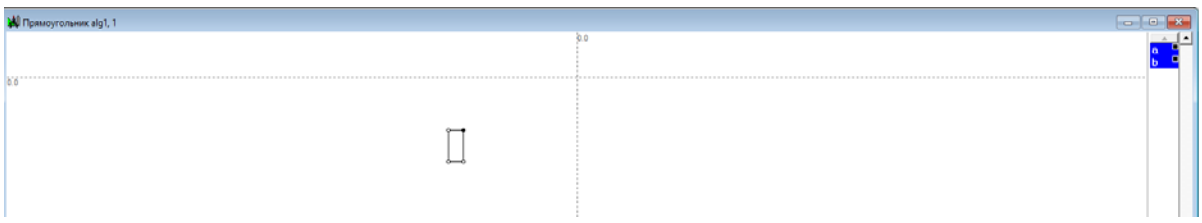


Рис. 4. Модуль «Прямоугольник»

Сначала необходимо задать алгоритм, в данном случае модулем будет простой прямоугольник.

Далее мы создаем кривую Безье и делим ее, например, на 12 точек. Привязываем к каждой точке наш заданный алгоритм и получаем сетку.

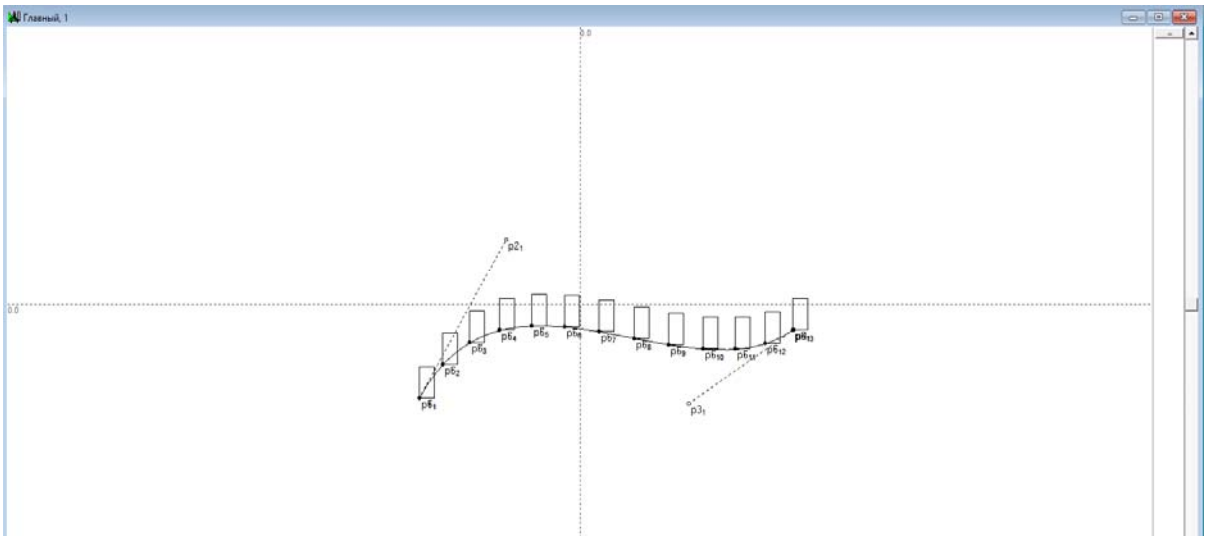


Рис. 5. Вариант сетки с использованием кривой Безье и заданным алгоритмом в виде модуля «Прямоугольник»

Альтернативный вариант сетки с заданным ранее алгоритмом, привязанный к 2-ум горизонтальным прямым.

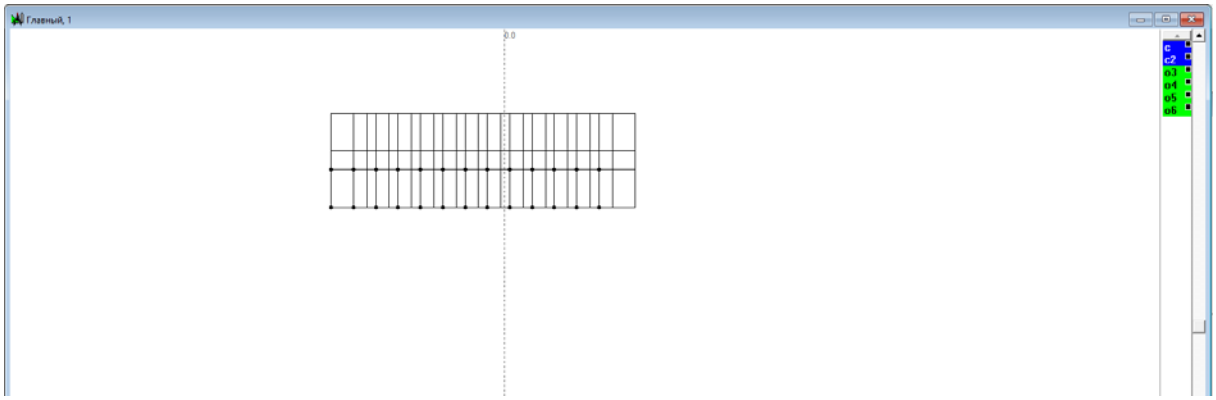


Рис. 6. Вариант сетки с использованием 2-ух горизонтальных прямых и заданным алгоритмом в виде модуля «Прямоугольник»

Еще один пример, но уже с использованием 4-х вертикальных прямых и алгоритма в виде модуля «Квадрат» (рис. 7).

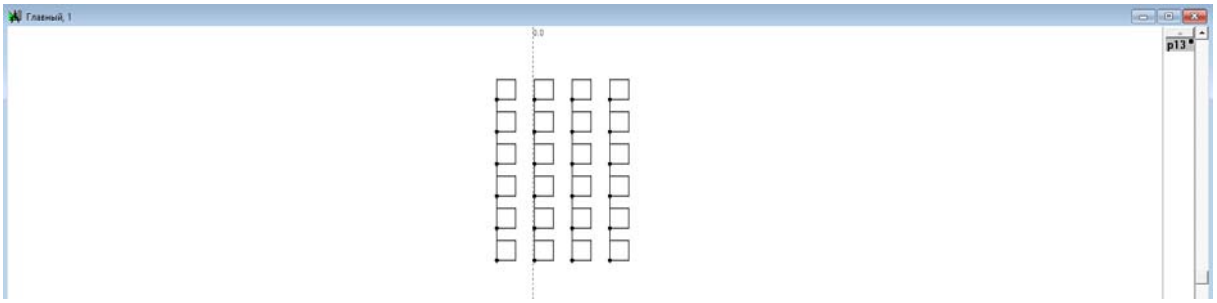


Рис. 7. Вариант сетки с использованием 4-х вертикальных прямых и заданным алгоритмом в виде модуля «Квадрат»

Инструментарий Симплекса предоставляет возможность генерировать бесчисленное количество вариантов всевозможных алгоритмов и позволяет автоматизировать процесс создания модульных сеток.

Список используемых источников

1. Обухов Н. В. Дизайн в цифровой среде [Электронный ресурс]. URL: http://tilda.education/courses/web-design/grid/

2. Модульная сетка в дизайне [Электронный ресурс] // Habr. URL: https://habrahabr.ru/sandbox/34277/

3. Волошинов Д. В. «Справочная информация о системе геометрического моделирования Симплекс» [Электронный ресурс]. URL: http://dww.no-ip.org/SIMPLEX/CONTENTS/index.htm

УДК 004.621.398

СПОСОБ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТЬЮ С РАСПОЗНАВАНИЕМ ВТОРЖЕНИЙ И АНАЛИЗОМ ДИНАМИКИ ДЕЙСТВИЙ НАРУШИТЕЛЯ

С. С. Гурьянов, В. А. Липатников, А. А. Литвинов, А. О. Сазонов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Способ управления информационно-вычислительной сетью с распознаванием вторжений и анализом динамики действий нарушителя на основе древовидного классификатора и карт Кохонена. Функции алгоритма управления: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в информационно-вычислительную сеть и выделенный сервер, распознавание вторжения, выбор и реализация способа защиты.

информационно-вычислительная сеть, защита информации; древовидный классификатор и карта Кохонена.

В связи с беспрецедентно быстрым развитием компьютерных технологий, в том числе появлением сети Интернет, объединяющей огромное количество разнородных сетей, и переходом к информационному обществу проблема обеспечения информационной безопасности (ИБ) и построения распределенных вычислительных систем стала одной из наиболее актуальных проблем [1]. В [1, 2] рассматривается подход к разработке и использованию систем информационной безопасности (ИБ), основанный на выделении интеллектуальной надстройки над традиционными способами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Представляются отдельные способы управления ИБ. Предложен способ управления безопасностью информационно-вычислительных сетей на основе выделенного сервера (ВС) с контейнерной виртуализацией (КВ). Не в полной мере рассмотрены вопросы распознавания вторжений и прогнозирования состояния защиты информационно-вычислительной сети (ИВС) системы распределенных ситуационных центров. Средства проактивной защиты должны обеспечивать сбор необходимой информации, анализ защищенности, мониторинг состояния сети, обнаружение атак, прогнозирование, противодействие их реализации, введение злоумышленника в заблуждение [3]. Однако, задача уточнения классификации при распознавании вторжений в интеллектуальных способах управления ИБ системы распределенных ситуационных центров остается актуальной. При исследовании проактивной защиты недостаточно внимания уделено анализу динамики действий нарушителя, которые включают сценарии внешних и внутренних вторжений. Основным требованием, предъявляемым к таким системам, является способность находить аномалии и, соответственно, вторжения в реальном времени. Возникает противоречие между эффективными новыми средствами информационного вторжения и существующими способами защиты ИВС. Задача защиты ИВС от вторжений со стороны внешних и внутренних нарушителей актуальна. Цель – повышение ИБ ИВС за счет анализа динамики действий нарушителя.

Постановка задачи. Разработать способ управления ИВС с распознаванием вторжений и прогнозированием состояния ИБ при выявлении угроз вторжений с помощью математических алгоритмов, разработанных на основе древовидного классификатора и карт Кохонена. Способ должен содержать: мониторинг обстановки, оперативный контроль, распознавание последовательности действий нарушителя, моделирование стратегии воздействия нарушителя, процесс определения ситуационных параметров во взаимной противоборствующей обстановке с достоверным прогнозом

стратегии компьютерных атак (КА). Для решения задач защиты и мониторинга ИВС необходимо не только обнаруживать и блокировать действия нарушителей, но также и анализировать КА и отвлекать нарушителей от информационных систем, путем заманивая нарушителей на ложные информационные системы и производить сбор информации о тактике нарушителей, осуществлять идентификацию и разоблачение. На основании анализа деятельности нарушителя определяются слабые стороны системы защиты информации в ИВС. Суть идеи заключается в определении угроз вторжений и определении состояния ИБ с помощью математических алгоритмов, разработанных на основе древовидного классификатора и карт Кохонена для повышения вероятности защищенности ИВС. Определение угроз вторжений и определение состояния ИБ ИВС с помощью математических алгоритмов, разработанных на основе древовидного классификатора и карт Кохонена.

Функции алгоритма управления ИВС: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в ИВС и ВС, распознавание вторжения, выбор и реализация способа защиты (рис. 1).

Рис. 1. Структурная схема ИВС с агентами распознавания вторжений

Алгоритм реализует:

1) анализ текущей ситуации на основе данных ВС с контейнерной виртуализацией;

2) кластеризацию значений параметров;

3) обработку полученных значений;

4) формирование прогноза на основе выходных значений сети;

5) фильтрацию полученных значений и выделение целевого класса, определяющего прогнозируемое состояние ИБ ИВС.

Методы и алгоритмы обнаружения аномалий трафика в ИВС играют ключевую роль в создании систем обнаружения и предотвращения вторжений вредоносных программ в современных коммуникационных инфраструктурах. Сложность этой проблемы во многом обусловлена неполнотой, несоответствием и разнообразием законов распределения в потоках трафика. Возможными сценариями, обнаруживаемыми агентной системой обнаружения вторжений (АСОВ), являются:

1) мониторинг и контроль атакующего (действия по определению конфигурации сети, обнаружению хостов, функционирующих на хосте сервисов, определению операционной системы, приложений);

2) внедрение в систему – действия злоумышленника по взлому хоста и внедрению в систему;

3) повышение прав – попытки вторжения, направленные на получение повышенных прав по доступу к объектам хоста;

4) распространение поражения на хосте – нелегитимное распространение злоумышленника по объектам хоста (каталогам, файлам, программам);

5) распространение поражения по сети – распространение атакующего по защищаемой ИВС.

Алгоритм процесса интеллектуальной АСОВ реализует (рис. 2) [4]:

1. Сбор данные об атаке злоумышленника.

2. Получение из базы КА, обученных системой заранее для дальнейшего сопоставления с вторжений злоумышленника.

3. Предварительную классификацию вторжений на основе карты Кохонена. Данный способ универсален и зависит лишь от структуры входных данных.

4. Сопоставление образа вторжения с известными атаками и оценка уровня ИБ.

5. Условие проверки наличия алгоритма вторжения в базе данных агента.

Выводы. Представлен новый способ обнаружения аномалий трафика с распознаванием вторжений и анализом динамики действий нарушителя в ИВС. Он основан на использовании модифицированных адаптационных алгоритмов. Предложена структурная схема ИВС с ВС и агентами распо-

знавания вторжений, а также прогнозирования состояния ИБ. Разработан алгоритм управления ИВС с распознаванием вторжений и принятия решений при интеллектуальных процессах защиты, а также алгоритм процесса АСОВ (см. рис. 3 ниже).

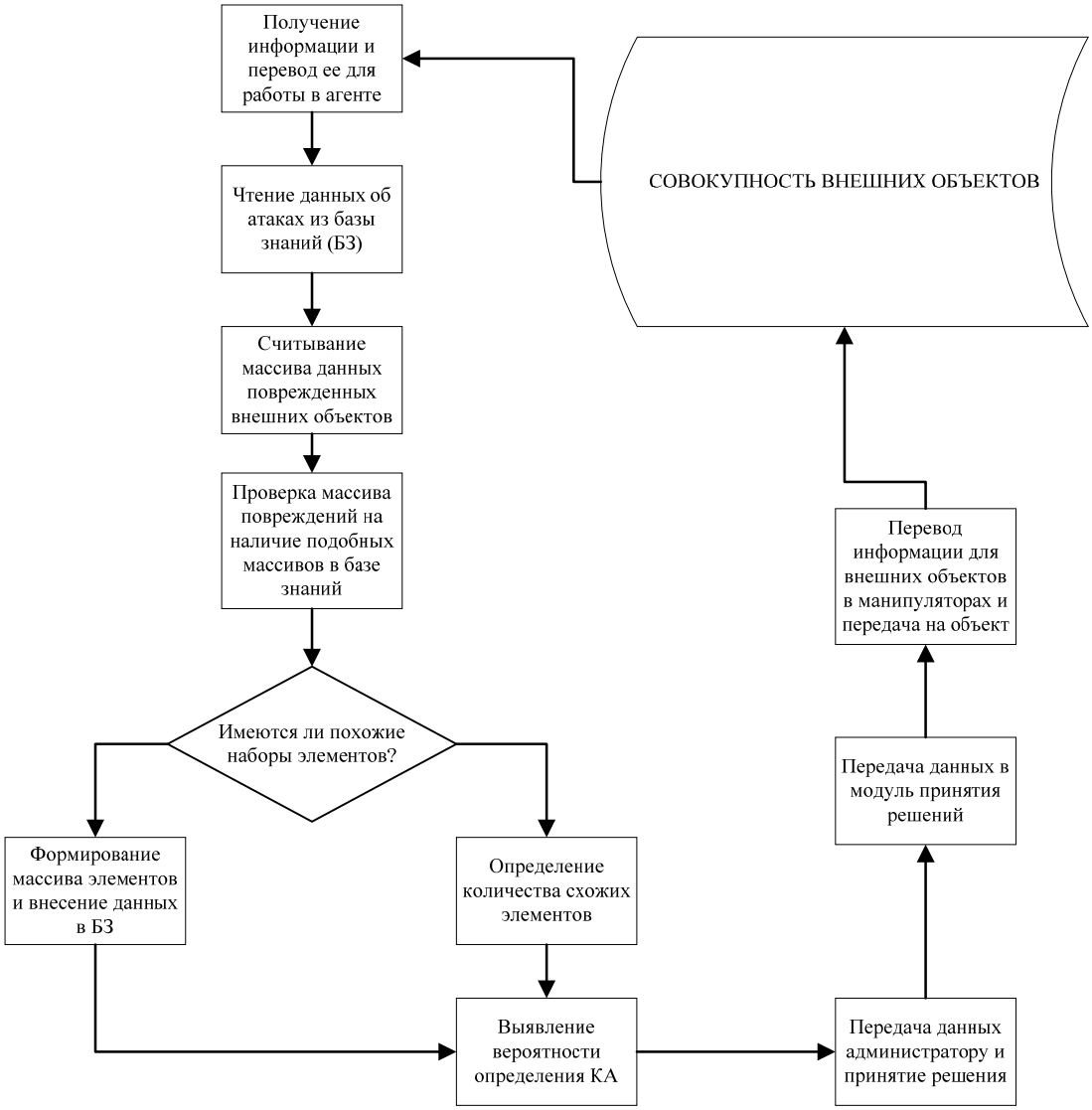


Рис. 2. Алгоритм процесса агенторaспознавания вторжений

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности. Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург, 2012. 396 с.

2. 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.

3. 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.

4. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2 (94). С. 128–140.

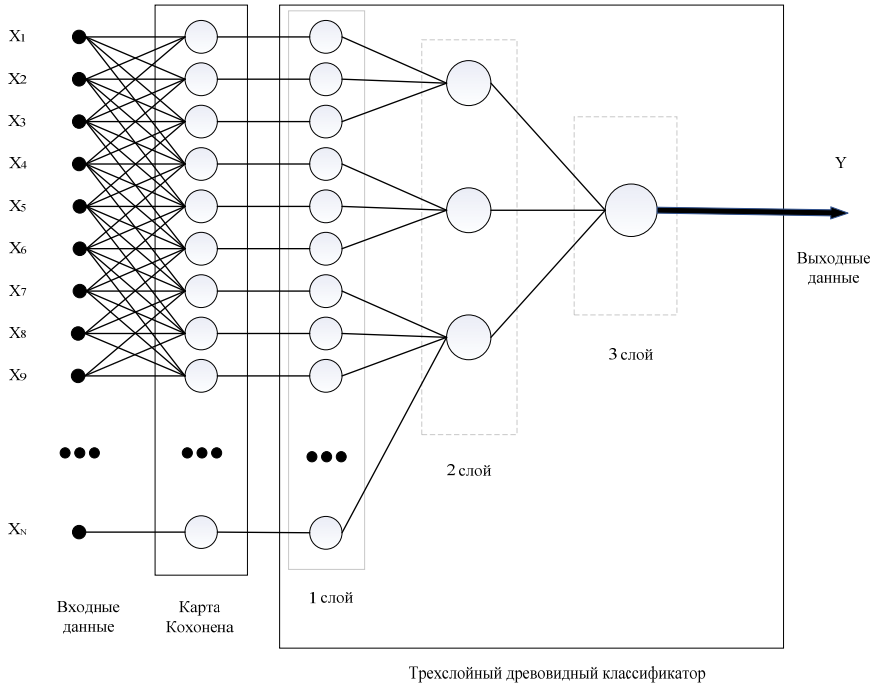


Рис. 3. Обобщенная схема модели обнаружения аномальных отклонений

УДК 004.7:004.422.8

ОПРЕДЕЛЕНИЕ ВРЕМЕННОГО ПРОФИЛЯ КРИТИЧЕСКИХ СИТУАЦИЙ В МУЛЬТИАГЕНТНОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Д. С. Гусев, Л. К. Птицына

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

Рассмотрены причины востребованности мультиагентных систем защиты информации в распределённых инфраструктурах. Описаны способы определения критических ситуаций в мультиагентной системе защиты информации. Представлен обобщённый класс моделей мультиагентной системы. Приведены методы определения временного профиля критических ситуаций в мультиагентной системе защиты ин-

формации. Показаны приёмы наращивания вариаций в определении временного профиля критических ситуаций. Предложены способы их инвариантного определения.

информационная безопасность, система защиты информации, мультиагентная система защиты, угрозы информационной безопасности.

В последние годы четко прослеживается тенденция разработки новых технологий в сфере информационной безопасности. Технологический базис подкрепляется формированием новых методологий объединения и интеграции крупномасштабных вычислительных сетей, ростом объемов циркулирующей в информационном пространстве информации, расширением и унификацией существующих архитектур разработки и управления системами защиты.

Увеличение объемов профессиональной деятельности, выполняемой в среде информационной инфраструктуры, приводит к расширению пространства полей возможных угроз и повышению степени априорной неопределенности относительно их описания и последствий воздействия на результаты труда.

Условия развития информационных систем, сформировавшиеся в сложившихся реалиях, обуславливают планомерное развитие научного пространства в сфере мультиагентных систем защиты информации.

В [1] представлены основные угрозы информационной безопасности для мультиагентных систем. Для решения задач информационной безопасности мультиагентной системы предлагается воспользоваться следующими методами: метод защищенных состояний агентов; метод мобильной криптографии; модель безопасности Ксюдонга; товарищеская модель взаимной безопасности; методы организации систем самоорганизующихся доверительных отношений; методы, основанные на использовании алгоритмов конфиденциальной связи.

Однако, несмотря на существование обширного множества известных методов, ни один из них не обеспечивает комплексного решения проблем информационной безопасности. Выше представленные методы могут быть дополнены новыми за счет отображения знаний о результатах исследований в области информационной безопасности.

В [2] представлен обобщенный класс моделей мультиагентной системы. Согласно изложенному, традиционно выделяются три базовых класса архитектур агентных систем и соответствующих им моделей интеллектуальных агентов, а именно: делиберативные архитектуры и модели, реактивные архитектуры и модели, гибридные архитектуры и модели.

Делиберативную архитектуру описывают как архитектуру агентов, содержащих точную символическую модель мира и принимающих решения на основе логического вывода.

Реактивные архитектуры обязаны своему возникновению поискам путей разрешения проблем, возникающих при использовании классических методов искусственного интеллекта. Реактивность обеспечивает функционирование мультиагентной системы, адекватное обнаруживаемым изменениям в окружающей среде.

Помимо описанных моделей, существуют решения, представляющие синтез из нескольких моделей. Гибридные решения труднее в реализации, но позволяют нивелировать недостатки каждой отдельно взятой модели.

Динамичное развитие технологий и методологий в информационных системах позволяет обеспечить плавный переход от концепции обнаружения атак к концепции обнаружения угроз информационной безопасности. Концепция подразумевает определение новых требований и принципов конструирования систем обнаружения атак, ориентированных на комплексную обработку информации о защищаемой инфраструктуре для своевременного выявления и предупреждения о возможности реализации угроз, присущих информационной системе.

Основополагающую роль в определении временного профиля критических ситуаций отводят системам обнаружения угроз информационной безопасности. Существующие технологии предписывают разделение систем обнаружения на системы обнаружения злоумышленного поведения и системы обнаружения аномального поведения. Совместная работа предложенных систем охватывает полностью поток событий, происходящих в системе. Сочетание технологических решений по обнаружению угроз информационной безопасности отражено на рис.

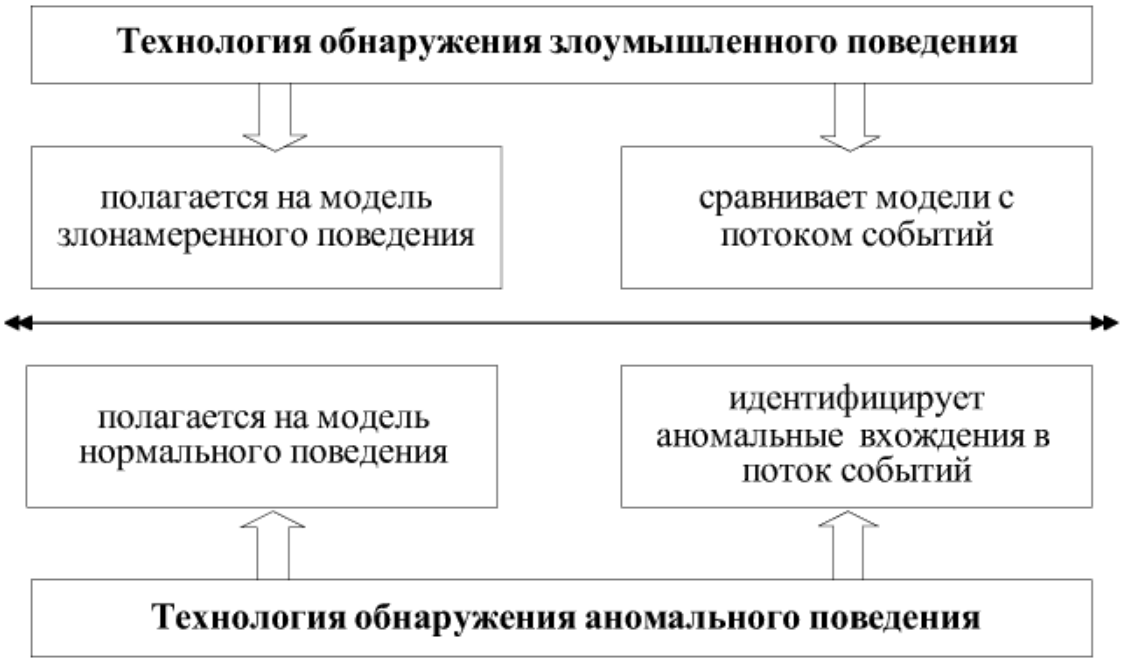


Рисунок. Сочетание технологий для обнаружения угроз информационной безопасности

Использование технологий систем обнаружения подразумевает ориентацию на реактивную среду при выполнении поставленных задач информационной безопасности.

Формирование описаний и анализ реактивных действий в информационном пространстве мультиагентных технологий представлены в работе [3]. Предлагаемая в работе [3] методологическая основа представляет собой базис методов и моделей для формирования модельно-аналитического интеллекта, включаемого в архитектуру интеллектуального информационного агента.

Методология моделирования описывается кортежем:

$$\mathbf{M} = \langle \mathbf{M}_M, \mathbf{M}_A, \mathbf{M}_V \rangle,$$

где $\mathbf{M}_M$ – методика построения расширенной объектно-ориентированной модели системы действий информационного агента; $\mathbf{M}_A$ – методы аналитического определения показателей качества функционирования интеллектуальных информационных агентов; $\mathbf{M}_V$ – методы верификации образуемого модельно-аналитического интеллекта.

Ключевой особенностью методологической основы из [3] является расширение методологии формирования модельно-аналитического интеллекта информационных агентов для реактивных сред.

В контексте сочетания технологий для обнаружения угроз информационной безопасности предлагается расширенная методологическая основа моделирования, которая характеризуется следующими компонентами описания:

$$\mathbf{M} = \langle \mathbf{M}_{MT}, \mathbf{M}_I, \mathbf{M}_{MF}, \mathbf{M}_{AT}, \mathbf{M}_{AF}, \mathbf{M}_{VT}, \mathbf{M}_{VF}, \mathbf{A}_{TF} \rangle,$$

где $\mathbf{M}_{MT}$ – методика построения расширенной объектно-ориентированной модели системы действий информационного агента при нормальном поведении; $\mathbf{M}_{AT}$ – методы аналитического определения показателей качества функционирования интеллектуальных информационных агентов при нормальном поведении; $\mathbf{M}_{VT}$ – методы верификации образуемого модельно-аналитического интеллекта при нормальном поведении; $\mathbf{M}_{MF}$ – методика построения расширенной объектно-ориентированной модели системы действий информационного агента при злонамеренном поведении; $\mathbf{M}_{AF}$ – методы аналитического определения показателей качества функционирования интеллектуальных информационных агентов при злонамеренном поведении; $\mathbf{M}_{VF}$ – методы верификации образуемого модельно-аналитического интеллекта при злонамеренном поведении; $\mathbf{M}_I$ – методика построения расширенной объектно-ориентированной модели злонамеренного поведения; $\mathbf{A}_{TF}$ – методика определения временного профиля критических ситуаций и обнаружения угрозы информационной безопасности.

Проблема существующих систем классификаций в определении критических ситуаций заключается в том, что со временем появляются новые угрозы безопасности, что приводит к снижению эффективности комплексных систем защиты информации. Помимо прочего, новые угрозы могут не попадать под описание ни одной из существующих классификаций.

Основная идея предлагаемой концепции наращивания вариаций в определении временного профиля критических ситуаций заключается в формировании онтологического подхода к классификации представленных методов, архитектур и систем.

Понятие онтологического подхода подробно описано в работе [4]. Основным преимуществом использования онтологий является возможность перехода от управления данными, которые характеризуют количественную сторону информации, к управлению знаниями, как качественной составляющей этих процессов.

При онтологическом подходе формируется общая схема отношений в семантической модели предметной области.

Формирование обобщенной схемы связи классифицируемых элементов позволит генерировать новые методы определения временного профиля критических ситуаций в мультиагентных системах защиты информации. Эффективность сгенерированных методов обусловлена эффективностью онтологического подхода.

Реализация изложенной концепции может осуществляться на множестве альтернативных архитектур мультиагентных систем защиты информации.

Список используемых источников

1. Маслобоев А. В., Путилов В. А. Разработка и реализация механизмов управления информационной безопасностью мобильных агентов в распределенных мультиагентных информационных системах // Вестник МГТУ. 2010. Т. 13, № 4/2. С. 1015–1032.

2. Антамошкин О. А., Кукарцев В. В. Обобщенная модель агента распределенной мультиагентной системы поддержки принятия решений // Информационные технологии и математическое моделирование в экономике, технике, экологии, образовании, педагогике и торговле. 2016. № 8. С. 5–54.

3. Птицына Л. К., Лебедева А. А., Белов М. П. Метод анализа реактивных действий информационного агента при воздействии инфокоммуникационной среды // Международная конференция по мягким вычислениям и измерениям. 2017. № 1. С. 155–158.

4. Щеглов С. Н. Онтологический подход и его использование в системах представления знаний // Известия ЮФУ. Технические науки. 2009. № 4. С. 146–153.

УДК 004.031

ОСОБЕННОСТИ ХРАНЕНИЯ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ БАНКА

Е. В. Давыдова, К. С. Макарова

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

Рассмотрены программно-аппаратные компоненты, обеспечивающие бизнес-процессы в банковской сфере. Проанализированы вопросы обеспечения сохранности и безопасности персональных данных клиентов частных банков. Проведен анализ возможностей применения системы «КриптоПро» для их защиты. Представлены требования к технической и технологической составляющим приема и обработки данных с учетом обеспечения их сохранности и безопасности.

клиент, информация, защита, частный клиент/корпоративный клиент, бизнес-процесс, сохранность персональных данных, «КриптоПро», банковская тайна.

Для осуществления банковских операций и иной деятельности, предусмотренной Уставом Банка, действующим законодательством РФ, нормативными актами Банка России, оператором осуществляется обработка персональных данных клиента.

В соответствии Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) «О персональных данных», персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). Субъект персональных данных – физическое лицо, являющееся клиентом Банка (Частный Клиент), либо представляющее интересы клиента Банка – юридического лица (представитель Корпоративного Клиента).

Установлены три органа государственной власти, уполномоченных осуществлять мероприятия по контролю и надзору в отношении операторов, осуществляющих обработку персональных данных [1]. Роскомнадзор является уполномоченным органом по защите прав Субъектов персональных данных, осуществляет контроль и надзор за соответствием обработки персональных данных требованиям ФЗ № 152-ФЗ. Контроль и надзор за выполнение требований к обеспечению персональных данных при их обработке, требований к материальным носителям биометрических данных и технологиям хранения таких данных осуществляют: ФСБ России (требования в области криптографии) и ФСТЭК России (требования по защите информации от несанкционированного доступа и требования от утечки по техническим каналам).

Общая схема взаимодействия представлена на рис. 1.

Рис. 1. Общая схема взаимодействия

Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В связи с этим возникает необходимость использования различных программно-аппаратных решений, обеспечивающих надежное хранение и защиту персональных данных клиентов.

Одним из таких решений являются средства криптографической защиты информации (СКЗИ) – это программное обеспечение или программно-аппаратный комплекс, с помощью которых происходит шифрование данных и передача их по сети Интернет.

СКЗИ обеспечивает выполнение следующих функций защиты информации [2]:

– авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012);

– обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и защиты, в соответствии с ГОСТ 28147-89;

– обеспечения аутентичности, конфиденциальности и защиты соединений по протоколу TLS;

– контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;

– управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Одним из СКЗИ является средство «КриптоПро CSP». Особенностью данного программного обеспечения является использование шифровального алгоритма в соответствии с ГОСТ 28147-89 [3].

Данная система осуществляет реализацию следующих алгоритмов:

– алгоритм выработки значения хэш-функции; реализован в соответствии с требованиями ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

– алгоритмы формирования и проверки электронной подписи; реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

– алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализованы в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».

При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами в соответствии ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012. При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ Р 34.11-94 и ГОСТ 28147-89.

Дополнительные алгоритмы поддержки ключевых систем, параметры алгоритмов, форматы сертификатов, поддерживаемые в СКЗИ, определены в документах RFC 4357, RFC 4490, RFC 4491.

В состав СКЗИ «КриптоПро CSP» входит модуль уровня ядра операционной системы (криптодрайвер), что позволяет использовать основные криптографические функции (шифрование, дешифрация, проверка подписи, хеширование) на уровне ядра операционной системы.

Шифрование информации – взаимно-однозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин «шифрование» объединяет в себе два процесса: «зашифрование»

и «расшифрование» информации. Если «зашифрование» и «расшифрование» осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае – асимметричным. Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же закрытый ключ шифрования.

Процесс шифрования информации в системе «КриптоПро CSP» представим на рис. 2.

Рис. 2. КриптоПро CSP. Процесс шифрования информации

Программное обеспечение средства «КриптоПро CSP» позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей X.509 со следующим программным обеспечением:

– центр сертификации – Microsoft Certification Authority, входящий в состав OS Windows 2000 Server, Advanced Server;

– электронная почта – Microsoft Outlook 98, 2000, XP;

– электронная почта – Microsoft Outlook Express, входящая в состав Internet Explorer версии 5.0 или выше;

– средства контроля целостности ПО, распространяемого по сети – Microsoft Authenticode.

Для защиты TCP/IP соединений в сети Интернет используется протокол TLS/SSL.

Преимущество данного продукта также заключается в его гибкости, так как, он ориентирован на российский рынок и может удовлетворить большинство запросов пользователей.

Список используемых источников

1. Грачева Е. Ю. Банковское право Российской Федерации : учебное пособие. М. : НОРМА: ИНФРА-М, 2013. 399 с.

2. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. Технические средства и методы защиты информации: учеб. для вузов / Под ред. А. П. Зайцева и А. А. Шелупанова. М. : Машиностроение, 2009. 508 с.

3. Резниченко В. В. Особенности реализации удостоверяющего центра на базе программно-аппаратного комплекса «КриптоПро УЦ» // Вестник Южно-уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2012. № 23. С. 187–188.

Статья представлена заведующей кафедрой, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.056

КОМПЬЮТЕРНЫЕ АТАКИ И ИХ ХАРАКТЕРИСТИКИ

Е. И. Данилова, О. С. Лаута, М. В. Митрофанов, С. Н. Ракицкий

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Компьютерные атаки на элементы информационно-телекоммуникационной сети реализуются в виде целенаправленных воздействий, приводящих к нарушению или снижению эффективности выполнения технологических циклов в информационно-телекоммуникационной сети. К наиболее распространенным компьютерным атакам на элементы ИТКС относится компьютерная атака «Логическое отключение абонентов». Компьютерные атаки обладают вероятностно-временными характеристиками, определение которых позволяет оценить степень ее опасности, выбрать и реализовать меры защиты.

компьютерная атака, логическое отключение абонентов, вероятностно-временные характеристики.

Компьютерные атаки (КА) на элементы информационно-телекоммуникационной сети (ИТКС) реализуются в виде целенаправленных программно-аппаратных воздействий, приводящих к нарушению или снижению эффективности выполнения технологических циклов в ИТКС [1].

К одной из наиболее распространенных компьютерных атак на элементы ИТКС относится компьютерная атака «Логическое отключение абонентов».

Компьютерные атаки обладает вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень ее опасности, выбрать и реализовать меры защиты.

Для исследования и определения ВВХ КА необходима разработка ее модели (профильной, математической) и метод топологического преобразования стохастических сетей.

Суть метода топологического преобразования стохастических сетей заключается в том, что исследуется не система, а процесс, который она реализует. Сложный процесс декомпозируется на элементарные процессы, каждый из которых характеризуется функцией распределения, средним временем и его дисперсией.

Логика и последовательность выполнения процессов определяется двухполюсной сетью, состоящей из входного, промежуточных и выходного узлов (вершин), при этом ребрам соответствует набор элементарных процессов, а вершинам (узлам) – условия их выполнения. Каждый узел (вершина) выполняет две функции – входную, определяющую условие (логическую операцию), при котором функция может быть выполнена, и выходную, определяющую какие из операций, следующих за узлом, будут выполняться. Входной узел сети выполняет только предшествующую выходную функцию, а выходной только входную. Для каждого ребра определяется функция передачи – условная характеристическая функция, являющаяся преобразованием Лапласа функции плотности вероятностей времени свершения элементарного процесса.

Для совокупности ребер осуществляется топологическое преобразование стохастической сети по правилу Мэйсона. При этом топологическим инвариантом сети является связность сети. Поскольку входная и выходная вершины двухполюсной сети (графа) являются связными, то топологическое преобразование приводит к получению эквивалентной функции, сохраняющей в своей структуре параметры распределения и логику взаимодействия элементарных случайных процессов [1, 2, 3].

Эквивалентная функция позволяет определить первые моменты случайного времени выполнения целевого процесса, либо произвести ее обратное преобразование по Лапласу (определить ее оригинал в пространстве изображений Лапласа), результатом которого является функция плотности вероятностей времени выполнения этого процесса.

Таким образом, сущность метода топологического преобразования стохастических сетей состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации, т. е. реализации анализируемого процесса [1, 4, 5].

Рассмотрим профильную модель компьютерной атаки типа «Логическое отключение абонентов».

Злоумышленник осуществляет КА в следующей последовательности:

запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $t_{\text{вкл ср}}$ с функцией распределения времени $W(t)$;

перехват с вероятностью P_n IP-адресов абонентов атакуемой ИТКС за среднее время $t_{\text{перех ср}}$ с функцией распределения времени $M(t)$;

изменение IP-адресов абонентов атакуемой ИТКС за среднее время $t_{\text{изм ср}}$ с функцией распределения времени $D(t)$;

отключение абонентов за среднее время с функцией распределения времени $L(t)$.

Если *IP*-адреса не перехвачены, то с вероятностью $(1 - P_n)$ повторно выполняется их перехват за среднее время с функцией распределения времени $Z(t)$.

Требуется определить интегральную функцию распределения вероятности $F(t)$ и среднее время $\overline{T}$ реализации компьютерной атаки типа «Логическое отключение абонентов».

Рассмотрим математическую модель КА типа «Логическое отключение абонентов».

Описанный выше процесс реализации КА представим в виде стохастической сети (рис. 1).

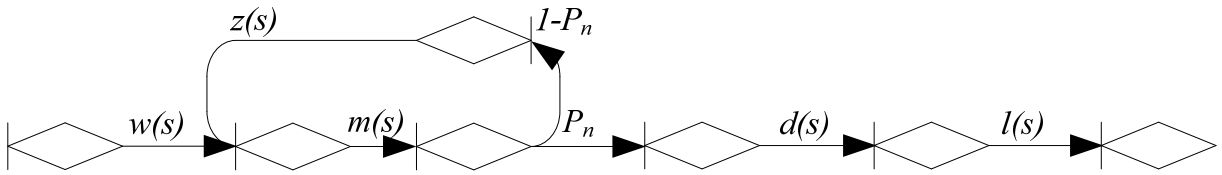


Рис. 1. Стохастическая сеть компьютерной атаки типа «Логическое отключение абонентов»

Используя уравнение Мейсона, преобразование Лапласа, разложение Хевисайда и метод топологического преобразования стохастических сетей [2], функцию распределения вероятности времени реализации КА можно определить следующим образом:

$$F(t) = \sum_{k=1}^{5} \frac{w \cdot m \cdot P_n \cdot d \cdot l \cdot (z + S_k)}{\varphi \cdot (S_k)} \cdot \frac{1 - \exp[S_k t]}{-S_k},$$

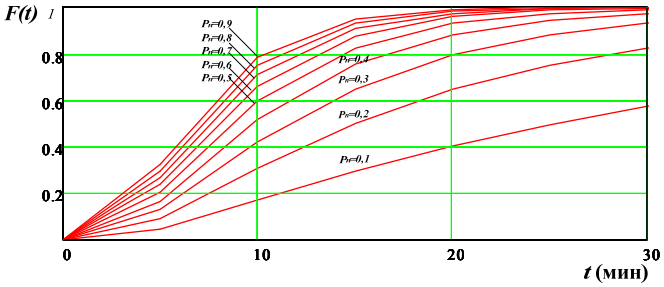
а среднее время $\overline{T}$, затрачиваемое на реализацию компьютерной атаки:

$$\overline{T} = \sum_{k=1}^{5} \frac{w \cdot m \cdot P_n \cdot d \cdot l \cdot (z + S_k)}{\varphi \cdot (S_k)} \cdot \frac{1}{(-S_k)^2}.$$

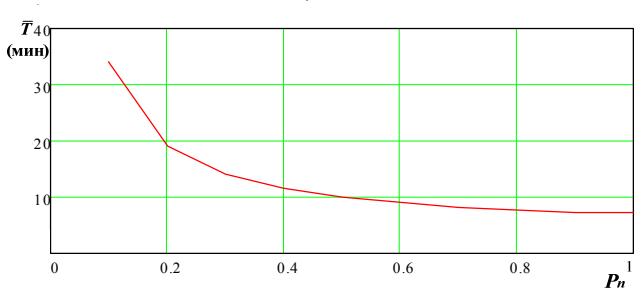
Зависимости функции распределения вероятности $F(t)$ и среднего времени $\overline{T}$ представлены на рис. 2. В качестве исходных данных используются следующие значения времени и вероятности, соответствующие профильной модели компьютерной атаки типа «Логическое отключение абонентов»:

$t_{\text{вкл ср}} = 3$ мин, $t_{\text{перех ср}} = 1$ мин, $t_{\text{изм ср}} = 1$ мин, $t_{\text{откл ср}} = 1$ мин, $t_{\text{повт ср}} = 1$ мин,

$P_n = 0{,}1 \ldots 0{,}9$



а)



б)

Рис. 2. Вероятностно-временные характеристики компьютерной атаки типа «Логическое отключение абонентов»: а) зависимость интегральной функции распределения вероятностей от времени реализации компьютерной атаки; б) зависимость среднего времени реализации компьютерной атаки от вероятности перехвата IP-адреса

Анализ полученных результатов позволяет сделать выводы:

среднее время реализации компьютерной атаки «Логическое отключение абонентов» с вероятностью $P_n = 0{,}1$ составляет 35 минут и 8 минут при $P_n = 0{,}9$.

полученные зависимости позволяют оценить влияние вероятности перехвата IP-адресов абонентов на показатель эффективности реализации компьютерной атаки. Видно, что увеличение вероятности P_n повышается эффективность компьютерной атаки. Однако, по мере возрастания значения P_n степень влияния на интегральную функцию распределения $F(t)$ уменьшается и при преодолении значения $P_n > 0{,}4$ степень влияния пренебрежимо мала.

результаты моделирования могут быть использованы при обосновании направлений разработки системы защиты ИТКС, целью которой является предотвращение (затруднение) реализации компьютерной атаки.

Список используемых источников

1. Климов С. М. Методы и модели противодействия компьютерным атакам. Люберцы : Каталист, 2008. 316 с.

2. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб. : ВМА, 2000.

3. Лепешкин О. М., Карпов А. В., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь: сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 1198.

4. Карпов А. В., Лепешкин О. М., Попов Н. А. Структура электромагнитного поля при нелинейной радиолокации // Радиолокация, навигация, связь: сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 1118.

5. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях; Военная академия связи имени Маршала Советского Союза С. М. Буденного. СПб., 2013.

УДК 004.056

МОДЕЛИРОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В СИСТЕМЕ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ

В. А. Десницкий[1, 2, 3], А. В. Мелешко[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургскийнациональный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Проводится моделирование инцидентов безопасности в рамках модели киберфизической системы управления водоснабжением. Разрабатываемый стенд моделирования базируется на микроконтроллерах платформы Arduino, сенсорах уровня и потока воды, электроприводных кранах и программном компоненте централизованного мониторинга безопасности и управления системой на языке Python. Обосновывается выбор конкретных программно-аппаратных средств для построения стенда моделирования. Продемонстрирована возможность отслеживания на программно-информационном уровне данных о событиях физической безопасности с последующим формированием инцидентов безопасности определенного типа.

Инцидент безопасности, моделирование, киберфизическая система, система управления водоснабжением, Arduino.

На сегодняшний день все большое распространение получают узкоспециализированные киберфизические системы (КФС). Такие системы

применяются в различных областях деятельности, на транспорте, в здравоохранении и в других областях. Среди объектов внедрения КФС выделяют объекты с критически важной инфраструктурой. Безопасности КФС на таких объектах необходимо уделять особое внимание, так как любые сбои могут приводить к катастрофичным последствиям.

К особенностям КФС относят осуществление реагирования системой на изменения в ее окружении, причем взаимодействие осуществляется посредством различных датчиков. КФС получает от них данные о состоянии окружающей среды и в дальнейшем реагирует на изменение её параметров. Поэтому подменив информацию о параметрах окружения, злоумышленник способен удаленно воздействовать на функционирование системы. В случае системы управления водоснабжением нарушение в функционировании могут приводить к разнообразным, в том числе и катастрофическим последствиям, например, затоплению города.

Для предотвращения подобных негативных последствий необходимо заранее смоделировать возможные инциденты безопасности в КФС на испытательном стенде, что поможет выбрать и использовать адекватные алгоритмы реагирования на них.

Проведены поисковые исследования существующих систем и технологий управления водоснабжением, а также проведен обзор работ, затрагивающих вопросы безопасности в таких системах. На сегодняшний день можно выделить как довольно простые системы управления водоснабжением, например, систему капельного полива, так и более сложные – систему управления водоснабжением в многоквартирных домах. Однако документация, архитектуры и исходный код таких технических решений в открытом доступе не представлен.

В [1] приведен общий подход для выбора контрмер на события безопасности с использованием графов атак и графов зависимостей для вычисления метрик безопасности и управления событиями безопасности. В [2] предлагается подход к моделированию атак с целью их дальнейшего предотвращения. Предлагается таксономия кибератак AVOIDIT, описывающая, в частности, вектор атаки, операционное воздействие, защиту, информационное воздействие и цели.

В [3] описана система диагностики дамб, позволяющая отследить обрыв цепи датчиков, определить уровень сигнала в коммуникационной шине и наличие короткого замыкания. Такая система может применяться не только для диагностики, но и для выявления инцидентов безопасности.

В [4, 5] исследуются системы мониторинга и моделирования безопасности плотин в режиме реального времени. Подобные системы позволяют смоделировать предстоящую аварийную ситуацию, опираясь на данные постоянного мониторинга окружающей среды, а также основываясь на статистических данных о погодных условиях. Хотя данные системы

не прогнозируют события кибер-безопасности, но они позволяют моделировать угрозы стихийного характера.

В [6] приведено описание системы управления гидроэнергетической плотиной, причем подробно раскрыты состав подсистемы управления и предложенный интерфейс человеко-машинного взаимодействия. Анализ актуальных источников литературы позволил выявить следующие ключевые направления в области систем управления водоснабжением: моделирование и анализ инцидентов безопасности объектов критически важной инфраструктуры; контроль безопасности дамб в реальном времени; системы управления плотинами и подсистемы их диагностики.

В качестве основы для моделирования инцидентов безопасности был выбран макет дамбы – гидротехнического сооружения, представляющего грунтовую насыпь трапецеидального сечения для регулирования водных потоков. [2] Она позволяет поддерживать постоянный уровень воды с одной из своих сторон. Достигается это путем перекрывания или наоборот открывания затворов. Затворы дамбы открываются в случае превышения допустимого уровня воды и закрываются при его снижении ниже установленной границы (рис. 1).

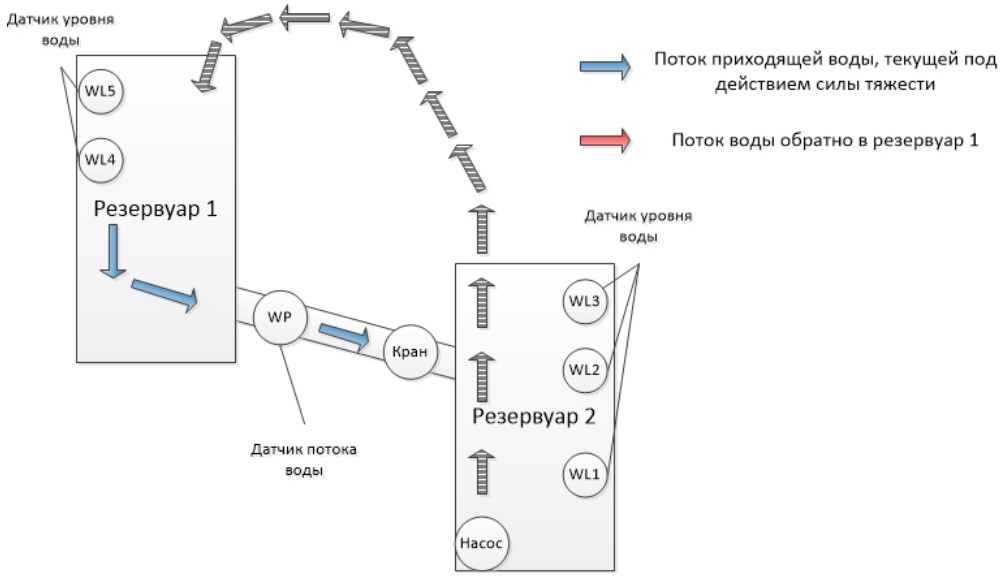


Рис. 1. Схема разработанного макета дамбы

Вода под действием силы тяжести поступает из резервуара 1 в резервуар 2, тем самым моделируя течение реки, а управляемый кран играет роль затвора дамбы. Для контроля уровня воды в резервуаре 2 предусмотрено несколько датчиков уровня воды. В случае если уровень воды становится критическим, то перекрывается управляемый кран, а вода из резервуара 2 посредством насоса подается обратно в резервуар 1. Т. е.

моделируются реальные условия – вода по одну сторону уходит по течению, а с другой стороны приходит новая.

Для организации считывания показания датчиков и реагирования на изменения физической среды использован микроконтроллер Arduino UNO. Для моделирования инцидентов безопасности на языке Python разработана программа мониторинга состояния системы с возможностью принудительного управления краном и насосом.

Для взаимодействия микроконтроллера и персонального компьютера разработан протокол передачи данных о состояния системы. Передача организована по проводному каналу связи через serial-порт. Формат кадра протокола содержит граничные начальный и конечный символы, значение количества датчиков, состояния каждого датчика, количество исполнительных элементов (актуаторов), и текущие состояния актуаторов. Для контроля целостности в конце кадра добавляется его хэш.

Осуществляется корреляция событий безопасности, направленная на выявление связей между ними в соответствии с заданными правилами, что позволяет определить конкретные инциденты безопасности, например, злонамеренную модификацию данных в системе. В общем виде правило корреляции событий имеет следующий вид: $(\{ev\_sw_i)\}_i \cup \{ev\_ph_i\}, t) \rightarrow Type_{Inc}$, где ev_sw_i – набор событий программно-информационного характера, в ev_ph_i–события физического характера, выполнение которых в рамках фиксированного временного промежутка t, определяет наличие инцидента заданного типа $Type_{Inc}$.

В качестве примера приведем правило корреляции, определяющее инцидент несоответствия показаний датчиков уровня воды. Данный инцидент является результатом атаки с параллельным физическим воздействием на датчик уровня воды и воздействием на уровне пользовательского интерфейса: $((l_1 == false), (l_2 == true), ep, opn) \rightarrow inc$, где несрабатывание датчика уровня воды l_1при сработавшем датчик l_2, событие ep несанкционированного получения доступа к управлению системой и событие opn– открытия затвора обуславливают инцидент возможного затопления водяного резервуара.

На разработанном стенде смоделированы следующие атакующие воздействия: атака на датчики системы; атака на актуаторы системы; модификация программного кода микроконтроллера; внедрение в канал связи контроллера и ПК (*man-in-the-middle*). Атака на датчик системы включают фальсификацию или подмену его показаний или его физическое разрушение.

Атака на актуатор системы так же предполагает фальсификацию обратной связи, например, ложное оповещение о том, что затвор закрыт, хотя на самом деле это не так. Модификация программного кода микрокон-

троллера предполагает, что злоумышленник способен добраться до него и перезаписать алгоритм реагирования не изменение параметров окружающей среды. Атака man-in-the-middle означает, что злоумышленник может подключиться к каналу связи «микроконтроллер – программа мониторинга» и посылать ложные команды. Последний вид угрозы особенно критичен если канал связи беспроводной.

Перечисленные инциденты приводят к некорректной работе системы управления водоснабжением или к прекращению её работы. Отметим, что возможность реализации каждого из перечисленных инцидентов зависит от специфики конкретной системы, например, физическое разрушение датчиков окажется маловероятным при отсутствии у злоумышленника физического доступа к ним. Однако построенный макет может помочь выработать требования и универсальный набор контрмер для таких систем.

В работе анализируются инциденты безопасности критически важных КФС управления водоснабжением. Моделирование инцидентов безопасности служит основой для разработки механизмов предотвращения атакующих воздействий злоумышленников. Для решения задач моделирования инцидентов безопасности построен макет системы управления водоснабжением, включающие следующие компоненты: компонент управления данными от сенсоров и актуаторов; компонент управления функциями системы; протокол взаимодействия с обеспечением целостности передаваемых данных. С использованием данного макета определены типовые инциденты безопасности. Разработанный макет может быть применен для выявления слабых мест данного класса систем и снижения рисков возникновения нештатных ситуаций и критически важных инцидентов безопасности [8].

В дальнейшей работе планируется моделирование частных инцидентов безопасности и исследование вопросов по выработке контрмер и предложений по совершенствованию компонентов защиты систем управления водоснабжением. В рамках построенного макета планируется организация беспроводной передачи данных с микроконтроллера на персональный компьютер, а также перенос программного обеспечения на мобильные платформы.

Работа выполнена в СПИИРАН при поддержке Гранта президента Российской Федерации № МК-5848.2018.9.

Список используемых источников

1. Doynikova E., Kotenko I. Countermeasure selection based on the attack and service dependency graphs for security incident management // 10th International Conference on Risks and Security of Internet and Systems: CRiSIS, LNCS, Springer. 2016. Vol. 9572. PP. 107–124.

2. Simmons C. B., Shiva S .G., Bedi H., Dasgupta D. AVOIDIT: A Cyber Attack Taxonomy // The 9th Annual Symposium on Information Assurance (ASIA'14). 2014.

3. Bande V., Pop S., Pitica D. Smart Diagnose Procedure for Data Acquisition Systems Inside Dams // 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME). 2014. PP. 179–182.

4. Dong L., Shu W., Sun D., Li X., Zhang L. Pre-Alarm System Based on Real-Time Monitoring and Numerical Simulation Using Internet of Things and Cloud Computing for Tailings Dam in Mines // IEEE Access. 2017. Vol. 5. PP. 21080–21089.

5. Li Y., Wang Y. Design and implementation of reservoir dam safety monitoring platform based on ASP.NET // 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). 2017. PP. 2644–2648.

6. Iacobici N. L., Frigura-Iliasa F. M., Vatau D., Andea P. Command and control interface for a navigation lock at a Hydro Power Dam // 2017 International Conference on Information and Digital Technologies (IDT). 2017. PP. 142–145.

7. Горная энциклопедия / Под редакцией Е. А. Козловского. М. : Советская энциклопедия, 1984–1991.

8. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // ТРУДЫ СПИИРАН. 2016. № 5 (48). С. 5–31.

УДК 004.7

ОСОБЕННОСТИ ПЕРЕНОСИМОСТИ ИСХОДНОГО КОДА ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ JAVA

Р. А. Джусупов, Д. О. Федосеев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Язык программирования Java обеспечивает простейшую и наиболее знакомую форму переносимости-переносимость исходного кода. Это значит, что java-программы должны давать одинаковые результаты независимо от основного процессора, операционной системы или компилятора.

Java, кроссплатформенное программирование, мониторинг, база данных.

Данная идея не нова; такие языки, как C и C++, уже много лет предоставляют возможность для такого уровня переносимости. Однако, C и C++ предлагают множество возможностей для создания также и непереносимого кода. Если программы, написанные на C и C++, не предназначены для переносимости с самого начала, возможность перемещения на разные машины более теоретическая, чем практическая. C и C++ оставляют неоп-

ределенными такие детали, как размер и обратный порядок байт (обозначающий или относящийся к системе данных упорядочения в памяти компьютера, в результате чего сначала ставится старший (бай-дин) или наименее значимый (мало-конечный) байт.) из атомарных типов, данных, поведение плавающей запятой, значение неинициализированных переменных, и поведение, когда доступна свободная память [1].

Несмотря на то, что синтаксис C и C++ определен хорошо, семантика этих языков нет. Данный семантический недостаток позволяет одному блоку C или C++ исходного кода компилировать программы, которые дают разные результаты при запуске на разных процессорах, операционных системах, и даже на одном компиляторе/процессоре/ОС, в зависимости от различных параметров компилятора.

В Java все по-другому – Java обеспечивает гораздо более строгую семантику и оставляет меньше работы конструктору (рис. 1). Кроме того, Java определяет больше свойств, чем C и C++. В Java память не освобождается до тех пор, пока она больше не будет недоступна, и язык не имеет никаких неинициализированных переменных. Все эти функции помогают минимизировать различия в поведении программы Java при переносе с одной платформы на другую и при ее компиляции [2].

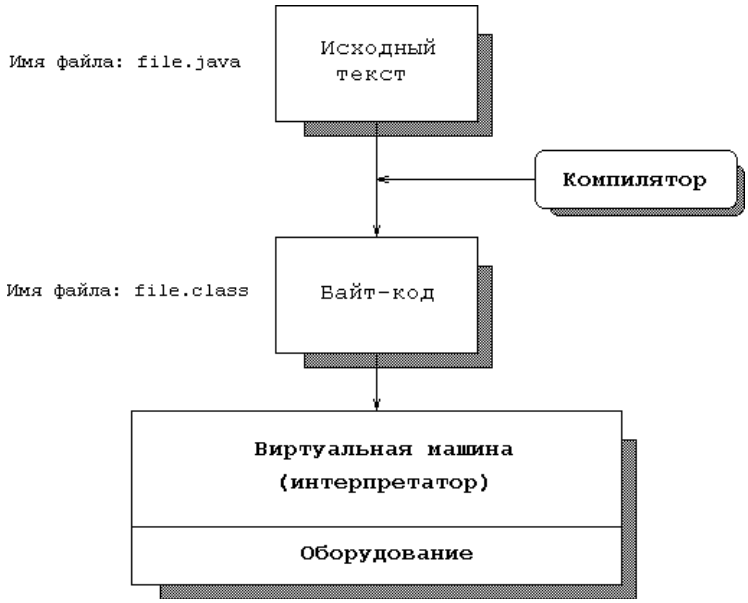


Рис. 1. Схематичное представление процесса запуска и функционирования программы на Java

К сожалению, функции, которые делают Java настолько портативным, имеют обратную сторону. Java предполагает 32-разрядную машину с 8-разрядными байтами и математикой с плавающей точкой IEEE754. Машины, которые не подходят для этой модели, включая 8-битные микроконтроллеры и суперкомпьютеры Cray, не могут эффективно запускать Java. Справедливо, что C и C++ используется на большем количестве платформ, чем язык Java. Также справедливо, что программы Java будут портироваться проще, чем C или C++ между поддерживаемыми платформами.

Большинство программ для Windows, написанные на C или C++ нелегко портировать на Macintosh или Unix-среды, даже после перекомпиляции. Даже если программисты принимают дополнительные меры для борьбы с семантическими недостатками C и C++, процедура сложная

и трудоемкая. После исключения семантических проблем в C и C++, программисты еще должны иметь дело с различными операционными системами и их различными методами вызова графического интерфейса API. Программы для Windows создают много различных вызовов операционной системы, в отличии от программ Macintosh и Unix. Данные вызовы имеют решающее значение для написания нетривиальных программ, поэтому до решения этой проблемы переносимости перенос будет оставаться трудным.

Java решает эту проблему, предоставляя набор библиотечных функций (содержащиеся в Java-поставляемые библиотеки – *awt*, *util* и *lang*), что позволяет взаимодействовать с виртуальной ОС и мнимой GUI. Также как JVM представляет собой виртуальный процессор, библиотеки Java – виртуальную ОС/графический интерфейс. Каждая реализация java предоставляет библиотекам реализации этой виртуальной ОС/графический интерфейс (рис. 2).

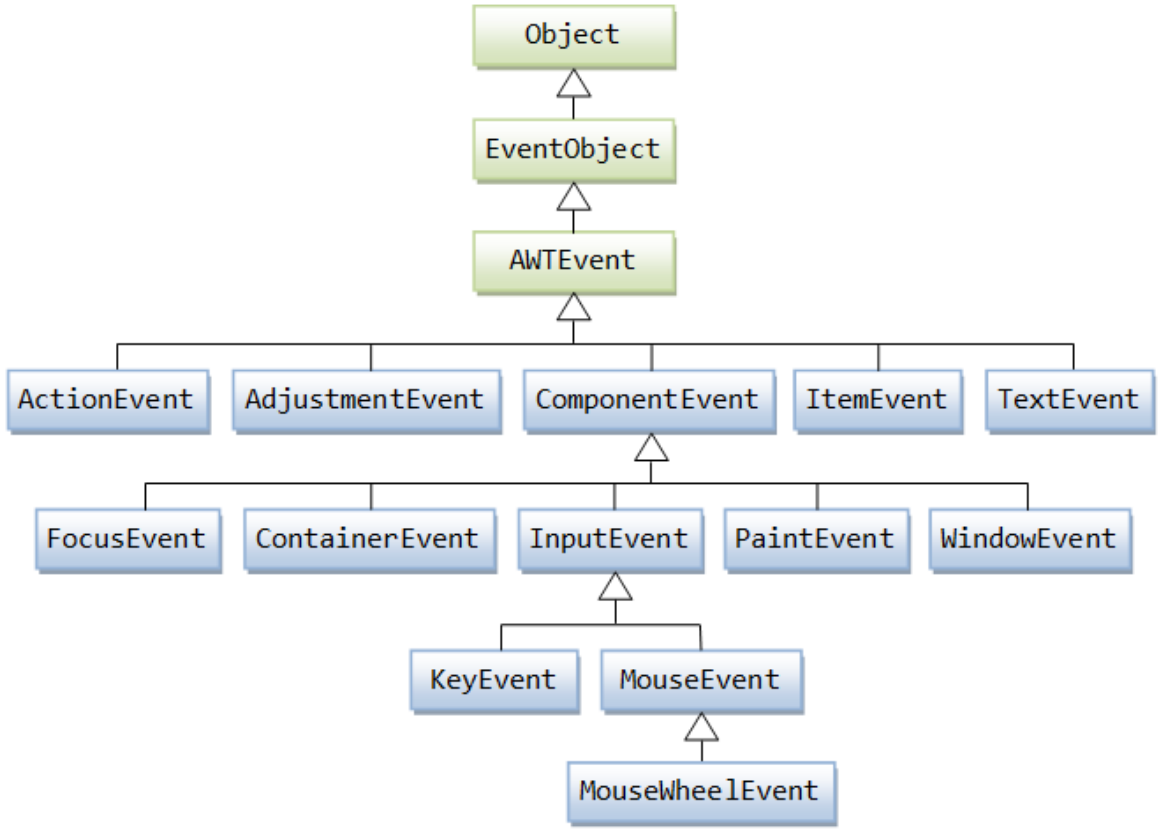


Рис. 2. Компоненты Java GUI

Java предоставила функциональность наименьшего общего знаменателя в своих библиотеках OS / GUI. Функции, доступные только на одной ОС / GUI, такие как диалоговые окна с вкладками, были опущены [3]. Преимущество этого подхода заключается в том, что сопоставление общей

функциональности с родной ОС/GUI довольно легко и, с осторожностью, может обеспечить приложения, которые работают, как ожидается, на большинстве OS/GUI. Недостатком является то, что функциональность, доступная для приложений в родном режиме, недоступна для приложений Java.

Список используемых источников

1. Битнер В. И. Брюс Эккель – Философия Java. М. : Горячая линия – Телеком, 2011. 312 с.

2. Джошуа Блох Java. Эффективное программирование – типичные проблемы и их решения. Oracle Press, 2010. 405 с.

3. Кей Хорстманн Java. Библиотека профессионала. 10-е изд. (Т. 1, 2). Sun Systems, 2010. 981 с.

УДК 004.656

К ВОПРОСУ СОЗДАНИЯ И ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕГО КАТАЛОГА ДЛЯ НОМЕНКЛАТУРЫ БАЗОВОГО ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

М. А. Добросельский[1], В. И. Курносов[2], А. А. Ларин[1]

[1]АО «НИИ «Рубин»

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

Дается анализ методов и подходов к построению информационно-управляющего каталога в интересах управления номенклатурой предметов снабжения в отрасли связи. Обосновывается выбор модели функционирования системы управления номенклатурой ПС на основе применения информационно-управляющего каталога. Излагается методика выбора рационального состава информации, включаемой в стандартные форматы описания предметов снабжения, даются предложения к перечню функциональных задач, решение которых целесообразно с использованием ИУК системы каталогизации предметов снабжения.

информационно-управляющий каталог, рациональный состав, номенклатура предметов снабжения, функциональные задачи.

Современный этап реформирования и развития ведомственных систем связи характеризуется пересмотром многих положений и взглядов на порядок формирования заказа на разработку, производство и поставку служ-

бам связи базового телекоммуникационного оборудования (БКТС)). При этом в ряду объемных и сложных задач одно из главных мест занимает задача управления номенклатурой БКТС, именуемых в руководящих документах предметами снабжения (ПС).

Работы по управлению номенклатурой ПС, проводившиеся до настоящего времени, не привели к коренному изменению существующей тенденции роста номенклатуры ПС, составных частей и комплектующих изделий. Как показал проведенный анализ, номенклатура БКТС практически на порядок превышает теоретически оптимальную. Используемые для управления номенклатурой методы базируются на эмпирических подходах, знаниях и опыте специалистов.

В то же время опыт ведущих зарубежных стран показывает, что одним из перспективных методов управления номенклатурой является использование информационно-управляющих каталогов (ИУК). ИУК позволяют автоматизировать решение задач управления номенклатурой и применить объективные, научно-обоснованные методы для выработки управляющих воздействий.

Для разрешения данных противоречий, Правительство Российской Федерации в начале 2000-х годов приняло два основополагающих постановления по развертыванию в стране работ по каталогизации: от 11 января 2000 г. № 26 «О федеральной системе каталогизации продукции для федеральных государственных нужд» и от 2 июня 2001 г. № 436 «О создании и введении в действие федерального каталога продукции для федеральных государственных нужд».

В настоящее действует система каталогизации продукции для федеральных государственных нужд, регламентированная рекомендациями по каталогизации Р 50.5.004-2002, принятыми и введенными в действие Постановлением Госстандарта России от 18.04.2002 г. № 156-ст, а также национальный стандарт Российской Федерации ГОСТ Р 51725.9-2009 «Порядок формирования и ведения сводной части федерального каталога продукции для федеральных государственных нужд» (разработан Федеральным государственным учреждением «Федеральный центр каталогизации», внесен Техническим комитетом по стандартизации ТК 430 «Каталогизация продукции», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 1153-ст).

Важнейшей составляющей федерального каталога продукции является Единый каталог предметов снабжения. В свою очередь одной из составляющих этого каталога является раздел техники связи. Его создание является важной и актуальной научно-технической задачей.

Из сказанного следует актуальность целевой установки: исследование системы управления номенклатурой ПС, разработка методического обес-

печения управления номенклатурой ПС в целях повышения эффективности процессов развития, заказа, разработок, эксплуатации и утилизации ПС за счет автоматизации решения задач по управлению их номенклатурой.

Предполагается, что указанная цель будет достигнута путем разработки методики формирования ИУК и научно-обоснованных рекомендаций по его применению в интересах лица принимающего решение (ЛПР) для выбора рационального варианта планирования заказа ПС на предприятиях промышленности средств связи.

Новизна исследования в данной постановке определяется формированием принципов и общей схемы управления номенклатурой ПС на основе применения ИУК, разработкой математической модели формирования ИУК, методикой рационального описания образцов БКТС, их составных частей, комплектующих изделий и ЗИП для включения в ИУК, методикой многокритериальной оценки и сопоставительного анализа технических характеристик.

В отличие от известных, результаты этих исследований учитывают максимально полную совокупность разнородных показателей, существенных при выборе варианта развития групп однородных образцов и возможность получения количественных оценок для качественных показателей ПС.

Таким образом, полученные результаты обеспечат научно-методическую основу для создания организационно-технических систем управления виртуальными объектами и процессами, описываемыми на формализованных языках, близких к естественному [1, 2].

Данное направление работ является закономерным развитием и продолжением исследований Ионова С. В., Карташова А. В., Ситнова А. П., Рахманова А. А., Корзухина И. С., King T., Ooreebeek N., Pierra G., проводимых в области программно-целевого управления созданием и развитием систем, комплексов и средств связи и каталогизации продукции. К актуальным результатам следует отнести:

– анализ современного состояния системы каталогизации предметов снабжения служб связи министерств и ведомств РФ;

– предложения по структуре основных элементов ПС;

– анализ номенклатуры ПС и существующих подходов к ее классификации;

– анализ принципов и методов управления номенклатурой ПС;

– обоснование необходимости создания системы управления номенклатурой (СУН) предметов снабжения, определение ее цели;

– формулирование основных принципов управления номенклатурой ПС, обеспечивающих эффективность создания и функционирования СУН;

– обоснование необходимости использования ИУК, как центрального звена СУН;

– моделирование процесса разработки информационно-управляющего каталога и общей схемы управления номенклатурой ПС;

– разработка модели управления номенклатурой ПС на основе применения ИУК системы каталогизации;

– формулировка задач, решаемых в СУН, обоснование состава и структуры СУН, определение возможного состава и механизмов формирования управляющих воздействий;

– анализ и обоснование существенных показателей для оценки качества группы однородных ПС;

– выбор последовательности оценки качества группы однородных образцов;

– разработка математической модели и общей схемы решения задачи формирования ИУК;

– представление результатов разработки методики формирования ИУК;

– процедура технико-экономического обоснования и поддержки принятия решения заказчика при выборе номенклатуры ПС на основе ИУК;

– методика рационального описания ПС, обеспечивающая выбор набора характеристик ПС, необходимого и достаточного для решения задач управления номенклатурой на всех этапах жизненного цикла;

– разработка методики выбора рационального состава информации, включаемой в стандартный формат описания (СФО) для ПС;

– рекомендации по применению разработанных методик по построению ИУК;

– методика технико-экономического обоснования и поддержки решений заказчика при использовании ИУК;

– определение источников получения информации, содержание исходных данных, последовательность решения задачи технико-экономического обоснования при программном планировании развития БКТС;

– предложения по выбору рационального варианта планирования заказа с использованием ИУК, а также предложения по оценке качества заказа;

– перечень функциональных задач, решение которых целесообразно с использованием ИУК;

– организация информационной поддержки системы каталогизации и особенности каталогизации ЗИП;

– представление результатов применения разработанных методик и предложений при создании раздела ПС Единого каталога предметов снабжения РФ.

Список используемых источников

1. Клышинский Э. С., Кочеткова Н. А. Метод извлечения технических терминов с использованием меры странности // Новые информационные технологии в автоматизированных системах. 2014. № 17. С. 365–370.

2. Клышинский Э. С., Кочеткова Н. А., Логачева В. К. Метод кластеризации слов с использованием информации об их синтаксической связности // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2013. № 11. С. 36–39.

УДК 004.056.57

ЦЕЛЕВАЯ ФУНКЦИЯ ФУНКЦИОНАЛЬНО-РОЛЕВОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА

Я. А. Домбровский, О. М. Лепешкин, И. А. Фиалкин

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Эффективность системы разграничения доступа может определяться способностью системы обеспечивать безопасный доступ пользователей к объектам (конфиденциальность), при сохранении множества доступов, необходимых пользователям системы для выполнения своих функциональных и должностных обязанностей (доступность). В качестве целевой функции эффективности системы разграничения доступа можно воспользоваться линейной комбинацией функции доступности информации и функции конфиденциальности информации.

система разграничения доступом, автоматизированная информационная система, целевая функция, функция доступности информации, функции конфиденциальности информации.

Любые меры безопасности и ограничения объективно снижают отдельные характеристики эффективности системы [1]. С другой стороны, отсутствие каких-либо защитных механизмов может привести к значительному ущербу, связанному с нарушениями безопасности. Поэтому в общем случае, независимо от особенностей предметной области автоматизированной информационной системы и коллектива пользователей, эффективность системы разграничения доступа может определяться способностью системы обеспечивать безопасный доступ пользователей к объектам (конфиденциальность), при сохранении множества доступов, необходимых пользователям системы для выполнения своих функциональных и должностных обязанностей (доступность). При этом данные составляющие эффективности системы разграничения доступа к ресурсам являются противоположными по смыслу и направлению [2, 3].

Исходя из этого, в качестве целевой функции эффективности системы разграничения доступа L можно воспользоваться линейной комбинацией функции доступности информации L_1 и функции конфиденциальности информации L_2:

$$L = c_1 L_1 + c_2 L_2, \quad (1)$$

где $c_1 + c_2 = 1$ – весовые коэффициенты, отражающие политику безопасности в системе в плане общего взгляда (установок) на соотношение доступности и конфиденциальности информации в системе. Данный подход описан в работе.

Функции L_1 и L_2, в свою очередь, должны определяться системой и конкретными характеристиками доступа субъектов к объектам. Так, в частности, очевидно, что чем больше назначений доступа с наиболее «сильными» правами у пользователей к наибольшему количеству объектов, тем выше открытость системы и наоборот.

Тот вариант схемы и конкретных назначений доступа, который дает максимум значения функции L, можно считать оптимальным (задачи второй группы). Изменение функции L, а также функций L_1 и L_2 в отдельности, в процессе администрирования системы (добавление/удаление пользователей и объектов, изменения назначений на доступ и т. д.) будут отражать соответственно изменения общей эффективности доступа в системе или соответствующих ее компонент – открытости и закрытости.

Таким образом, задачей создания средств количественного анализа и оптимизации систем разграничения доступа является синтез таких функций L_1 и L_2, которые своими аргументами имели бы параметры всех субъектов, объектов и назначений доступа [4, 5].

Рассмотрим обобщенную модель системы разграничения доступа. В общем случае, абстрагируясь от процессов и механизмов доступа, рассматривая только назначения доступа, систему разграничения доступа можно представить двудольным графом G (U, O, E) (отметим, что здесь и далее понятие субъект тождественно понятию пользователь).

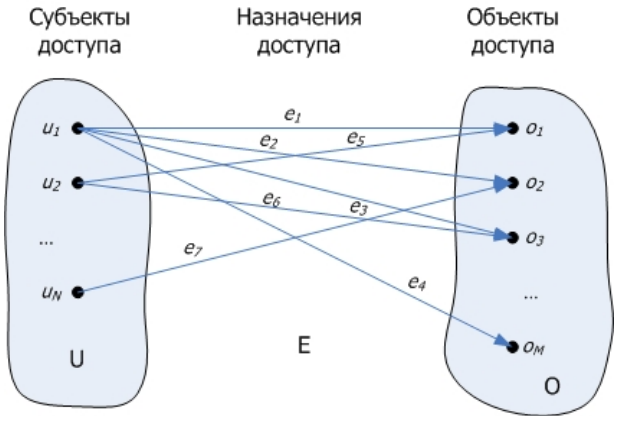


Рисунок. Модель обобщенной системы разграничения доступа в виде двудольного графа

На рисунке дуги графа означают требуемый набор прав доступа пользователей к объектам системы. Набор пользователей $U(u_1, u_2, \ldots, u_N)$, набор объектов $O(o_1, o_2, \ldots, o_M)$ и совокупность требуемых назначений доступа

$E(e_1, e_2, ...)$ составляют исходные параметры и ограничения задачи разграничения доступа.

Состояние системы определяется потоком прав доступа в графе G. Причем, назначение доступа можно описать вещественно-значимой функцией, определяющей вес соответствующей дуги графа с точки зрения доступности (вес $e^{(1)}{}_i$) и с точки зрения безопасности возможных действий пользователя в системе (вес $e^{(2)}{}_i$). Для субъектов доступа можно задать количественные параметры значимости (вес важности $u^{(1)}{}_n$) и безопасности (вес доверия $u^{(2)}{}_n$). Для объектов доступа можно определить их вес с точки зрения важности соответствующих объектов для функционирования системы (вес $o^{(1)}{}_m$) и с точки зрения неопасности для системы (вес $o^{(2)}{}_m$). Отсюда двудольно-графовую модель системы доступа на рисунке можно представить совокупностью двухкомпонентного вектора весов субъектов доступа $\vec{U}(U^{(1)}, U^{(2)})$, двухкомпонентного вектора весов объектов доступа $\vec{O}(O^{(1)}, O^{(2)})$ и двухкомпонентной $N \times M$ матрицы назначений доступа $\vec{E}(E^{(1)}, E^{(2)})$.

Ясно, что чем выше параметры $u^{(1)}{}_n$, $e^{(1)}{}_{nm}$ и $o^{(1)}{}_m$, тем выше открытость системы. И, наоборот, чем выше параметры $u^{(2)}{}_n$, $e^{(2)}{}_{nm}$ и $o^{(2)}{}_m$, тем выше закрытость системы. Тогда очевидно, что эффективность доступа складывается из суммы взвешенных коэффициентами c_1, c_2 сетевых потоков открытости и закрытости системы, каждый из которых является суммой произведений $u^{(1)}{}_n \cdot e^{(1)}{}_{nm} \cdot o^{(1)}{}_m$ и $u^{(2)}{}_n \cdot e^{(2)}{}_{nm} \cdot o^{(2)}{}_m$, соответственно.

Следовательно, общую целевую функцию (1) эффективности доступа в системе, описываемой графом $G(U, O, E)$, можно выразить в следующем виде [2]:

$$L = c_1 U^{(1)T} E^{(1)} O^{(1)} + c_2 U^{(2)T} E^{(2)} O^{(2)} =$$

$$= c_1 \frac{1}{NM} \begin{pmatrix} u_1^{(1)} & u_2^{(1)} & \dots & u_N^{(1)} \end{pmatrix} \begin{pmatrix} e_{11}^{(1)} & e_{12}^{(1)} & \dots & e_{1M}^{(1)} \\ e_{21}^{(1)} & e_{22}^{(1)} & \dots & e_{2M}^{(1)} \\ \dots & \dots & \dots & \dots \\ e_{N1}^{(1)} & e_{N2}^{(1)} & \dots & e_{NM}^{(1)} \end{pmatrix} \begin{pmatrix} o_1^{(1)} \\ o_2^{(1)} \\ \dots \\ o_M^{(1)} \end{pmatrix} +$$

$$+ c_2 \frac{1}{NM} \begin{pmatrix} u_1^{(2)} & u_2^{(2)} & \dots & u_N^{(2)} \end{pmatrix} \begin{pmatrix} e_{11}^{(2)} & e_{12}^{(2)} & \dots & e_{1M}^{(2)} \\ e_{21}^{(2)} & e_{22}^{(2)} & \dots & e_{2M}^{(2)} \\ \dots & \dots & \dots & \dots \\ e_{N1}^{(2)} & e_{N2}^{(2)} & \dots & e_{NM}^{(2)} \end{pmatrix} \begin{pmatrix} o_1^{(2)} \\ o_2^{(2)} \\ \dots \\ o_M^{(2)} \end{pmatrix}.$$

Значение целевой функции L находится на отрезке от 0 до 1, $L \in [0; 1]$, причем, чем ближе L к 1, тем выше эффективность системы разграничения доступа.

Реализация данного подхода включает:

разработку методики получения весов $E^{(1)}$ и $E^{(2)}$ итоговых прав в системе функционально-ролевого доступа;

разработку методики определения весов субъектов доступа, т. е. элементов векторов $U^{(1)}$ и $U^{(2)}$;

разработку методики вычисления весов объектов доступа, т. е. элементов векторов $O^{(1)}$ и $O^{(2)}$.

Список используемых источников

1. Лепешкин О. М., Радько С. А. Функционально-дискреционная модель управления доступом в социотехнических системах // Информационное противодействие угрозам терроризма. 2010. № 14. С. 156–162.

2. Лепешкин О. М., Харечкин П. В. Управление конфликтным процессом решения коллективной задачи социотехнической информационной системы в условиях ресурсной координации // Информационное противодействие угрозам терроризма. 2010. № 14. С. 162–166.

3. Будко Н. П., Будко П. А., Булгаков О. Ю., Васильев В. В., Давидчук В. В., Евграфов А. Е., Жук А. П., Карпов В. В., Князев В. В., Кублик Е. И., Лепешкин О. М., Лощенков И. В., Ляченков С. В., Мезенцев А. В., Павловский И. С., Пирогов М. В., Попов А. А., Потюпкин А. Ю., Прошин Д. С., Радько С. А. интеллектуализация сложных систем язык схем радикалов в проблемных вопросах предпроектных исследований, оснащения, сопровождения систем и в экспериментальных задачах внедрения критических наукоемких технологий: коллективная : монография // Информационно-измерительные и управляющие системы. 2009. Т. 7. № 3. С. 1–92.

4. Лепешкин О. М., Корсунский А. С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления // Автоматизация процессов управления. 2011. № 4. С. 76–81.

5. Бурлов В. Г., Лепешкин О. М., Кириллова Т. В. Методологический подход к оценке безопасности функционирования социальной и экономической системы управления региона // Проблемы экономики и управления в торговле и промышленности. 2013. № 2. С. 99–103.

УДК 681.5

СИСТЕМА ОБРАБОТКИ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

А. В. Дымченко, О. А. Козлова

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

В настоящее время автоматизированная обработка графической информации имеет широкое распространение во многих отраслях человеческой деятельности. В сущности любая интеллектуализированная система содержит в себе модуль, рабо-

тающий с графическими данными. В данном направлении можно особенно выделить систему технического зрения. В статье будут рассмотрены компоненты связанные с системами распознавания графических образов.

компьютерное зрение, распознавание образов, анализ изображения, алгоритм.

Известный факт – большинство информации обычный среднестатистический человек воспринимает с помощью органов зрения. И современные автоматизированные системы также не могут обойтись без работы с графической информацией.

Можно привести бесчисленное количество примеров таких систем. В частности, это различные сканеры, камеры слежения, системы технического зрения и многое другое.

Все эти частные случаи можно свести к одному общему классу систем – системам распознавания образов.

Элементарный алгоритм применительно к обработке графической информации будет выглядеть следующим образом:

– получение исходного изображения;
– выделение контуров объектов на изображении;
– соотношение объектов с базой эталонов;
– вывод результатов.

На первый взгляд все достаточно просто, однако существует огромное количество сложностей, которые могут возникнуть при реализации таких задач [1].

К одной из самых часто встречающихся проблем можно отнести плохое качество исходного изображения. Среди причин этого особо выделяются:

– низкое качество оптики;
– шумы при передаче и/или приеме изображения;
– сложности, вызванные окружающей средой, не позволяющие техническим средствам полноценно отобразить картинку реального мира (например, туман);
– плохое качество материального носителя считанного изображения (старая потертая фотография);
– другие.

К тому же, объекты на изображении могут быть близкими друг к другу по своим свойствам: цвету, текстуре, т. д.

В этих случаях при работе алгоритма распознавания образов будут возникать ошибки.

В качестве примера можно привести черно-белую фотографию и стандартный графический редактор. На фотографии человеческий глаз достаточно легко может различить контуры поребрика, однако при попыт-

ке автоматически выделить его верхнюю поверхность, захватывается не только она, но и боковая поверхность и даже дорога, что демонстрирует пунктирный контур на рис.

Рисунок. Попытка выделения контура объекта стандартным редактором

Разумеется, в данном примере можно использовать ручное выделение и исправить ошибку редактора. Однако если речь идет не о ретушировании домашних фотографий, а о сложной системе, в которой результат распознавания образов будет идти на вход другой системы, и ручная его корректировка если и возможна, то уж точно не желательна, вот тут приходится искать методы решения данной проблемы.

Сама задача разбиения общего изображения на отдельные части таким образом, чтобы каждая из частей содержала в себе только один объект, называется сегментацией.

От выбора метода сегментации во многом и зависит дальнейшая работа с контуром изображения.

Принципиально выделяется автоматическая сегментация, которая подразделяется на ряд более узких классов:

– сегментация, производящаяся на области с заданными свойствами объекта. В этом случае должна присутствовать априорная информация о том свойстве, которое несет существенную информационную нагрузку для результата работы с изображением;

– сегментация, разделяющая картинку на однородные части. Достоинством этого вида можно считать универсальность, ввиду того, что она не требует никакой априорной информации.

Сегментация необходимый процесс распознавания изображения, однако, его качество определяется в совокупности с другими этапами работы с картинкой [2].

Большим вопросом при обработке графической информации можно считать выбор алгоритма, классификации, который является неотъемлемой частью задачи распознавания образов.

Классификаций таких алгоритмов, как и самих алгоритмов, существует бесчисленное множество.

На более общем уровне все алгоритмы делятся следующим образом:

– четкие, т. е. такие алгоритмы, степень принадлежности в которых может быть только «1» или «0», что означает, что объект относится к классу или не относится к классу на 100 % соответственно;

– нечеткие (они же *fuzzy* алгоритмы), которые позволяют соотносить объект одновременно со всеми классами с суммарной степенью принадлежности равной единице.

Первая группа алгоритмов сразу отсекает ряд признаков, которые хоть сколько-нибудь меньше других. Тогда как вторая дает большую возможность для варьирования дальнейшей работы, но требует дополнительных мощностей системы.

Еще одним важным аспектом при распознавании графических образов является база эталонов, с которой соотносят объекты и то, какой принцип используется при сравнении.

Если объект типовой, например, напечатанный стандартным шрифтом текст, то его без особых сложностей распознает практически любая система (в случае, если нет проблем с аппаратной компонентой). Однако работать с рукописными символами гораздо сложнее: даже если человек писал подражая машинным шрифтам, все равно его почерк содержит ряд шероховатостей, обосновывающихся человеческим фактором: наклоном линий, нетвердостью руки, округлостью прямых, т. п. И еще сложнее ситуация с текстом написанным почерком без попытки повторить стандартные печатные шрифты. Количество расхождений с эталоном в этом случае может быть бесконечным.

К тому же на протяжении всего жизненного цикла системы количество эталонных объектов может увеличиваться, а, значит, у базы должна быть возможность расширяться. В идеале система делает это самостоятельно: найдя новый объект, не похожий ни на один эталон, она описывает его в терминах, принятых для этой системы, ищет те реакции, которые необходимы и запоминает его так, что в следующий раз данный объект уже не будет новым [3].

На сегодняшний день спектр задач, которые решаются с применением графической информации, невероятно велик. При этом, каждая предметная область накладывает свои ограничения на системы, делая каждую из них уникальной. Однако многообразие программно-аппаратного комплекса позволяет преодолеть если не все, то многие проблемы, которые возникают

при обработке изображения, делая систему надежной и позволяя получить наилучшие результаты.

Список используемых источников

1. Письменный Н. Распознавание образов мобильным роботом [Электронный ресурс] // Журнал «Робот мысли, схемы & решения». 2007. URL: http://www.ampersant.ru/glaz/ (дата обращения 06.04.2017).

2. Поршнев С. В., Левашкина А. О. Универсальная классификация алгоритмов сегментации изображений [Электронный ресурс] // Журнал научных публикаций аспирантов и докторантов. 2008. N 3. С. 23 URL: http://jurnal.org/articles/2008/inf23.html (дата обращения 06.04.2017).

3. Козлова О. А., Козлова Л. П. Роботы тоже могут видеть // Известия. 2009. N 10. С. 47–52.

Статья представлена заведующей кафедрой, доктором технических наук, профессором Л. К. Птицыной.

УДК 519.688

ПРОЕКТИРОВАНИЕ ЦИФРОВОЙ ТРЁХМЕРНОЙ МОДЕЛИ РЕЛЬЕФА МЕСТНОСТИ НА ОСНОВЕ СТРУКТУРНЫХ ЛИНИЙ И ВЫСОТНЫХ ОТМЕТОК

А. В. Ершов, А. О. Цанян

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Для цифровой трёхмерной модели рельефа, заданного структурными линиями и высотными отметками, вводится новый тип ограничений, позволяющий более полно учитывать влияние горизонталей на форму рельефа. Предлагается эффективный алгоритм построения цифровой трёхмерной модели на основе триангуляции с ограничениями данного типа.

цифровая трёхмерная модель рельефа, триангуляция, слабые ограничения, сильные ограничения.

Важным объектом исследования современных геоинформационных систем является земной рельеф. Как правило, рельеф задается нерегулярными наборами высотных отметок и структурных линий, которые получаются с помощью методов дистанционного зондирования или векторизации картографических материалов. Высотные отметки обычно представляют локальные экстремумы и другие характерные точки рельефа. Структурные

линии определяют множества точек с резким изменением наклона рельефа (границы оврагов, обрывов, береговые линии) или одинаковыми высотами (горизонтали, изолинии), т. е. накладывают дополнительные ограничения на форму рельефа. Все линии задаются наборами узловых точек и для прощения дальнейшей обработки считаются ломаными.

Важнейшая задача при работе с рельефом заключается в построении его цифровой трёхмерной модели (ЦТМР), т.е. цифрового представления с помощью прямоугольной или треугольной сетки, в узлах которой заданы высоты. Цифровая трёхмерная модель позволяет получать производные данные как для анализа, так и для построения ортофотопланов местности на основе космо- и аэроснимков.

При задании рельефа наборами точек и линий построение его цифровой трёхмерной модели на основе треугольной сетки включает два шага [1].

На первом шаге по проекциям всех исходных высотных отметок и узлов структурных линий на плоскости XOY строится триангуляция Делоне. Задание высот в вершинах триангуляции определяет систему пространственных треугольников – простейшую кусочно-линейную поверхность, интерполирующую рельеф.

На втором шаге производится перестроение триангуляции, позволяющее включить в модель рельефа все структурные линии. Каждая линия должна целиком располагаться на интерполяционной поверхности, поэтому необходимые условия перестроения (ограничения триангуляции) формулируются очень просто: каждый отрезок структурной линии должен совпадать с одним из ребер сетки пространственных треугольников. Далее ограничения этого типа будем называть *слабыми*.

Способ включения отрезка структурной линии, не вошедшего в начальную триангуляцию Делоне (рис. 1*а*), зависит от дополнительных требований к ЦТМР. Если необходимо, чтобы сетка на *XOY* всегда оставалась триангуляцией Делоне, то отрезок нужно разбить на несколько частей. Точки разбиения станут новыми вершинами триангуляции, а каждая часть отрезка – ребром треугольника (рис. 1*б*). Если в качестве вершин треугольной сетки можно использовать только исходные точки, то начальную триангуляцию Делоне нужно перестроить так, чтобы каждый отрезок исходной линии стал ребром сетки (рис. 1*в*).

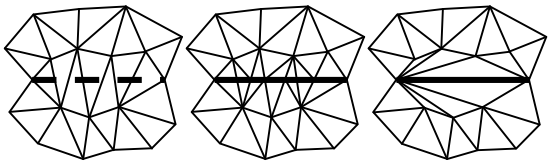
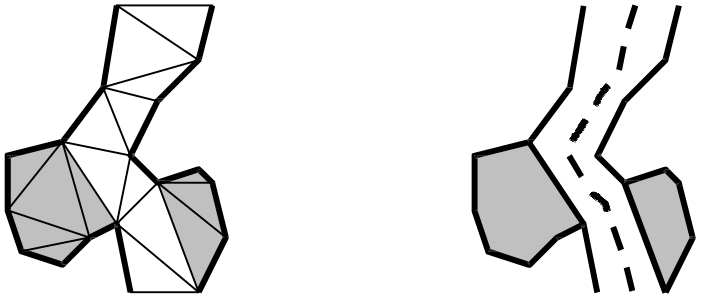


Рис. 1. Включение отрезка: а) начальная триангуляция; б) отрезок разбивается на части; в) отрезок становится ребром

Учет слабых ограничений при построении модели рельефа является необходимым, но недостаточным, если набор структурных линий содер-

жит горизонтали [2]. Чтобы в этом убедиться, нужно на треугольной сетке со слабыми ограничениями рассчитать изолинии с шагом изменения высоты в два раза меньшим, чем у исходных горизонталей (рис. 2). Из-за наличия в триангуляции горизонтальных треугольников (заштрихованных), все вершины которых лежат на одной изолинии, на исходных уровнях появятся паразитные линии, а на промежуточных уровнях линии окажутся чрезмерно спрямленными.



а) б)

Рис. 2. Изолинии на треугольной сетке со слабыми ограничениями (выделены горизонтальные участки модели рельефа): а) исходные; б) расчетные

Если набор исходных структурных линий содержит горизонтали, то интерполяционная поверхность должна не только полностью включать эти линии, но и удовлетворять следующим естественным ограничениям [3]:

1. Точки изолинии не могут быть локальными минимумами или максимумами поверхности.

2. Изолиния не должна быть границей горизонтального участка поверхности, для выделения плоских участков рельефа нужно использовать структурные линии других типов (граница промышленной зоны, береговая линия озера).

3. Любая исходная отметка, высота которой совпадает с уровнем какой-либо изолинии, должна быть либо вершиной исходной горизонтали, либо являться вырожденной изолинией из одной точки.

4. Любой горизонтальный отрезок, соединяющий вершины изолиний одного уровня и целиком лежащий на поверхности, должен либо совпадать с отрезком изолинии (и, следовательно, ребром сетки), либо соединять конечные вершины одной или двух горизонталей.

5. Если некоторая линия начинается и заканчивается на изолиниях соседних уровней z_A и z_B , $z_A < z_B$, не пересекает структурных линий и целиком лежит на интерполяционной поверхности, то в любой ее внутренней точке M должно выполняться условие $z_A < z_M < z_B$.

В соответствии с данными требованиями введем *сильные ограничения* триангуляции [3]:

на треугольной сетке выполняются слабые ограничения;

высотная отметка, которая не является узлом структурной линии, но имеет такую же высоту, как некоторая изолиния, считается вырожденной изолинией, содержащей одну конечную точку;

любое горизонтальное ребро пространственной триангуляции, соединяющее вершины изолиний, либо совпадает с отрезком изолинии, либо соединяет конечные вершины одной или двух изолиний.

Такие ограничения гарантируют отсутствие плоских горизонтальных участков на уровнях исходных горизонталей.

Построение треугольной сетки, удовлетворяющей сильным ограничениям, нужно начинать с триангуляции со слабыми ограничениями. Эта триангуляция может содержать горизонтальные ребра, на которых сильные ограничения не выполняются (для краткости будем называть такие ребра *недопустимыми*). Все треугольники, содержащие одно, два или три недопустимых ребра, необходимо перестроить, однако предварительно следует убедиться, что высоты исходных линий и точек определены корректно.

Алгоритм проверки сильных ограничений триангуляции. Предполагается, что по исходному набору точек и линий построена триангуляция со слабыми ограничениями [3].

Шаг 1. Проверка всех треугольников сетки, выделение и отметка всех недопустимых ребер.

Шаг 2. Перестроение всех треугольников с тремя недопустимыми ребрами.

Шаг 3. Цикл, пока есть цепочки треугольников с недопустимыми ребрами:

– обработка очередной цепочки,

– вычисление новой точки М и включение ее в триангуляцию.

Конец алгоритма

Предложенный в статье новый тип сильных ограничений триангуляции позволяет более полно учитывать влияние горизонталей на форму рельефа. Эффективный алгоритм построения триангуляции с сильными ограничениями обеспечивает получение кондиционной цифровой трёхмерной модели рельефа в автоматическом режиме.

Список используемых источников

1. Скворцов А. В. Триангуляция Делоне и ее применение. Томск : Изд-во Том. ун-та, 2002. 128 с.

2. Препарата Ф., Шеймос М. Вычислительная геометрия. Введение: пер. с англ. М. : Мир, 1989. 478 с.

3. Костюк Ю. Л., Фукс А. Л. Предварительная обработка исходных данных для построения цифровой модели рельефа местности // Вестник ТГУ. 2003. № 280. С. 281–285.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.382.4+004.457+004.453.4

МИКРОКОМПЬЮТЕР RASPBERRY PI (3 MODEL B) И ПРАКТИЧЕСКИЕ ПЕРСПЕКТИВЫ ЕГО ИСПОЛЬЗОВАНИЯ

А. Жаркимбекова, А. Б. Оспанова, Х. М. Сагиндыков, Б. Р. Сауанов, Б. И. Тулеуов

Евразийский национальный университет им. Л. Н. Гумилева

В работе описан завоевывающий все большую популярность среди разработчиков и пользователей одноплатный миникомпьютер Raspberry Pi. Описаны основные необходимые аппаратно-программные компоненты для запуска и организации работы компьютера, а также для расширения возможностей его использования (для последней на данный момент модели Raspberry Pi 3 Model B). Рассмотрены примеры проектов и источники, посвященные Raspberry Pi.

Дан алгоритм по сборке мобильного устройства на его основе и установке программного обеспечения, приведены соответствующие практические рекомендации. Описаны некоторые перспективы по использованию Raspberry Pi.

Raspberry Pi, (одноплатный) микрокомпьютер, платы расширения, аппаратные модули.

Raspberry Pi – это хорошо известный одноплатный бюджетный компьютер, набирающий популярность среди разработчиков в мире благодаря своим особенностям (рассмотрен Raspberry Pi 3 Model B – [1]):

– маленькие размеры платы, обладающей, при этом внушительными характеристиками, достаточными для многих задач: процессор с четырмя ядрами, 1 Gb ОЗУ, встраиваемая память (*MicroSD*), адаптеры беспроводной сети, разъемы для комплектации дополнительными устройствами (USB, GPIO, HDMI, др.) и т. п.

– возможность создания или приобретения плат расширения, предоставляющих новые пути разработчикам: платы с более мощными видео- и звукоадаптерами; поддержкой видеокамер и других периферийных уст-

ройств; платы с блоками питания, обеспечивающими портативность устройства; платы расширения типа Arduino, обеспечивающие широкие возможности конструирования и робототехники.

– доступность различных, в том числе «облегченных», операционных систем, загружаемых с ISO-образа, делает устройство незаменимым в обучающих, исследовательских, экспериментальных целях. Являясь полноценным компьютером с поддержкой многих популярных операционных систем, Raspberry Pi позволяет создавать разноплановое программное обеспечение.

– возможность практически мгновенно сменить операционную систему.

– Raspberry Pi поддерживает разрешение FullHD 1920×1080 (1080 p).

Другие существующие одноплатные микрокомпьютеры со схожими аппаратными возможностями; имеющиеся на рынке различные платы расширения и периферийные устройства, а также рекомендации и инструкции по созданию собственных печатных плат с микросхемами; источники, где предлагаются различные готовые платы расширения; некоторые примеры проектов на основе RP и использованные конфигурации, операционные системы для данных компьютеров, а также задачи, стоящие в перспективе, источники, ссылки и другие материалы приведены в [2].

Далее на рис. 1 представлена структурная схема Raspberry Pi 3B, описание элементов в таблице. Аппаратные интерфейсы устройства и их спецификации подробно рассмотрены в источниках [3, 4, 5].

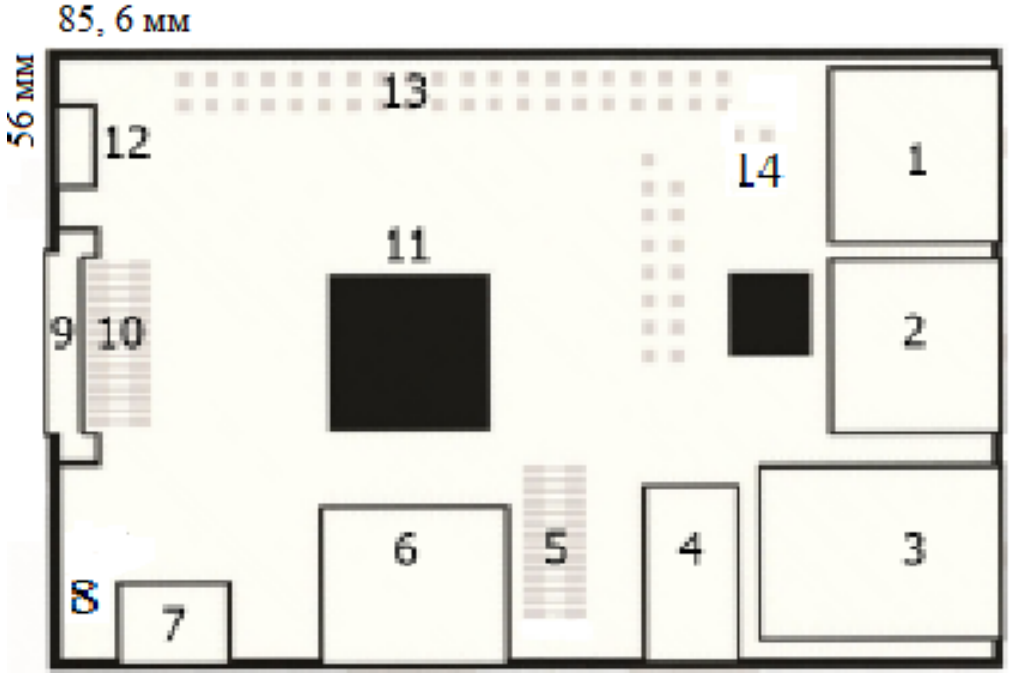


Рис. 1. Структурная схема Raspberry Pi 3B

ТАБЛИЦА. Элементы на плате Raspberry Pi 3B и их описание (см. рис. 1)

№	Элемент и описание
1, 2	Порты USB 2.0 (по 2). Эти 4 разъема позволяют подключать клавиатуру, мышь, внешние накопители, например, USB-флеш
3	Сетевой интерфейс Ethernet 10/100 Mbps с выходом на стандартное гнездо 8P8C (RJ45). Разъем позволяет полноценно работать с сетью
4	Совмещенный аналоговый аудиовыход и композитный видеовыход RCA Video/Audio Jack 3.5 мм 4 pin, к которому можно подключить, например, телевизор без HDMI входа
5	Разъем для подключения видеокамеры MIPI CSI-2
6	Цифровой видеовыход HDMI, позволяет подключается к устройству отображения информации – монитору или телевизору
7	Электропитание Micro USB(<=2,5A)
8	LED-индикаторы питания и чтения карты памяти
9	Разъем для подключения DSI дисплея
10	Слот для MicroSD HC карты памяти. Другие модели поддерживают стандарты SD/MMC/SDIO
11	Однокристальный чип Broadcom BCM2837 Quad Core – 4-хядерный процессор ARM v8 Cortex-A53 (версия архитектуры v8), разрядность 64bit, частота 1,2 GHz (на 50 % быстрее Pi 2), оперативная память 1 Gb, LPDDR2-900 SD RAM
12	Встроенный модуль (антенна) Wi-Fi 802.11n и Bluetooth спецификации 4.1 с поддержкой технологии Bluetooth Low Energy (BLE)
13	Интерфейс ввода/вывода общего назначения (GPIO) 40 контактов. Включает интерфейсы UART, I2C, SPI, I2S, линии 3.3v, 5v, GND, ШИМ, GPCLK
14	Отверстия для монтажа разъема RUN

Возможные конфигурации. Необходимые аппаратно-программные комплектующие для запуска и организации работы компьютера

Минимальный набор. Для полноценной работы устройства с запуском операционной системы необходимо:

– Raspberry Pi 3B;
– Зарядное устройство с выходом 2,5A/5V;
– MicroSD карта с предустановленной операционной системой.

На основе данной конфигурации можно, к примеру, собрать маршрутизатор, прокси- или web-сервер. Требуется лишь настроить соответствующее программное обеспечение, устройства ввода-вывода не нужны.

Устройство с экраном, работающее от сети переменного тока. Для создания такого устройства помимо минимального набора, описанного выше, необходимо дополнительно обеспечить один из следующих вариантов:

а) Подключить один из дисплеев, специально разработанных для данного микрокомпьютера.

б) Использовать любой монитор с HDMI-разъемом.

в) Использовать любой монитор с VGA-разъемом и цифро-аналоговый преобразователь HDMI в VGA (обычно выполнен в виде переходника с разъемом HDMI на одном конце и VGA-разъемом – на другом).

В случае а) заметим, что для дисплея в зависимости от его характеристик и используемой операционной системы необходимо будет выполнить некоторые системные настройки. В случае б) также может потребоваться настройка дисплея. Далее описано устройство на базе Raspberry Pi 3B с сенсорным TFT-дисплеем диагональю 3,5 дюйма и операционной системой Kali Linux (рис. 2)).

Мобильное устройство. Для сборки портативного устройства к устройству из предыдущего пункта, собранному по одному из вариантов а)–в), но с дисплеями небольшой диагонали необходимо установить источник дополнительного питания. На рис. 3 представлен один из вариантов локального источника питания – литиевая батарея на 2500 мАч, размещенная на плате с GPIO-разъемом.

Рис. 2 Устройство с TFT-дисплеем

Рис. 3 Локальный источник питания

Создание мобильного устройства для широких целей

Существующая информация по нижеперечисленным пунктам разрознена, часто не актуальна либо попросту отсутствует, либо предлагаемые решения ошибочны: самостоятельный подбор оптимального по цене, содержанию и качеству набора комплектующих к микрокомпьютеру; самостоятельная установка необходимой операционной системы и запуск компьютера (особенно при отсутствии HDMI-дисплея); получение доступа к сетевому соединению по SSH-протоколу, беспроводному интерфейсу и прочие вопросы; установка необходимых драйверов (в частности, для LCD-дисплея); оптимизация рабочего окружения, в том числе установка подходящего для используемого дисплея разрешения экрана и настроек

операционной системы для обеспечения приемлемой скорости работы микрокомпьютера с такими дополнительными устройствами, как LCD-дисплей, аккумулятор и прочее.

Далее кратко опишем процесс создания устройства на основе Raspberry Pi 3B с операционной системой Kali Linux. Более подробное описание и рекомендации приведены в [2]. Отметим, что здесь очень полезным были ресурсы [6, 7, 8].

– Запись образов операционных систем на MicroSD карту.

– Дисплей присоединен посредством GPIO-интерфейса (на рынке имеются также дисплеи с другими способами присоединения к компьютеру).

– Получение доступа к системе для установки драйвера для дисплея и выполнения настроек. Получить доступ к системе можно несколькими способами:

а) подключить HDMI-дисплей;

б) подключить Raspberry Pi 3B через Ethernet-кабель непосредственно к маршрутизатору, для получения динамического IP-адреса и подключения к устройству через SSH протокол;

в) заметим также, что некоторыми разработчиками предлагаются частные решения с использованием специального оборудования, но применять их не рекомендуется ввиду многих сложностей и нецелесообразности.

Отметим здесь, что в случае б) существующие в Интернете инструкции наиболее разрознены и ошибочны. При его реализации для решения проблем с запуском ssh полезен ресурс [7]. Так как обычно такая сеть защищена, то в Headless-режиме без начальной настройки аппарат сам не может активировать беспроводной сетевой интерфейс. О способе его настройки можно узнать по ссылке [8]. Однако, когда отсутствует консольный доступ к аппарату, данный метод не работает; но, имея доступ к разделу с установленной системой, можно решить проблему [2].

– Подготовка системы для работы и установка драйвера для работы дисплея. Использованы рекомендации и разработки, представленные в [6].

– В целях увеличения быстродействия системы можно сменить рабочее окружение на менее ресурсоемкое (использовать оконные менеджеры).

– Некоторые решения возможных проблем приведены в [2].

Отметим здесь также возможность иметь несколько операционных систем, аппаратных комплектующих, в частности, экранов различных размеров в зависимости от текущих задач.

Список используемых источников

1. Официальный сайт Raspberry Pi / URL: https://www.raspberrypi.org/ (дата обращения 11.01.2018).

2. Материалы по Raspberry Pi (обзоры, сборка, настройки, использование) / URL: www.ademi.online.

3. Gay W. Custom Raspberry Pi Interfaces: Design and build hardware interfaces for the Raspberry Pi. – St Catharines, Ontario, Canada, Apress, 2017.

4. Monk S. Cookbook by Raspberry Pi. – United States of America, O'Reilly, 2016.

5. Soper M. E. Expanding Your Raspberry Pi: Storage, printing, peripherals, network connections for your Raspberry Pi. – Indianapolis (Indiana, USA): Apress, 2017.

6. Latest Kali Linux on Raspberry Pi with Touch Screen, Bluetooth and touch optimised interface (New: Bluetooth, Rogue AP, Remote access AP, more tools) / URL: https://whitedome.com.au/re4son/kali-pi/; https://whitedome.com.au/re4son/sticky-fingers-kali-pi/ (дата обращения 11.01.2018).

7. Kali Raspberry Pi/Headless / URL: https://charlesreid1.com/wiki/Kali_Raspberry_Pi/Headless (дата обращения 11.01.2018).

8. Setting WiFi up via the command line / URL: https://www.raspberrypi.org/ documentation/configuration/wireless/wireless-cli.md (дата обращения 11.01.2018).

УДК 004.7

ПРИМЕНЕНИЕ ПРОГРАММЫ LABVIEW ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ УПРАВЛЕНИЯ И КОНТРОЛЯ УДАЛЕННЫМ ОБОРУДОВАНИЕМ

И. С. Жихорев

Военная академия связи им. Маршала Советского союза им. С. М. Буденного

Возрастающая информатизация общества повышает значение вычислительной техники в управленческих процессах. Применение возможностей современной вычислительной техники для автоматизации процесса обработки информации позволяет увеличить продуктивность труда, повысить результативность работы и ускорить обмен управленческой информацией.

LabVIEW, виртуальный прибор, автоматизация процессов обработки информации.

Проблема автоматизации рабочих процессов и процессов управления, как средства повышения труда всегда являлась и остается актуальной. На современном этапе автоматизации управления работой наиболее перспективным является автоматизация управленческих функций, установленных непосредственно на рабочих местах операторов и начальников лаборатории. Такие системы получили большое распространение в организационном управлении рабочим процессом под названием автоматизированных рабочих мест.

Автоматизированное рабочее место – это программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. АРМ объединяет программно-аппаратные средства, организующие взаимодействие человека с компьютером, предоставляется возможность ввода информации её вывод (через периферийные устройства) [1].

Создание автоматизированных рабочих мест позволяет эффективно обрабатывать большие массы информации, имеющих определенную структуру, зависящую от особенностей места применения. Это позволяет осуществлять индивидуальный подход к автоматизации именно тех функций, которые осуществляются выбранным для автоматизации рабочим местом. Внедрение автоматизированных рабочих мест позволяет значительно сократить время выполнения работ и повысить их точность.

В настоящее время для автоматизации рабочих процессов все чаще используют не реальные измерительные приборы, а измерительные комплексы, основанные на виртуальных измерительных приборах. В частности, массовое применение нашло программное обеспечение LabVIEW американской фирмы National Instruments, за счёт того, что в отличие от аналогичных программных продуктов, где производится имитация измерительных приборов, в LabVIEW «виртуальные» приборы выполняют реальные измерительные функции. Это позволяет широко использовать данный продукт для постановки лабораторного практикума [2].

Многие современные измерительные приборы построены на основе компьютера, они способны отображать результаты измерений в виде информации на дисплее. Такие приборы, в отличие от виртуальных измерительных приборов, имеют высокую цену, а также ограниченный ресурс эксплуатации в связи с неизбежным износом их деталей. Что делает более предпочтительным использование программного обеспечения LabVIEW.

LabVIEW (*Laboratory Virtual Instrument Engineering Workbench* – среда разработки лабораторных виртуальных приборов) является средой программирования, с помощью которой возможно создавать приложения, используя язык графического программирования, что отличает её от обычных языков программирования, таких как C, C++ или Java. Алгоритм в LabVIEW создается в графической иконной форме, образующей блок-диаграмму, что позволяет исключить множество синтаксических деталей. Компьютер, снабженный встраиваемой измерительно-управляющей аппаратной частью и LabVIEW, составляет полностью настраиваемый виртуальный прибор для выполнения поставленных задач.

Программное обеспечение LabVIEW называются виртуальными приборами (ВП, *virtual instruments* – VI), так как они функционально и внешне подобны реальным (традиционным) приборам.

Виртуальный прибор состоит из трёх основных частей:

– лицевая панель (*Front Panel*) представляет собой интерактивный пользовательский интерфейс виртуального прибора и имитирует лицевую панель традиционного прибора (рис. 1). На ней находятся кнопки, графические индикаторы и другие элементы управления, которые являются средствами ввода данных со стороны пользователя;

– выходные данные из программы. Пользователь вводит данные, используя устройства ввода информации, а затем видит результаты действия программы на экране монитора;

– блок-диаграмма (*Block Diagram*) является исходным программным кодом ВП, созданным на языке графического программирования G (рис. 2).

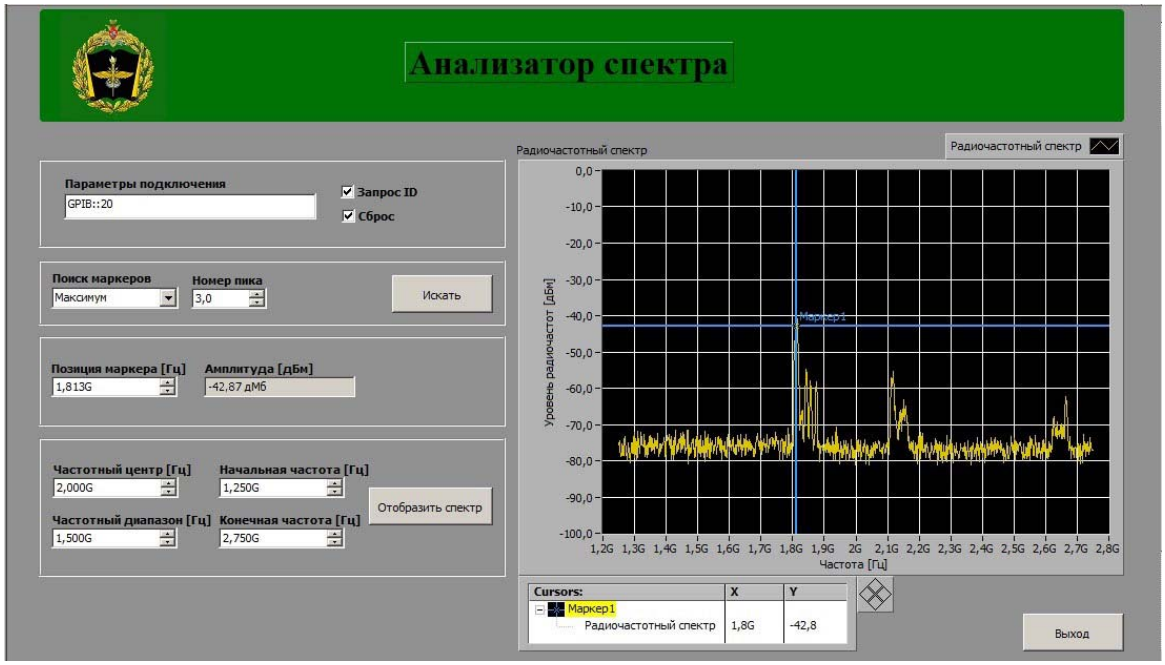


Рис. 1. Лицевая панель виртуального прибора «Анализатор спектра» реализованная в среде графического программирования LabVIEW

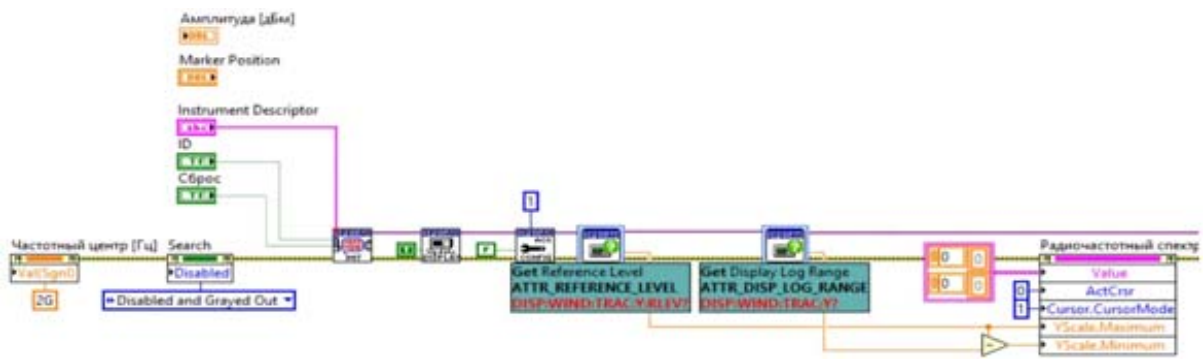


Рис. 2. Блок-диаграмма виртуального прибора «Анализатор спектра» реализованная на языке графического программирования G

Блок-диаграмма представляет собой реально исполняемое приложение. Компонентами блок-диаграммы являются: виртуальные приборы более низкого уровня, встроенные функции LabVIEW, константы и структуры управления выполнением программы [3].

Особенностью программного обеспечения LabVIEW является наличие специальных библиотек для ввода/вывода данных со встраиваемых аппаратных средств, возможность работы с каналом общего пользования, управление устройствами через последовательный порт RS-232, наличие программных компонент для анализа, представления и сохранения данных, взаимодействие через сети и Internet.

Такие особенности дают возможность интегрировать LabVIEW с другими программными средами, например, со специализированным математическим пакетом MATLAB.

Список используемых источников

1. ГОСТ 8.322-78. Государственная система обеспечения единства измерений. Генераторы сигналов измерительные. Методы и средства поверки в диапазоне частот 0,03–17,44 ГГц.

2. Евдокимов Ю. К., Линдваль В. Р., Щербаков Г. И. LabVIEW для радиоинженера: от виртуальной модели до реального прибора. Практическое руководство для работы в программной среде LabVIEW. М. : ДМК Пресс, 2007. 400 с.

3. Федосов В. П., Нестеренко А. К. Цифровая обработка сигналов в LabVIEW: учебное пособие / Под ред. В. П. Федосова. М. : ДМК Пресс, 2007. 456 с.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.4'272

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ МУЛЬТИМЕДИЙНОЙ ПЛАТФОРМЫ UNITY3D

Р. А. Земсков, А. С. Шершнёв
Военная академия связи им. Маршала Советского Союза С. М. Буденного

Unity3D – кроссплатформенный профессиональный игровой движок, который очень популярен в последние годы. Его графические, аудио и видео ресурсы, освещение, физические эффекты могут имитировать реальную окружающую среду, благодаря чему пользователь чувствует себя более погруженным, что соответствует высоким оценкам игровых дизайнеров. Помимо игровой индустрии, продукты, выпускаемые с помощью платформы Unity3D используются в различных аспектах жизни. В этой

статье было изучено применение Unity на 3D-дисплее, виртуальном роуминге и системах моделирования.

unity3D, кроссплатформенный игровой движок, системы моделирования, виртуальный роуминг.

Уже долгое время игры являются очень популярной индустрией в стране и за рубежом. С непрерывным развитием технологий виртуальной реальности и повышением требований к реалистичности игровых миров, появляется необходимость в более профессиональных игровых движках, одним из которых стал Unity3D. Это комплексный профессиональный кроссплатформенный игровой движок, разработанный Danish Unity Technologies, способный создавать 2D и 3D видеоигры, виртуальные конструкции, 3D-анимацию в реальном времени и другие типы замечательных продуктов интерактивного эффекта. В настоящее время, последняя официальная версия Unity3D все еще улучшается и каждое обновление значительно повышает её производительность. Движок имеет простой интерфейс, дружественную рабочую среду, высокую совместимость сформированных проектов на разных платформах, таких как Mac, Windows, Android, IOS, Web, Flash и т. д. Графические рендеринг DirectX и OpenGL сильно оптимизировали, что предоставило возможность создания высококачественных 3D-систем и реалистичные визуальные эффекты, благодаря которым движок пользуется большим спросом среди разработчиков игр и персонала IT-индустрии.

Применение 3D-дисплея

Самый прямой и интуитивно понятный способ представления продуктов – это физический показ перед клиентом. Тем не менее, по мере развития технологий, увеличения объемов информации и требований заказчиков этот старый метод не может полностью удовлетворить клиентов. Теперь основное направление отображения - использование графических изображений с текстом, но в основном это двумерная статичная форма, в которой действие внешнего вида продукта и характеристики неадекватны [1]. Трехмерный дисплей может не только всестороннее охарактеризовать продукт и усилить интуитивное понимание его внешнего вида, но и может позволить клиенту расширить точку зрения, что недоступно для двумерного варианта. 3D дисплей по сути является примером использования продуктов виртуальной реальности. Обычно в программном обеспечении для 3D-моделирования, таком как 3D Max или Maya, создают модели и соответствующие анимации, которые впоследствии экспортируют как файлы FBX. Затем файлы импортируют в проект Unity3D и используя скрипты

на таких языках, как C#, javascript отображают пользовательский интерфейс и анимацию [2].

Приложения могут включать интерактивные презентации продуктов, использоваться для обучения, пояснять принцип работы и т. д.

Применение виртуального роуминга

Виртуальный роуминг – важная отрасль технологии виртуальной реальности, посредством которой каждый может перенестись в любую точку мира. Человек будто оказывается перед зеркалом с картой, на которой выбирает любую страну, и она во всей красе предстает перед ним. Данная технология представляет собой очень захватывающую и интерактивную идею, быстро развивающуюся в игровой сфере, туризме, строительстве, медицине и многих других отраслей промышленности. Типичным аспектом виртуального роуминга является возможность создания виртуальной архитектуры, которая представляет собой объединение технологии построения виртуальных сцен с технологией виртуального роуминга. Виртуальный роуминг широко применяется при создании больших сцен: города, улицы, достопримечательности, игровые сцены и т. д. Он делится на вид от первого лица и вид от третьего лица [3].

Виртуальный роуминг от первого лица в основном применяется при необходимости просмотра сцен и в FPS играх. Он может применяться в виртуальном туризме по смоделированным сценам реальных ландшафтов, что избавляет пользователей от необходимости покидать дом для путешествий по миру.

При виртуальном роуминге от третьего лица пользователи могут четко наблюдать за протагонистом с устройствами ввода, получая улучшенную интерактивность. Это используется в различных игровых сценах, таких как RPG (*Role-playing Game*), Action играх, приключенческих играх, шутерах от третьего лица, Fighting играх, спортивных играх, гонках и т. д.

Применение систем моделирования

С быстрым развитием военных и научно-технических симуляторов возникла необходимость в методах разработки различных видов сложных систем, особенно в аэрокосмической области. Разработка методов моделирования технологий в автомобильных и спутниковых отраслях незаменима и может принести высокую экономическую выгоду. Симуляция означает повторение физических характеристик процессов в системе с использованием моделей и позволяет изучить существующую или экспериментальную систему. Когда система является дорогостоящей, возникают большие риски при её экспериментальных исследованиях, в связи с чем, нужно знать о последствиях вызванных изменением параметров системы в тече-

ние длительного времени, здесь на помощь приходит симуляция. Симуляционный эксперимент в системах моделирования, созданных движком Unity3D, может ускорить процесс развития и принести большие социальные и экономические выгоды. В авиационной промышленности, технология моделирования может ускорить проектирование воздушных судов, сокращая время разработки на 20 %. Пилоты могут использовать симулятор для обучения пилотированию, не ограничиваясь местами и климатическими условиями, что в свою очередь может сэкономить много топлива и финансовых средств.

Другим важным преимуществом является безопасность. Смоделированный эксперимент в аэрокосмической промышленности может уменьшить количество живых тестов на 80 %. В электроэнергетике использование смоделированной системы для отладки, обслуживания и устранения неисправностей атомной электростанции, может сэкономить много трудовых, материальных и финансовых ресурсов. Современные технологии моделирования применяются не только в области традиционной техники, но и широко используются в обществе, экономике, биологии и других областях, таких как городское планирование, управление транспортным потоком, использование ресурсов, борьба с загрязнением, рыночный прогноз, анализ и прогноз мировой экономики, контроль населения и т. д. Некоторые области довольно трудно экспериментировать на реальных системах, использование технологии моделирования в таких случаях имеет более важное значение [4].

Применение в других аспектах

В других аспектах применение приложений на Unity так же велико. Например, система виртуального образования, основанная на Unity3D, может использовать обширные коллекции доступных графических, аудио-, видео- и анимационных обучающих материалов, и в конечном итоге будет полезна учителям и студентам.

Симуляция чрезвычайных ситуаций, таких как землетрясение, цунами, тайфун, огонь и прочее может предотвратить катастрофу и сократить количество жертв.

Список используемых источников

1. Lebo NiPeng Qi, Lina Yu, Wang Jing. Research and Application of the Virtual Display Technology based on Unity3D Products. Digital technology and 1216 application, 2010, 09, pp. 54–55.

2. Xingjie Wang, Chunhua Li. 3D Virtual City Research and Application Based on Unity3D Platform. Computer technology and development, 2013, 2013 (23), pp. 241–244.

3. Jinmin Liu, Tieming Ma, Na Wang. Motor Show Virtual Simulation Platform Design based on Unity3D. Journal of heilongjiang August first land reclamation university, 2014, 01 (26), pp. 66–68.

4. Сайт фирмы-производителя платформы Unity3D. URL: https://unity3d.com/ru (дата обращения 28.01.2018).

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.8

ИСПОЛЬЗОВАНИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В УПРАВЛЕНИИ ВОЕННОЙ СВЯЗЬЮ

Р. А. Земсков, А. С. Шершнёв

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Система поддержки принятия решений – компьютерная автоматизированная система, целью которой является помощь людям, принимающим решение в сложных условиях для полного и объективного анализа предметной деятельности. Системы поддержки принятия решений возникли в результате слияния управленческих информационных систем и систем управления базами данных.

системы поддержки принятия решений, военная связь.

Все процессы в военной сфере, как известно, происходят под управлением со стороны оргштатных структур. Деятельность таких структур направлена на установление ограничений как по временным, так и по материальным ресурсам.

Сам процесс управления реализуется в системе, которую принято называть системой управления. В состав данной системы входят следующие элементы [1]:

органы управления,

контроль состояния объекта,

передача информации между элементами.

Поэтому, в составе системы управления можно выделить отдельный элемент, предназначением которого является помощь органами управления наилучших решений. Таким элементом выступает информационная система.

В зависимости от решаемых задач, выделяют три основных вида информационных систем:

1) Информационно – поисковые системы.

2) Интеллектуальные информационные системы.

3) Экспертные информационные системы.

Наибольшую популярность приобрели информационно – поисковые системы, так как они производят поиск и выборку приоритетных данных в базах данных специального назначения с использованием конкретного языка и правил поиска.

Интеллектуальные информационные системы по назначению можно отнести к системам поддержки принятия решений, так как данный вид информационных систем предназначен для помощи пользователю, принимающему решения, в использовании документов, моделей и знаний формировать соответствующие решения.

Экспертные системы в своём составе содержат механизм «интеллектуальности», который совершенно отличается от систем, описанных выше. Дело в том, что в информатике экспертные системы рассматриваются совместно с базами знаний как модели поведения экспертов в определённой области знаний с использованием процедур логического вывода и принятия решений, а базы знаний – как совокупность фактов и правил логического вывода в выбранной предметной области деятельности [2].

В качестве примеров данных систем, можно выделить следующие программные продукты:

MYCIN – система наблюдения за больным, при различных бактериальных инфекциях;

HASP/SIAP – система, позволяющая определить тип и местоположение корабля, анализируя данные акустических систем слежения;

CLIPS – система для разработки экспертных систем, опираясь на модель знаний;

OpenCyc – динамическая, глобальная экспертная система, позволяющая решать задачи в области искусственного интеллекта на основе человеческого мышления и логических выводов.

Результат создания таких систем, перед которыми ставится задача анализа и моделирования процессов опирающихся на математическое моделирование, позволил выделить данные системы в отдельный класс – системы интеллектуальной поддержки принятия решений (*Decision of Intellectual Support System* – DISS), которые являются элементом отдельного вида информационных систем – систем поддержки принятия решений (*Decision Support System* – DSS).

Для создания и внедрения систем поддержки принятия решения в интересах управления военной связью необходимо описать следующие этапы: 1) Актуальность создания. 2) Описание принципов создания. 3) Основные функции. 4) Описание состава и архитектуры. 5) Определение этапов создания и эффекта от внедрения.

При описании актуальности, необходимо взять во внимание следующее. В составе системы управления военной связью есть такой элемент, задача которого – оказывать помощь в принятии правильных решений, опираясь на анализ и обработку информации об обстановке и состоянии систем связи.

В качестве такого элемента управления связью может выступать информационная система, с наибольшим коэффициентом эффективности. Таким коэффициентом обладает отдельный вид информационных систем – системы интеллектуальной поддержки принятия решений, позволяющие производить синтез и анализ процессов военной связи на основе методов математического моделирования в интересах формирования рациональных вариантов их организации или управления ими.

Для более полного и информативного описания принципов создания систем поддержки принятия решения, следует описать алгоритм функционирования или алгоритм работы, который основывается на моделях, описывающих процессы анализа и синтеза систем военной связи. Все элементы, составляющие комплекс, должны придерживаться одной цели, либо определение коэффициентов эффективности при рассмотрении моделирования процесса связи, либо нахождения максимального показателя эффективности при оптимизации работы системы связи в целом. Каждый отдельный элемент системы должен свободно функционировать с другими элементами данной системы, а также иметь общее представление о входных и выходных параметрах.

Программное и информационное обеспечение системы поддержки принятия решений должно выбираться в зависимости от данных, используемых в моделировании и решении задач синтеза и переработки данных систем военной связи определённого звена управления, а также в зависимости от информации справочного характера. Информационное и программное обеспечение должно иметь однообразную структуру данных, для обеспечения простоты работы с базой знаний.

Из основных функций системы поддержки принятия решения можно выделить:

1) Обеспечение эффективности процессов военной связи при разных способах её реализации;

2) Оптимизация при создании системы связи для определённых условий работы.

В состав системы поддержки принятия решения, как минимум должны входить следующие элементы:

1) Программное обеспечение, позволяющее оценивать эффективность решений, принятых в обстановке, с заданными факторами.

2) База знаний или база данных, с подробной информацией об обстановке, средствах связи, боевой технике и противнике в целом, тем самым

предоставляя системе поддержки принятия решений необходимые данные для анализа и создания выборки решений с наилучшими коэффициентами предпочтительности.

3) Интерфейс взаимодействия пользователя с системой, обеспечивающий работу отдельных составляющих системы поддержки принятия решений как единого целого, а также удобство их применения.

Во время разработки системы поддержки принятия решений желательно придерживаться спиральной модели жизненного цикла, а также необходимо учитывать его основные, вспомогательные и организационные процессы.

Эффект же от её внедрения системы поддержки принятия решения на пунктах управления военной связью следует ожидать прежде всего в повышении обоснованности принятия решений на организацию связи при управлении силами, за счёт проработки большого числа возможных вариантов построения системы связи за отведённое на этап планирования боевых действий время, а также за счёт использования алгоритмов прямой или поэтапной их оптимизации.

Список используемых источников

1. Стадниченко С. Ю. Интеллектуальные системы поддержки принятия решения // Молодой ученый. 2010. № 6. С. 61–63.

2. Энгель Е. А. Модели и методы интеллектуальной поддержки при принятии управленческих решений // Вестник СибГАУ. 2011. № 4. С. 106–112.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 519.7

СОХРАНЕНИЕ СТРУКТУР В СИСТЕМАХ УПРАВЛЕНИЯ

О. И. Золотов, Н. Р. Якубова

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

Обычно система автоматического управления проектируется исходя из того, что параметры объектов и регуляторов (операторы, передаточные функции) неизменны. Однако в реальности часто мы имеем дело с изменением этих параметров. В статье рассматривается возможность стабилизации структур объектов и регуляторов, которая позволит улучшить качество работы систем управления. Теорети-

чески доказывается, что стабилизация структур возможна за счет использования универсального принципа обратной связи. Рассмотрены варианты для случаев изменения операторов одного и двух элементов. Введено понятие приращения структуры, при этом рассмотрен только аддитивный вариант.

структура, управление, сохранение, обратная связь.

В системах автоматического управления в основном используется принцип обратной связи или управление по отклонению. При этом управляется (или стабилизируется) выходная координата объекта.

Обычно в классических системах автоматического управления априори принималось, что уравнение объекта управления и регулятора неизменны, т. е. неизменны их структуры.

С увеличением сложности объектов, а часто и их уязвимости (например, различные сетевые структуры, инфокоммуникационные системы, такие сложные объекты как самолет, ракета и даже обычный автомобиль) возникает дополнительная задача обеспечения стабилизации структуры самого объекта управления.

Таким образом, возникают две задачи: первая привычная задача управления выходными параметрами объекта и вторая дополнительная – это поддержание структуры (оператора, уравнения) объекта.

Сначала рассмотрим, возможно ли хотя бы теоретически поставить и решить такую задачу.

Воспользуемся для этого абстрактной структурной теорией.

Абстрактная теория блочно-структурных схем [1], рассматриваемая совместно с требованиями управленческой парадигмы Мира (УПМ), открывает дополнительные возможности научного поиска. К ним относятся схемное представление и оценочный анализ сохранения структуры как подчинение утверждениям УПМ. Заслуживает внесения в практику исследований возможности наглядных изображений и соответствующих им приёмов отыскания обратных связей, компенсирующих поступающие в структуру возмущения.

Поиск, в частности, включает в себя извлечение и сравнение информаций о конкретных сценариях, подсказываемых УПМ общих закономерностей.

Перейдём к конкретным рассмотрениям.

1. Интересующую нас структуру, рассматриваемую в отсутствии возмущений и стабилизирующих её обратных связей, будем отождествлять либо с одиночным блоком R_1, либо с некоторым соединением блоков R_1, R_2, R_3 и т. д.

Итак, пусть вначале имеется невозмущённая структура – некоторый блок R_1 (рис. *а*). В результате поступающего возмущения структура, представляемая блоком R_1, строго говоря, разрушается и замещается некоторой

новой структурой, отождествляемой с отличающимися от R_1 блоком $\hat{R}_1$. Для примера будем ограничиваться лишь случаями, когда $\hat{R}_1$ отличается от R_1 на малый аддитивный объект, характеризуемый своим оператором $R_{1\varepsilon}$, т. е.

$$\hat{R}_1 = R_1 + R_{1\varepsilon}. \quad (1)$$

В структурном отношении (1), очевидно, означает, что блок $\hat{R}_1$ представляет собой параллельное соединение блоков R_1 и $R_{1\varepsilon}$ (рис. б).

Наша задача – прийти к структурному ви́дению закономерностей УПМ, сохраняющих, невзирая на возмущение $R_{1\varepsilon}$, первоначальный объект, т. е. – блок R_1. Для этой цели замкнём структурную схему рис. *б* обратной связью. Пусть R_{10} – блок цепи (канала) обратной связи. Тогда получим соединение, показанное на рис. *в*. Это соединение нескольких блоков может быть заменено одним блоком с оператором R. Операторное соотношение, связывающее в образовавшейся структурной схеме операторы блоков $\hat{R}_1$, R_{10} и R, запишется в виде:

$$\hat{R}_1 + \hat{R}_1 R_{10} R = R \ . \quad (2)$$

Условимся блок $\hat{R}_1$ представлять как заданный. В этом случае соотношение (2) позволяет рассматривать две задачи.

Первая. Задан блок R_{10} обратной связи. Из (2) необходимо найти результирующий блок R соединения в целом.

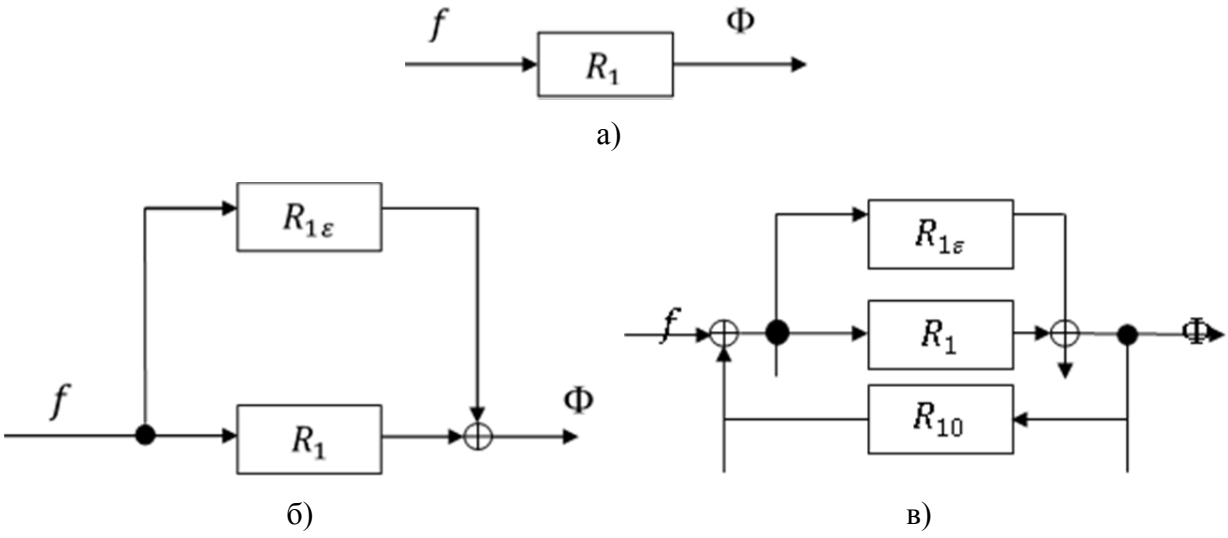


Рисунок. Структуры систем

Это – частный случай традиционной задачи структурной теории: зная структурную схему взаимосвязанных и взаимодействующих блоков и оператор каждого блока в отдельности, найти операторы блоков всех каналов связей – от каждого входа к каждому выходу.

В частности, из (2) устанавливаем выражения для R в следующих двух формах:

$$R = \left(I - \hat{R}_1 R_{10}\right)^{-1} \hat{R}_1 = \left(\hat{R}_1^{-1} - R_{10}\right)^{-1} ,$$

где I – единичный оператор.

Это и есть решение первой задачи.

Вторая. Задан блок R соединения в целом. Из (2) необходимо получить блок R_{10} обратной связи.

Эта постановка – обращение предыдущей – как раз и открывает возможность структурного моделирования механизмов УПМ. В самом деле, сохранение структуры эквивалентно в рассматриваемом случае выполнению равенства:

$$R \equiv R_1. \tag{3}$$

Зададим (потребуем) (3) и подставим (3) в (2). Будем иметь:

$$\hat{R}_1 + \hat{R}_1 R_{10} R_1 = R_1,$$

откуда для блока R_{10} обратной связи получаем:

$$R_{10} = -\hat{R}_1^{-1}\left(\hat{R}_1 - R_1\right)R_1^{-1} = \hat{R}_1^{-1} - R_1^{-1}. \tag{4}$$

Это – решение второй задачи.

Обратная связь (4), очевидно, и является стабилизирующей, т. е. сохраняющей, вопреки наличию оператора возмущения $R_{1\varepsilon}$, соответствующую структуру – блок R_1.

Как и следует ожидать, если возмущения отсутствуют, т. е. $R_{1\varepsilon} \equiv 0$, то в согласии с (1) $\hat{R}_1 \equiv R_1$ и тогда, как видно из (4), и $R_{10} \equiv 0$, т. е. обратная связь (в этом приближении) отключается.

Вновь особо подчеркнём, что мы не фиксировали конкретную природу блоков, и потому получаемые выводы справедливы для сохраняющихся объектов любой природы, в том числе – неживой (и не созданной человеком).

Список используемых источников

1. Золотов О. И., Пустыльников Л. М. Управленческая парадигма мира: монография. СПб. : СПбГУТ, 2012. 416 с.

УДК 004.5

МЕТОДИКА КИБЕРНЕТИЧЕСКОЙ УСТОЙЧИВОСТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ТАРГЕТИРОВАННЫХ КИБЕРНЕТИЧЕСКИХ АТАК

Д. А. Иванов, М. А. Коцыняк, О. С. Лаута, И. Р. Муртазин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматривается комплекс мероприятий по изучению воздействия таргетированной кибернетической атаки на элементы информационно-телекоммуникационной сети и проведение логико-вероятностный метода оценки опасности таргетированной кибернетической атаки, позволяющий выбрать вариант защиты элементов информационно-телекоммуникационной сети.

таргетированная кибернетическая атака, воздействие, уязвимость, информационно-телекоммуникационная сеть, метод анализа иерархии.

По мнению специалистов, в последнее время наблюдается смещение акцента с написания вредоносных программ на проведение таргетированных кибернетических атак (ТКА). Атаки направленны на определенную организацию, и подготовка к ним занимает много времени. Противники тщательно изучают используемые у потенциальной жертвы средства защиты и находят нужные уязвимости, которые используются для проведения атаки. Сегодня известно о более чем ста проводящих таргетированных кибернетических атак. От из действий страдают государственные и коммерческие структуры в 85 странах. Такой широкое распространение объясняется оптимизацией средств взлома, что проводит к упрощению и удешевлению проведения вредоносных операций.

Высокая сложность их обнаружения и колоссальный урон от их действий, который не гарантированно может быть обнаружен спустя длительный срок. Таргетированная (целевая) кибернетическая атака (ТКА) на элементы информационно-телекоммуникационной сети (ИТКС) реализуется в виде проведения комплекса мероприятий по изучению информационной системы и программного обеспечения [1, 2].

Результатом воздействия ТКА является хищение информации и шпионаж, изменение данных, манипуляция и шантаж, уничтожение данных.

Основными этапами воздействия ТКА является:

1. Поиска (сетевого сканирования).
2. Создания стенда воздействия.

3. Обхода стандартных средств защиты.
4. Поиска (сетевого сканирования).
5. Разработки набора инструментов.
6. Закрепления внутри инфраструктуры.
7. Распределения.
8. Пополнения.
9. Мониторинга и выбор метода достижения цели [3].

При воздействии ТКА на ИТКС затруднительно выбрать способы и средства защиты, так как ресурс ограничен. Одним из путей разрешения является дифференцированный подход к защите ИТКС и ее элементов, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направлений защиты ИТКС и ее элементов, ассиметричных возможностям ТКА, необходимо разработать методику прогнозирования воздействия ТКА противником на ИТКС и ее элементы. В настоящее время отсутствуют методики, предназначенные для этого. С целью прогнозирования предлагается методика прогнозирования воздействия ТКА на ИТКС.

Целью методики является прогнозирование ТКА с учётом места и роли элементов в ИТКС, определение очерёдности воздействия на элементы ИТКС и наиболее опасных ТКА, что, в свою очередь, позволит формировать исходные данные для принятия мер защиты элементов и ИТКС в целом.

Методика предназначена для обоснования принятия решений по защите элементов ИТКС от ТКА должностными лицами на этапах формирования, развёртывания и функционирования ИТКС.

Результатом прогнозирования воздействия ТКА на ИТКС будет матрица назначений ТКА противника на элементы ИТКС, а также очерёдность воздействия на них.

В основу методики положено определение степени опасности ТКА, для чего необходимо рассмотреть физические основы этапов ТКА, особенности их воздействия, характер проявления на элементах ИТКС.

Оценка опасности ТКА на ИТКС вызывает некоторое затруднение, связанное с недостаточной разработкой соответствующего методического аппарата. Для оценки опасности ТКА предлагается использовать логико-вероятностные методы.

Одним из наиболее распространённых логико-вероятностных методов является метод анализа иерархий, который позволяет понятным и рациональным образом структурировать сложную проблему принятия решений в виде иерархии, сравнить и выполнить количественную оценку альтернативных вариантов решения [4]. Поэтому для оценки опасности ТКА для ИТКС предлагается использовать метод анализа иерархий.

За степень опасности ТКА относительно вскрытия элементов ИТКС примем:

– степень воздействия на линию связи;
– степень воздействия на маршрутизатор;
– степень воздействия на коммутатор;
– степень воздействия на персональные электронно-вычислительные машины;
– степень воздействия на сервер электронной почты;
– степень воздействия на сервер базы данных;
– степень воздействия на сервер web.

На основании результатов учитывая идею распределения разноэффективных этапов ТКА по взаимозависимым, с различной степенью важности, элементам ИТКС, виды целевой функции и ограничений, в условия решения задачи, приемлемым методом решения является метод двух функций. Таким образом, разработана методика оценки комплексного информационного воздействия на основе распределения разнородного ресурса по взаимоувязанным элементам ИТКС, которая позволяет определить угрозы ИТКС и обосновать асимметричные им меры защиты.Данный метод позволяет оценить угрозы для элементов ИТКС по уровням эталонной модели взаимодействия открытых систем и на каждом уровне формировать постановку задачи на синтез системы защиты ИТКС в условия воздействия ТКА [3, 5]

Анализ полученных результатов показал, что в первую очередь ТКА будут направлены на линию связи и маршрутизатор, а наиболее часто используемой является ТКА типа «Сканирование сети и ее уязвимостей». Полученные результаты позволяют обосновать дифференцированный подход при выборе варианта защиты элементов ИТКС.

Необходимо отметить, что рассматриваемую задачу, исходя из характера действий ИТКС и принципов планирования, нужно решать для временных «сечений» по этапам функционирования системы управления. В этом случае после каждой смены этапа функционирования необходимо производить уточнение структуры и варианта защиты элементов ИТКС.

Список используемых источников

1. Коцыняк М. А., Лаута О. С., Осадчий С. А. Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика» // Информация и космос. 2013. № 3–4. С. 25–27.

2. Васюков Д. Ю., Коцыняк М. А., Коцыняк М. М., Лаута О. С., Лаута А. С. Устройство обнаружения удаленных компьютерных атак. Патент на изобретение RUS 2540838 от 03.03.2014.

3. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Модель таргетированной кибернетической атаки // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х т. 2017. С. 90–98.

4. Елисеев А. И., Долгов А. А., Хорохорин М. А., Лаута О. С., Набатов К. А. Обеспечение живучести информационных систем (Часть 3. Методы обеспечения и повышения живучести) // Вестник Воронежского института ФСИН России. 2013. № 1. С. 91–94.

5. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 83–89.

УДК 004.056.57

ЭВРИСТИЧЕСКАЯ МОДЕЛЬ ТАРГЕТИРОВАННОЙ КИБЕРНЕТИЧЕСКОЙ АТАКИ

Д. А. Иванов, М. А. Коцыняк, О. С. Лаута, Е. А. Хохлачева

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматривается эвристическая модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть, позволяющая выбрать дифференцированный подход к защите информационно-телекоммуникационной сети и её элементов который заключается в выборе наиболее актуальных направлений защиты.

таргетированная кибернетическая атака, воздействие, синтез системы защиты.

Таргетированная кибернетическая атака на элементы информационно-телекоммуникационную сеть (ИТКС) реализуется в виде несанкционированного активного процесса в инфраструктуре сети, удаленно управляемая в реальном масштабе времени, с целью нарушения или снижения эффективности выполнения технологических циклов [1].

Процесс функционирования комплекса ТКА включает функции:

1. Поиска (сетевого сканирования).
2. Создания стенда воздействия.
3. Обхода стандартных средств защиты.
4. Поиска (сетевого сканирования).
5. Разработки набора инструментов.
6. Закрепления внутри инфраструктуры.
7. Распределения.

8. Пополнения.

9. Мониторинга и выбор метода достижения цели.

Подсистема поиска. Для обнаружения уязвимостей используются специализированные программные продукты, называемые сетевыми сканерами. Принцип работы сетевых сканеров заключается в следующем:

1. Подсистема поиска с установленным сетевым сканером подключается к сети.

2. В заданном диапазоне IP-адресов производится поиск доступных сетевых ресурсов, идентификация сетевых сервисов и первичный анализ их уязвимости.

3. По результатам сканирования автоматически готовится отчет о составе сетевых ресурсов, состоянии защищенности каждого сетевого ресурса, обнаруженных уязвимостях в системе защиты и оценке возможности использования этих уязвимостей для проникновения в систему, который передаётся в подсистему обработки и управления.

Сканирование сетевых ресурсов, автоматическое обнаружение узлов и услуг позволяет собирать информацию обо всех сетевых устройствах, находящихся в исследуемой сети, таких как АРМ, почтовые серверы, межсетевые экраны, маршрутизаторы, серверы удаленного доступа и т. д. Эта функция позволяет составить полную карту работающих в сети активных устройств и активизированных сетевых услуг путём «опроса» сетевых устройств по соответствующим протоколам.

Сканер выполняет проверку всех IP-адресов и портов из заданного диапазона и таким образом строит карту сегмента сети. По созданной карте сегмента сети сканер начинает сбор данных по всем сетевым ресурсам. Подобное исследование сегмента сети значительно увеличивает сетевой трафик, что является одним из признаков проведения сканирования.

Затем анализирует собранную информацию с целью определения базовых параметров (типа операционной системы, включенных сетевых сервисов и т. п.) и потенциальных уязвимостей, обычно присутствующих в настройках ОС и сетевых служб. Сведения об уязвимостях заложены в базу данных сканера в виде правил, которые применяются для каждого конкретного узла из заданного диапазона. В данном случае сканер просто перебирает уязвимости и отмечает степень их потенциальной пригодности к использованию. Этот этап является активным и предполагает достаточно большое количество запросов, посылаемых по сети к каждому исследуемому узлу, но никаких деструктивных действий сканер не производит [2].

Результаты сканирования каждого узла сети представляются в виде отчёта, содержащего сведения об обнаруженных уязвимостях, типе операционной системы, перечне портов и соответствующих им функций.

Данные поступают в подсистему обработки и управления, где определяется оперативно-тактическая принадлежность объектов разведки (объект

вскрывается), а также производится управление функционированием всех подсистем.

Если по результатам обработки указанных данных, было выявлено, что сеть защищена средствами защиты, то реализуется *подсистема создания стенда воздействия ТКА*, в которой создается идентичная версия эксплуатируемого ПО, реализуются этапы проникновения в инфраструктуру сети ИТКС, в обход стандартных средств защиты с помощью скрытого внедрения.

Этот этап является главным переходом между пассивной и активной фазами проникновения в инфраструктуру сети ИТКС [3].

Результаты воздействия представляются в виде отчёта, содержащего сведения об реализации этапов проникновения в сеть. Эффективность функционирования подсистемы создания стенда воздействия можно оценить вероятностью создания ложной системы.

Далее осуществляются активные действия, с этой целью включается подсистемы *обхода стандартных средств защиты* ИТКС. Собранная информация уязвимостей в средствах защиты, позволяет обмануть либо обойти защитные механизмы, которые используют все привилегии легитимного процесса в своих целях, не обращая на себя внимание.

Результаты обхода средств защиты представляются в виде отчёта, содержащего сведенья об обходе защиты, закреплении во взломанной системе и сокрытии следов присутствия. Эффективность функционирования подсистемы обхода стандартных средств защиты ИТКС можно оценить вероятностью скрытия воздействия.

После обхода стандартных средств защиты повторно включается *подсистема поиска (сетевое сканирование)* с целью изучения работы топологии и с учётом структуры сети.

Результаты сканирования каждого узла сети представляются в виде отчёта, содержащего сведения об обнаруженных уязвимостях, типе операционной системы, перечне портов и соответствующих им функций. Эффективность функционирования подсистемы поиска и технического анализа можно оценить вероятностью обнаружения уязвимостей по известным сценариям.

Далее включается *разработка набора инструментов* воздействия на ИТКС.

Реализуя следующие мероприятия:

1. Внедрение вредоносного кода, используя уязвимости в программном обеспечении с целью:

– создания вредоносного кода, который учитывает уязвимости системы;

– закрепления внутри зараженной системы, скрытой автозагрузки;

– обеспечения передачи команд;

– внедрения в легитимный процесс для активизации вируса по шифрованному каналу, либо извлечение и запуск зашифрованной копии вируса с диска.

2. Обеспечение передачи команд подконтрольным вредоносным модулем, с которого собираются результаты работы.

3. Загрузка на инфицированный сервис основного вредоносного модуля ТКА, который может состоять из следующих подмодулей:

– клавиатурного шпионажа, который используется для контроля и записи (регистрации) каждого нажатия клавиш на компьютерной клавиатуре;

– записи деятельности экрана пользователя;

– удаленного доступа, который обеспечивает возможность доступа к файлам и их передачи;

– модуль распространения внутри инфраструктуры, для извлечения информации, срыва или создание помех критическим аспектам выполнения задач, программ или служб;

– шифрования информации на диске;

– очистка следов активности, самоуничтожение;

– чтение локальной почты;

– поиск информации на диске.

Результаты разработки набора инструментов представляется в виде отчёта, содержащего сведения об реализации внедрения вредоносного кода и загрузки вредоносного модуля. Эффективность функционирования подсистемы разработки набора инструментов можно оценить вероятностью распределения средств воздействия.

Закрепление внутри инфраструктуры, осуществляется гарантированным доступом в инфраструктуру ИТКС путем выполнения роли загрузчика, позволяющий загружать вредоносный модуль при включении АРМ и выгружать его при выключении или копировании системной папки загрузчика со следующими атрибутами: системные; скрытые; только для чтения. Запуск осуществляется с помощью сервиса со схожим системным именем, отличающийся одной точкой.

Результаты закрепления внутри инфраструктуры представляются в виде отчёта, содержащего сведенья гарантированного доступа в инфраструктуру. Эффективность функционирования подсистемы закрепления внутри инфраструктуры можно оценить вероятностью поражения и захвата модуля.

Подсистема распределения, осуществляет запуск вредоносного модуля, путем подключения к выбранному АРМ удаленным RDP-клиентом, который используется для обеспечения удаленной работы пользователя с сервером.

Результаты распределения представляются в виде отчёта, содержащего сведенья заражения сети. Эффективность функционирования подсистемы распределения можно оценить вероятностью эффективности воздействия.

В случае отсутствия определенной функции в арсенале, осуществляется этап *пополнения,* который автоматически обновляет модуль.

Завершающий этапом ТКА выполняет *подсистема мониторинга и выбора метода достижения цели.* Имея доступ в инфраструктуре АРМ, реализуется пассивные вредоносные действия, которое не оказывают непосредственное влияние на работу АРМ, но может нарушить ее политику безопасности.

Результаты распределения представляются в виде отчёта о выполнении вредоносного действия [4]. Эффективность функционирования подсистемы мониторинга и выбора метода достижения цели можно оценить вероятностью поражения.

На всех подсистемах осуществляется контроль по сокрытию следов, если присутствие опознано, на любом из подсистем, то выполняется чистка журнала событий.

В случаи если в сети не используются средства защиты, либо они неправильно были настроены пользователем, то реализация ТКА после выполнения подсистемы поиска (сетевого сканирования) приступает сразу к подсистеме разработки набора инструментов воздействия на ИТКС.

После первой успешной реализации для уменьшения времени ТКА, сохраняется файл возврата, для дальнейшей реализации атак с подсистемы мониторинга и метода достижения цели [5].

Из модели видно, что в условиях воздействия ТКА довольно затруднительно выбрать способы и средства защиты ИТКС ОЗУ, так как их ресурс ограничен. Одним из путей разрешения этого противоречия является дифференцированный подход к защите ИТКС ОЗУ и ее элементов, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направлений защиты ИТКС ОЗУ и ее элементов, ассиметричных возможностям ТКА, необходимо разработать модель ТКА. В настоящее время такая модель отсутствует.

Список используемых источников

1. Баранов В. В., Иванов Д. А., Коцыняк М. А., Московченко В. М., Нечепуренко А. П. Применение метода топологического преобразования стохастической сети для моделирования системы воздействия // Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 38–43.

2. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информацион-

ного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 83–89.

3. Елисеев А. И., Долгов А. А., Хорохорин М. А., Лаута О. С., Набатов К. А. Обеспечение живучести информационных систем (Часть 3. Методы обеспечения и повышения живучести) // Вестник Воронежского института ФСИН России. 2013. № 1. С. 91–94.

4. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Модель таргетированной кибернетической атаки // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х т. 2017. С. 90–98.

5. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. 2017. С. 420–425.

УДК 004.056 (075.8)

МЕТОДЫ ВЕРОЯТНОСТНО-ВРЕМЕННОГО МОДЕЛИРОВАНИЯ ПРИ ПРОВЕДЕНИИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Ю. О. Изотова, Д. В. Юркин

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

Вероятностно-временные методы оценки являются инструментом для моделирования процедуры определения временных характеристик вероятностных процессов с конечным числом дискретных состояний. В данной работе приведена реализация метода вероятностно-временного моделирования расчета производящей функции для построения процесса проведения оценки соответствия автоматизированных систем требованиям по информационной безопасности. Вероятностно временной подход также позволяет оценить вероятность успешного выполнения оценки в заданное время.

автоматизированные системы, информационная безопасность, вероятностный граф, производящая функция, весовая функция, путь, контур, преобразование графа, вероятностно-временная методика.

Эффективность применения вероятностного графа для анализа и моделирования дискретной системы событий, по оценке механизмов защиты различных компонент автоматизированных систем (АС) уже была рассмотрена в ряде работ [1, 2]. Математический аппарат вероятностно-временного метода оценки АС ранее был описан [3]. Данная методика позво-

ляет получить вероятностно-временные характеристики обобщенной процедуры проверки АС по установленным требованиям в сфере информационной безопасности, благодаря которой можно получить оценку влияния различных условий и порядок организации проведения испытаний на среднее время выполнения, вероятность успешного завершения в заданное время и трудоемкость тестовых испытаний.

Использование производящих функций при анализе вероятностных процессов с помощью графов упрощает решение задач оценки.

Описать переходы графа можно при помощи производящей функции, выведенной в работе [1] на основе [4].

После определения среднего времени выполнения проверки $\bar{T}$, можно так же определить вероятность успешного выполнения оценки в заданное время $P(T_{exec} \le T)$. Для определения вероятности успешного выполнения применяется метод получения нижней оценки вероятности.

Для этого делается допущение, что решение об успешном или неудачном завершении попытки принимается после анализа последней оценки. Тогда, время ошибочного завершения тестового испытания теряет свойство случайности, и становиться величиной постоянной.

Выражение для нижней оценки $P(T_{exec} \le T)$ целесообразно получить, используя вероятность противоположного события, например, вероятность неудачной проверки в заданное время $P(T_{exec} \le T)$. Величина $P(T_{exec} \le T)$ определяется вероятностью того, что все тестовые испытания в заданный промежуток времени завершаться неудачей:

$$P(T_{exec} \le T) \le (1 - P_1)^K,$$

где K – максимальное количество проверок в заданный промежуток времени, P_1 – вероятность безошибочной проверки всех установленных требований. Следовательно, среднее время вероятности ошибки описывается следующим неравенством:

$$P(T_{exec} \le T) \ge 1 - (1 - P_1)^K.$$

Основываясь на ранее описанной методике моделирования, вероятностно-временная оценка сводится к следующим этапам:

– представление процесса оценки в виде вероятностного графа;

– определение значений производящих функций ребер вероятностного графа;

– вычисление результирующей производящей функции всего вероятностного графа;

– вычисление зависимости среднего времени выполнения от вероятности ошибки оценщика;

– вычисление дисперсии зависимости среднего времени выполнения от вероятности ошибки оценщика.

Моделирование процесса проведения оценки АС на соответствие требованиям ИБ состоит из следующих этапов:

1) Определение состояния вероятностного графа проведения оценки соответствия (рис. 1). Где узловые точки 1–4 соответствуют следующим состояниям: 1 – подготовительный этап; 2 – проведение испытаний оценки; 3 – анализ результатов тестовых испытаний; 4 – отчет по результатам оценки и рекомендации.

Рис. 1. Состояния вероятностного графа

2) Определение переходов между состояниями (рис. 2).

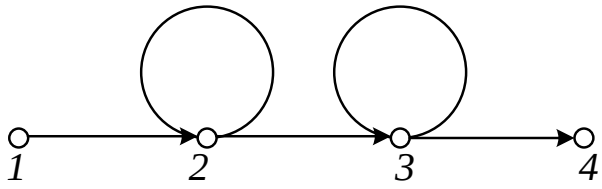


Рис. 2. Определение переходов между состояниями графа

Где значениями переходов являются: переход 1 – 2 – проведение подготовительного этапа; переход 2 – 3 – проведение оценки требований ИБ; переход 2 – 2 – повторное проведение оценки требования ИБ; переход 3 – 3 – повторный анализ результатов оценки; переход 3 – 4 – проведение анализа результатов оценки.

3) Определение весовых функции вероятностного графа согласно формуле производящей функции и в случае расчета среднего времени от вероятности ошибки (рис. 3).

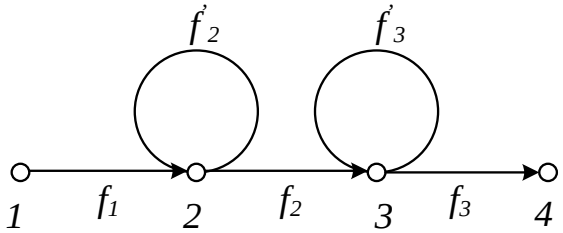


Рис. 3. Определение весовых функций вероятностного графа

$$f_1 = x^{t_1},\ \text{где}\ t_1 = 1,$$

$$f_2 = (1 - p_0)x^{t_2},\ \text{где}\ t_2 = 1,$$

$$f_3 = (1 - p_0)x^{t_3},\ \text{где}\ t_3 = 1,$$

$$f'_2 = 1-[1-(1-p_o)]x^{t_2},$$

$$f'_3 = 1-[1-(1-p_o)]x^{t_3}.$$

4) Вывод результирующей производящей функции всего графа. Полная производящая функция:

$$f_{14} = x^{t_1}\cdot\frac{(1-p_0)x^{t2}}{1-[1-(1-p_o)]x^{t2}}\cdot\frac{(1-p_0)x^{t3}}{1-[1-(1-p_o)]x^{t3}}.$$

Расчет математического ожидания (значения среднего времени выполнения проверки):

$$\overline{T}(p_0) = \frac{dy}{dx}f_{14}\bigg|_{x=1}.$$

Расчет дисперсии среднего времени:

$$D(T) = \frac{dy}{dx}f_{14}\bigg|_{x=1} - \left\{\frac{dy}{dx}f_{14}\bigg|_{x=1}\right\}^2.$$

Графическое построение зависимости среднего времени выполнения оценки от вероятности ошибки.

Согласно результирующей производящей функции и ее производной, график функции среднего времени выполнения оценки от вероятности ошибки – $T(p_0)$ оценщика представлен на рис. 4.

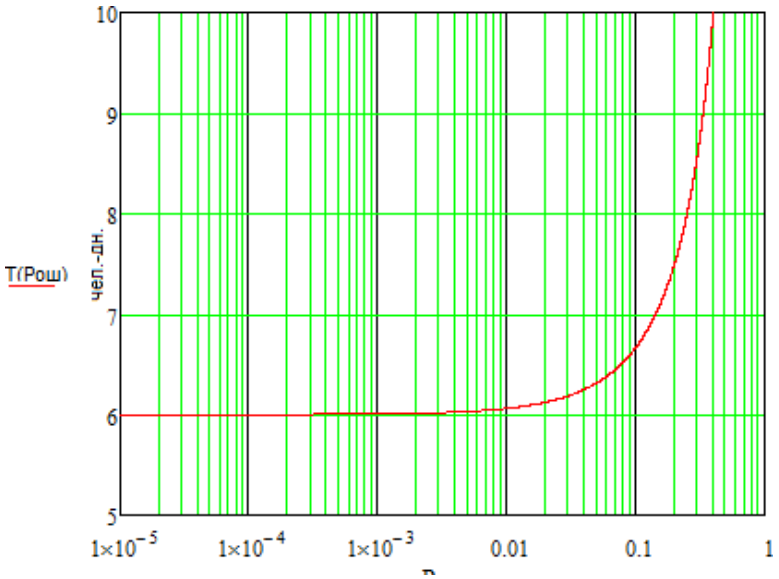


Рис. 4. График зависимости среднего времени оценки от вероятности ошибки

Таким образом, предлагаемый вероятностно-временной метод оценки среднего времени и вероятности ошибки оценщика позволил в программном комплексе Mathcad оценить зависимость среднего времени оценки от вероятности ошибки. Как видно из графика, чем выше среднее время проведения оценки, тем выше вероятность ошибки оценщика. С практической точки зрения, данные результаты говорят о том, что для снижения вероятности ошибки оценщика необходимо снижать время проведения самой оценки. Это возможно достичь за счет увеличения числа специалистов.

Также, можно отметить, что методика определения времени оценки в Национальном стандарте РФ ГОСТ Р ИСО/МЭК 27006-2008 – детерминированная и неполноценна. Несмотря на то, что стандарт отмечает необходимость учета индивидуальности СМИБ, риски ИБ и других факторов, в документе не предложено методики оценки продолжительности с учетом дополнительных факторов. Метод таблицы времени аудитора не позволяет рассчитать среднее время выполнения проверки для случайной проверки, определить вероятность успешной оценки в заданное время или отклонение от среднего времени выполнения оценки.

В связи с указанными недостатками методики ГОСТ Р ИСО/МЭК 27006-2008, предлагается дополнить данный стандарт вероятностно-временной методикой оценки продолжительности проведения оценки аудита.

Предложенная методика дает гибкость и прозрачность во временной оценке, что положительно скажется на точности расчета финансовых и временных затрат аудита. Методика позволит аудиторам лучше планировать свое время, что будет способствовать выполнению взятых перед заказчиком обязательств в срок и, как следствие, улучшению деловой репутации.

Список используемых источников

1. Юркин Д. В., Винель А. В., Таранин В. В. Анализ временных и сложностных характеристик парольной аутентификации в защищенных операционных системах семейства UNIX // Информационно-управляющие системы. 2013. № 3 (64). С. 62–66.

2. Никитин В. Н., Юркин Д. В. Влияние механизмов защиты на пропускную способность каналов с ошибками // Защита информации. Инсайд. 2009. № 3 (27). С. 46–51.

3. Юркин Д. В., Малых А. В. Вероятностно-временные методы оценки соответствия автоматизированных систем требованиям информационной безопасности / Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция (АПИНО 2017) в 4-х т. С. 496–500.

4. Захаров А. И. Анализ систем с переспросом // Материалы семинара по кибернетике. Кишинев, 1968. Вып. 5.

УДК 621.004

О МЕХАНИЗМАХ ДИСКРЕЦИОННОГО РАЗГРАНИЧЕНИЯ ДОСТУПА В ОПЕРАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Ленинградское отделение научно-исследовательского института радио, Санкт-Петербургский филиал

Автоматизированные системы, реализованные с использованием операционных систем специального назначения, обеспечивают защиту различных видов информации от несанкционированного доступа. Использование специальных режимов ограничения прав пользователей в операционных системах специального назначения позволяет построить более гибкий и надежный механизм защиты информации в автоматизированных системах.

автоматизированная система, операционная система специального назначения, защита информации, несанкционированный доступ, дискреционная модель разграничения доступа.

При построении перспективных и модернизации существующих автоматизированных систем (АС) актуальной задачей является использование типовых решений стандартизации аппаратно-программного обеспечения, включая операционные системы, среды разработки программного обеспечения [1]. АС, реализованные с использованием операционных систем специального назначения (ОС СН), обеспечивают защиту различных видов информации от несанкционированного доступа.

ОС СН являются POSIX-совместимыми системами. В качестве реализации дискреционной модели разграничения доступа в ОС СН используется стандарт POSIX ACL (*Access Control Lists* – списки контроля доступа).

Кроме этого стандарта, поддерживаемого большинством UNIX-совместимых систем, ОС СН поддерживают стандарт ACL, специфичный для объектов файловой системы extfs.

Благодаря этому файл, созданный в ОС СН, не потеряет разрешения на доступ, будучи скопирован, например, в файловую систему любой из версий ОС UNIX или других дистрибутивов ОС Linux.

Механизм разрешений на доступ POSIX ACL поддерживается на уровне архитектуры файловой системы ОС СН путем включения стандартных (*Minimal* ACL) и расширенных (*Extended* ACL) атрибутов доступа к каждому файлу и директории.

Благодаря идее владения (*ownership*) пользователи получают возможность устанавливать разрешение на доступ к своим файлам и директориям, разделяя правила доступа для себя и других пользователей.

Согласно минимальной схеме механизма POSIX ACL (*Minimal* ACL) разрешения на доступ к файлу (директории) могут устанавливаться и для групп пользователей. Особенностью группового владения является то, что владелец файла может не являться членом группы, владеющей файлом. Это дает большую гибкость в организации доступа к файлам.

Совместное пользование файлами можно организовать практически для любого состава пользователей, создав соответствующую группу и установив для нее права на требуемые файлы. При этом для того, чтобы пользователь получил доступ к этим файлам, достаточно включить его в соответствующую группу, владеющую файлом.

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу [2, 3].

Эти классы, присущие всем файловым системам ОС UNIX и Linux, следующие:

1. User access (*u*) – доступ для владельца файла.

2. Group access (*g*) – доступ для группы, владеющей файлом.

3. Other access (*o*) – доступ для остальных пользователей (кроме суперпользователя *root*).

Для каждого из этих классов определены три типа разрешений:

1. На чтение содержимого файла (*read*) – символ «*r*».

2. На запись внутри файла или изменения его содержимого (*write*) – символ «*w*».

3. На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора) (*execute*) – символ «*x*».

Пересечение классов субъектов доступа и типов разрешений для конкретных файлов и директорий составляют их минимальный список разрешений на доступ (*Minimal* ACL – *Access Control List*).

Когда пользователь ОС СН регистрируется в пользовательском сеансе, то интерпретатор или рабочий стол использует его идентификаторы uid (пользователя) и gid (группы) и на их основании управляет разрешениями на доступ к файлам (директориям).

При этом пользователи самостоятельно не взаимодействуют с файлами (директориями), а используют для работы с ними программы, выполняющие операции над файлами (директориями) от имени пользователей. Для этого программы наследуют uid и gid пользователей.

В силу этого они не могут получить разрешения на доступ к файлам (директориям), доступ к которым пользователям (или группам) не разрешен.

Например, файл паролей /etc/shadow имеет разрешение на чтение и запись данных в нем только для владельца (администратора ОС СН) и разрешение на чтение для группы (группа *shadow*) и запрет на любой доступ остальных субъектов доступа.

Между тем, с помощью команды passwd любой пользователь может изменить собственный пароль в своей учетной записи файла /etc/shadow.

Следовательно, на момент изменения пользователем собственного пароля команда passwd временно получает разрешения администратора ОС СН на доступ к файлу /etc/shadow.

Такая временная смена разрешений на доступ в рамках Minimal ACL называется сменой режима доступа.

В механизме разрешений POSIX ACL, используемом ОС СН для дискреционного разграничения доступа, используется два специальных режима доступа:

1. suid (*set uid* – установить идентификатор пользователя).
2. sgid (*set gid* – установить идентификатор группы).

Когда для исполняемого файла (программы или сценария интерпретатора) установлен режим доступа suid, он запускается с разрешениями владельца файла, а не с разрешениями пользователя, фактически запустившего этот исполняемый файл.

Аналогично, если для такого файла установлен режим доступа sgid, то файл запускается с разрешениями пользователя, являющегося членом группы, владеющей файлом, а не с разрешениями группы, к которой принадлежит пользователь, запустивший файл.

На рис. 1 показан пример разрешений на доступ команды passwd.

```
root@astra-client:/usr/bin# ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 51685 марта  2  2016 /usr/bin/passwd
root@astra-client:/usr/bin#
```

Рис. 1. Разрешения доступа команды passwd

Вместо разрешения «*x*» (выполнение) владельца команды установлено новое разрешение «*s*», означающее, что для команды passwd установлены как разрешение на выполнение, так и режим доступа suid.

Команда passwd будет запускаться так, как если бы ее запустил администратор ОС СН, а не пользователь, который фактически запустил команду.

И поскольку программа passwd имеет разрешение выполнять запись в поле пароля файла /etc/shadow, пароль будет установлен.

Режимы доступа suid и sgid устанавливаются вместо разрешения «*x*» для владельца файла и группы, владеющей файлом. Если файл является

исполняемым, режимы доступа suid и sgid отображаются как символ «*s*» (символ в нижнем регистре), для неисполняемых файлов – как символ «*S*» (в верхнем регистре).

Для установки режимов доступа suid и sgid используется команда chmod.

Например, опция команды chmod *u*+*s* устанавливает режим доступа suid, а опция *g*–*s* снимает режим доступа sgid.

В восьмеричном формате режиму доступа suid соответствует число «4» в старшем разряде разрешений, а режиму sgid – число «2».

Символьные и восьмеричные значения режимов доступа suid и sgid представлены в таблице 1.

ТАБЛИЦА 1. Символьное и восьмеричное представления режимов доступа suid и sgid

Режим доступа	Символьное представление	Восьмеричное представление
suid	«*s*» («*S*»)	4000
sgid	«*s*» («*S*»)	2000

Когда режим доступа sgid устанавливается для директории, то все созданные в ней файлы и поддиректории будут наследовать gid (а, значит, и групповые разрешения) этой директории. Это полезно для проектов, представленных вложенными директориями и файлами, над которыми работает группа пользователей.

Пользователь, имеющий разрешения на запись в директорию (*w*), может удалять находящиеся в ней файлы, вне зависимости от прав разрешения на просмотр и исполнение.

Это может быть приемлемо для проекта рабочей группы, но не желательно для файлового пространства, находящегося в глобальном общем доступе, например, для таких директорий, как /tmp.

Для решения этой проблемы POSIX ACL поддерживает режим доступа, который называется «закрепление в памяти» (sticky).

В символьном виде этот режим доступа представлен символом «*t*», а в восьмеричном виде – числом «1» (табл. 2).

ТАБЛИЦА 2. Символьное и восьмеричное представления режима доступа sticky

Режим доступа	Символьное представление	Восьмеричное представление
sticky	«*t*»	1000

В выводе команды ls–ld символ режима «закрепление в памяти» находится на месте символа «*x*» (выполнение) для остальных пользователей (*other*).

Если режим «закрепление в памяти» установлен для директории, то удалять файлы или ссылки на файлы, находящиеся в этой директории, может только их владелец или администратор.

Таким образом, применение специальных режимов ограничения прав пользователей suid, sgid и режима «закрепление в памяти» в ОС СН позволяет построить более гибкую и надежную систему защиты информации от несанкционированного доступа в автоматизированных системах.

Список используемых источников

1. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition : учебное пособие / Под ред. д-ра техн. наук П. Н. Девянина. М. : Горячая линия – Телеком, 2018. 311 с.

2. Саенко И. Б., Чирушкин К. А. и др. Основы построения и администрирования операционной системы МСВС : учебное пособие. СПб. : ВАС, 2015. 156 с.

3. Саенко И. Б., Авраменко В. С. и др. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах военного назначения : учебник / Под ред. профессора И. Б. Саенко. СПб. : ВАС, 2010. 520 с.

УДК 004.896; 004.41

«УМНЫЙ ДОМ» ДЛЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Е. С. Казначеева, А. А. Шиян

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

Современная жизнь задает нам свой особый стремительный ритм, но, несмотря на это, повседневная жизнь любого человека должна быть комфортна. А жизнедеятельность людей с ограниченными физическими возможностями должна быть не только уютна, но и безопасна. Сейчас большое внимание уделяется этой группе населения и благодаря технологии умный дом можно сделать их жизнь комфортной.

умный дом, маломобильные группы населения, алгоритмы, интеллектуальное управление.

Развитие современных технологий, связанных с электроникой и программированием делает доступными многие блага, о которых ранее можно было прочитать только в фантастической литературе. Одним из таких благ является «Умный дом», который может сделать комфортным обитание людей в домах, квартирах, гостиницах и прочих зданиях. Актуальность

данной темы определяется последними тенденциями. В настоящее время при строительстве или ремонте жилья могут устанавливаться полноценные системы «Умный дом» или их отдельные части, которые позволяют управлять освещением, отоплением, вентиляцией, аудио-, видеотехникой и охранной сигнализацией.

Под «умным домом» понимается система, которая по заранее определенным правилам, принимает решение по управлению инженерными устройствами, основываясь, на поступающей извне информации (данные с датчиков света, температуры, газа, камер наружного видеонаблюдения и др.). Кроме этого, «умный дом» должен коммуницировать не только с имеющимися компонентами системы, но и с интернет-сервисами [1]. Характерной чертой «умного дома», в отличие от прочих методов формирования жизненного пространства, в большей мере является авангардный путь коммуникации человека и жилого пространства, обладающий возможностью задания желаемой ситуации с помощью передачи инструкции автоматической системе, которая в соответствии с определенным заранее алгоритмом, предопределяет и проверяет режимы функционирования всех электрических и инженерных систем. В случае, когда система «умный дом» полностью настроена и адаптирована под нужды конкретного «владельца», необходимость использования различных привычных средств управления техническими устройствами, такими как: пульт дистанционного управления телевизором, электровыключатели, различные управляющие модули систем отопления и вентиляции, системы видеоконтроля и оповещения, несколько теряется. Это обусловлено тем, что система «умный дом», согласно своему предназначению и названию, самостоятельно берет на себя частичное или полное управление компонентами системы. В доме, оборудованном системой домашней автоматизации, для выбора одного или нескольких предпочтительных сценариев развития, достаточно произнесения голосовой команды или одного нажатия на сенсорную панель, в качестве которой может выступать планшетный компьютер, смартфон. Автоматическая система анализирует пожелания «владельца» и производит настройку работы всех подсистем для обеспечения комфортной обстановки внутри дома, в зависимости от периода времени, дня недели, имеющихся метеоусловий, уличной освещенности. Однако стоит заметить, что во всех подобных системах, вопросы эффективности функционирования и надежности управления подсистемами должны быть поставлены на первое место.

Умный дом предназначен для максимально комфортной жизни людей посредством использования современных высокотехнологических средств. К основным подсистемам умного дома относятся: климат-контроль, освещение, мультимедиа (аудио и видео), охранные системы, селекторная связь, и другие (рис. 1).

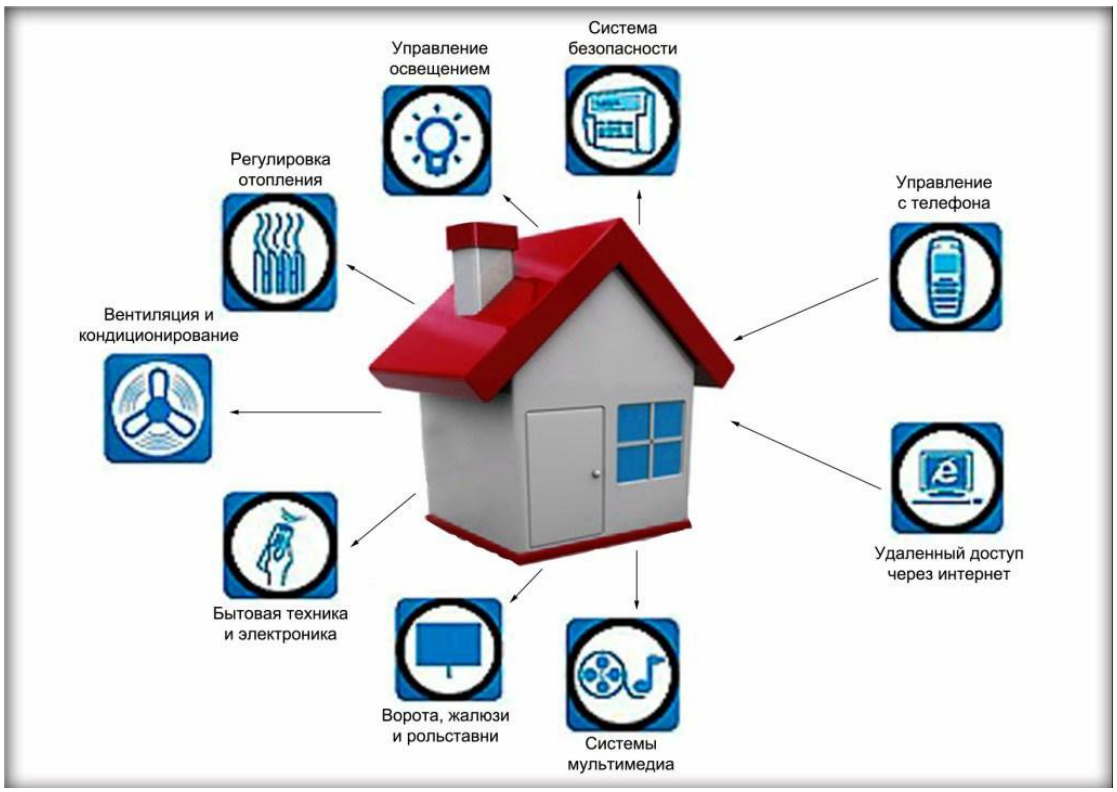


Рис. 1. Схема умного дома

Принцип работы системы умный дом заключается в автоматизации всего, из чего состоит жилая постройка: освещение, кондиционирование, система безопасности, электроэнергия, отопление и так далее. Говоря простым языком, умный дом – это революционная система. С её появлением отпала необходимость заботиться о своем жилище, поскольку теперь жилище само заботится о своем владельце.

Современная жизнь задает нам свой особый стремительный ритм, но несмотря на это, повседневная жизнь любого человека должна быть комфортна. А жизнедеятельность людей с ограниченными физическими возможностями должна быть не только уютна, но и безопасна. Сейчас большое внимание уделяется этой группе населения. Создана специальная программа «Доступная среда», которая направлена на обеспечение беспрепятственного доступа инвалидов к объектам транспортной, социальной и инженерной инфраструктур. Качество жизни этой группы населения зависит и от микросреды, в которой он проживает, то есть от дома, квартиры. Жилище таких людей должно быть грамотно и удобно оснащено с соблюдением санитарных норм жилой площади, включая не только коммунальные удобства, но и оснащение соответствующей мебелью, техникой. Все это, должно помочь таким людям почувствовать себя уверенными в жизни. Сейчас имеется немало современных разработок в плане вспомогательных устройств и приспособлений, специальных архитектурно-планировочных решений.

Как же работают технологии умный дом? По какому принципу и по каким правилам? На рис. 2–3 показаны алгоритм включения котла и поддержания температуры в доме.

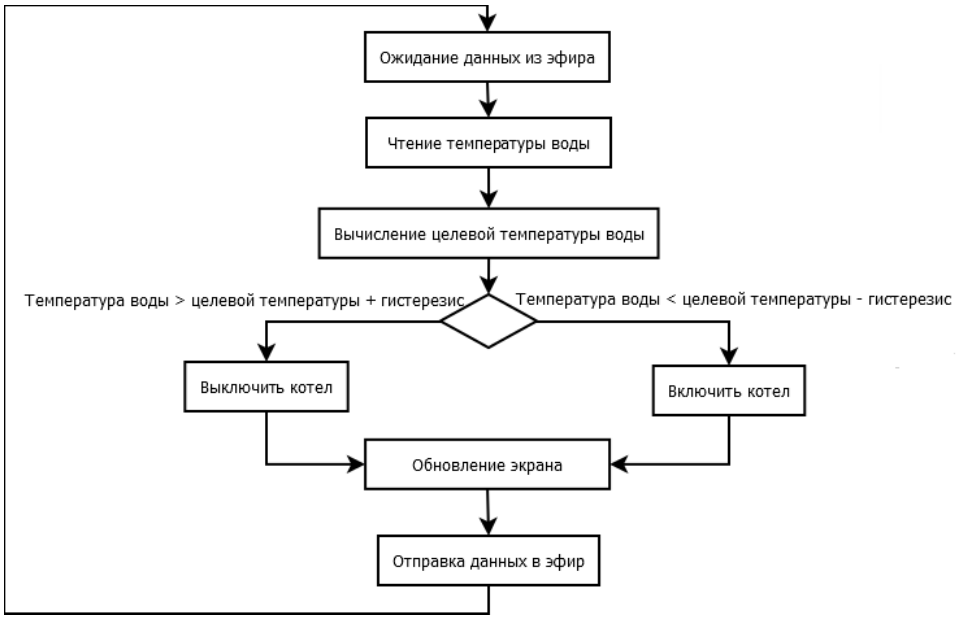


Рис. 2. Алгоритм работы умного дома на примере включения котла

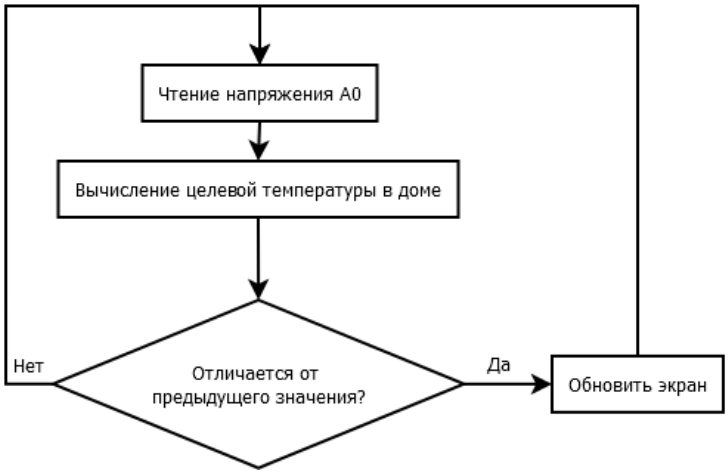


Рис. 3. Алгоритм работы умного дома на примере поддержания температуры в доме

Вся техника, находящаяся в доме, требует к себе индивидуального подхода. И требуется затратить время на ее включение, разобраться с инструкцией к эксплуатации. Чтобы облегчить все эти действия предлагается разработать единый алгоритм для работы со многим системами в доме, а именно (рис.4): электроснабжение; водоснабжение; климат-контроль; открытие / закрытие окон в доме; видеонаблюдения; интернет.

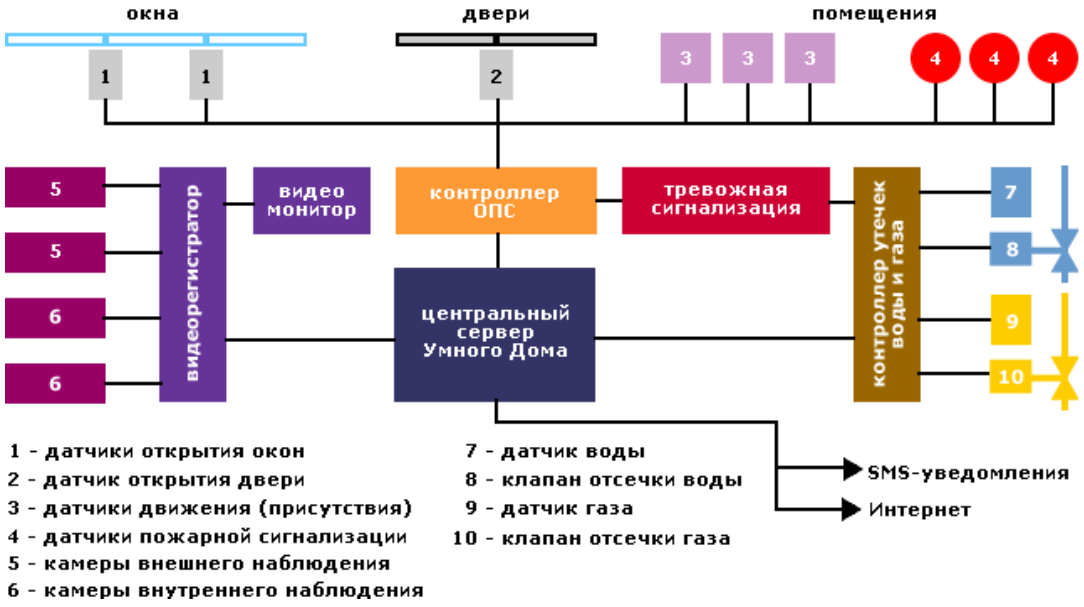


Рис. 4. Контроль всех систем в доме

Работа всех систем будет осуществляться с единого пульта управления, например, смартфон, планшет или ноутбук. На главном экране будет находиться система управления, при включении которой отобразятся все домашние устройства пользователя. Далее с нажатия кнопки можно привести в действие или запланировать включение какой-либо домашней техники к определённому времени. Например, человек встает к 9-ти утра на работу и хочет, чтобы к 07:00 в ванной комнате был включён теплый пол, на кухне согрелся чайник, а на кухне приготовился завтрак. Все эти функции можно включить несколькими нажатиями клавиш на смартфоне или любом другом виде техники. Дополнением будет – sms-оповещение, удалённое управление. Положительным моментом удалённого управления системой – это безопасность собственного жилища, в отсутствии хозяина дома, благодаря чему весь дом будет под присмотром, а в случае аварийных ситуаций хозяин будет моментально проинформирован. Стоит задуматься на одну минуту, сколько раз происходит нажатие на кнопки бытовой техники приходя домой. Все смотрят телевизор, общаются по телефону, играют или работают на компьютере. А теперь, благодаря современным технологиям половина из перечисленного находится на смартфоне [2]. Приходя домой, по нажатию пары кнопок – дверь в дом плавно открывается, свет тихо включается, телевизор горит на любимом канале, микроволновая печь греет еду, поставленную туда заранее. И ведь эта мечта осуществима уже сегодня! Такие системы существуют уже в США, Японии, Китае, Англии, Франции, Германии и даже кое-где в России. Таким образом, системы умного дома спешат на помощь людей и облегчают их жизнь, в частности – для людей с ограниченными возможностями жизнь станет намного комфортней и проще.

Список используемых источников

1. Харке В. Н. Умный дом. Объединение в сеть бытовой техники и систем коммуникаций в жилищном строительстве. М. : Техносфера, 2006. 292 с.
2. Кашкаров А. П. Умный дом своими руками. М. : Дмк-Пресс, 2013. 256 с.

УДК 004.054

ИССЛЕДОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОКОММУНИКАЦИОННОЙ СЕТИ ДЛЯ КОМПЛЕКСА СИСТЕМЫ УПРАВЛЕНИЯ И МОНИТОРИНГА ТЕХНИЧЕСКОГО СОСТОЯНИЯ СИСТЕМЫ ЭНЕРГООБЕСПЕЧЕНИЯ

Д. М. Канатьев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье предложен способ контроля технического состояния электрооборудования систем электроснабжения, а также повышения эффективности, на основе, которой предложен метод бесконтактного мониторинга технического состояния. Описана схема разработки программно-аппаратного комплекса системы управления и мониторинга системы энергообеспечения.

мониторинг технического состояния, система энергообеспечения, автоматизация.

Современные инфотелекоммуникационные сети с каждым днем передают большее количество трафика, также в сетях постоянно происходит изменение ее структуры из-за обновления, неполадок и других ситуаций. По этой причине необходимо производить постоянный мониторинг объектов сети и ее состояния в целом.

Анализ применения современных автоматизированных измерительных комплексов военного назначения показал необходимость разработки и внедрения в данные комплексы средств автоматизации [1]. Повышение сложности эксплуатируемых систем и объектов, установленной на них аппаратуры, а также динамики их работы обуславливают необходимость своевременного мониторинга их состояния. Это необходимо для оперативного контроля, автоматизации и, в целом, обеспечения операций технического обслуживания.

Целью проекта является исследование методов повышения эффективности функционирования инфокоммуникационной сети для комплекса системы управления и мониторинга в части модуля мониторинга технического состояния системы энергообеспечения, посредством разработки макета программно-аппаратного комплекса системы управления и мониторинга в части модуля мониторинга технического состояния системы энергообеспечения военного городка (рис.) [2].

Такая система мониторинга**,** построенная на базе программно-технических средств, предназначена для осуществления мониторинга технологических процессов и обеспечения функционирования оборудования непосредственно в зданиях и сооружениях и передачи информации об их состоянии по каналам связи в диспетчерские службы этих объектов для последующей обработки с целью оценки, предупреждения и ликвидации последствий дестабилизирующих факторов в реальном времени, а также для передачи информации.

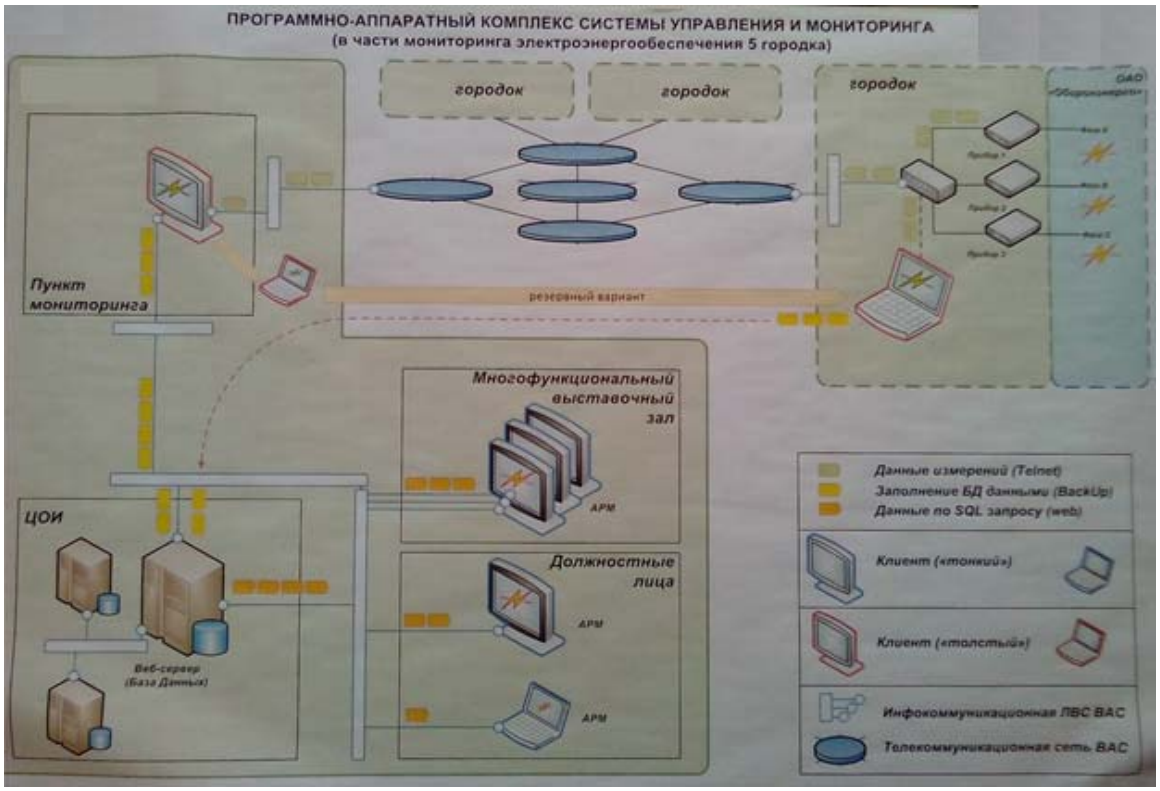


Рис. 1. Схема программно-аппаратного комплекса системы управления мониторинга

Рассматривая организационно-техническую и методическую базу развертывания системы мониторинга технического состояния, следует отметить, что существующая технология сбора и обработки информации о техническом состоянии ориентирована на бумажные формы представления данных и на визуально-ручную технологию их формирования и обработ-

ки [3]. Электронное дублирование бумажных форм ничего не меняет, поскольку сама форма документа не ориентирована на автоматизацию работы с ним.

Таким образом, существует необходимость в разработке системы управления и мониторинга в части модуля мониторинга технического состояния системы энергообеспечения военного городка, которая должна обладать:

а) большей оперативностью тестирования;

б) меньшей информационной избыточностью;

в) меньшими временными и людскими ресурсами.

Система мониторинга технического состояния системы энергообеспечения должна включать в себя три подсистемы:

1) подсистему считывания и получения данных и о количестве потребляемой электроэнергии и состоянии контролируемых объектов;

2) подсистему средств и линий связи и передачи данных;

3) подсистему диспетчерского управления.

Первая подсистема состоит из счетчиков, датчиков и контроллеров, осуществляющих считывание данных о количестве потребляемой электроэнергии, и техническом состоянии системы. Пакеты информационных символов являются заявками на обслуживание сформированные на выходе измерительных датчиков в случае выхода значения контролируемого технологического параметра за пределы установленных допусков. Заявки, поступающие с датчиков, определяются динамикой контролируемого параметра к установленному допуску [4].

Первая подсистема может иметь четыре состояния контролируемого объекта:

1) нормальное (нет заявок);

2) пред предельное (обслуживание заявок низкого приоритета);

3) предельное (обслуживание заявок высшего приоритета);

4) поступивших в период обслуживания заявок низкого приоритета);

5) аварийное (обслуживание заявок высшего приоритета).

Тем самым отслеживая состояние первой подсистемы, передавая данные на подсистему диспетчерского управления.

Вторая подсистема (средств и линий связи и передачи данных) состоит из инфокоммуникационных ЛВС и телекоммуникационной сети, а также резервных частей сети.

Третья подсистема является диспетчерским управлением системой, а также составлением и представлением статистики, организованной через web интерфейс, данные которой хранятся и считываются через базы данных веб-сервера с центра обработки информации.

Таким образом, первая подсистема занимается считыванием информации, вторая передачей данной информации, а третья представлением

и обработкой, выводя пользователю либо администратору данные энергопотребления, анализ технического состояния системы и анализ за определенный период.

Использование предлагаемого способа мониторинга позволит повысить достоверность ее диагностирования за счет вероятностного прогнозирования возникновения отказов, ошибок (сбоев) на заданный интервал времени.

Одним из направлений повышения эффективности эксплуатации систем специального назначения, является дальнейшее совершенствование системы диспетчерского управления, как в целом, так и их составляющих систем, в том числе систем электроснабжения. Основу таких систем составляет электрооборудование различного назначения. Для эффективного функционирования системы диспетчерского управления оператору необходимо иметь достоверные данные о техническом состояние электрооборудования системы электроснабжения в реальном масштабе времени. Такое направление предусматривает переход от принципов эксплуатации по назначенным ресурсным показателям к эксплуатации по техническому состоянию указанных объектов. При этом мониторинг технического состояния электрооборудования системы электроснабжения является одним из основных элементов системы диспетчерского управления.

Качество функционирования современной сети связи, функционирующей на определенной территории, во многом определяются их техническим состоянием. Техническое состояние сети связи определяется совокупностью параметров и их значениями, поэтому современные телекоммуникационные системы, несмотря на неоднородность применяемого оборудования, конструктивную сложность, различные технологии создания, должны подвергаться достоверному контролю.

Методы бесконтактного неразрушающего контроля позволяют по косвенным признакам обнаружить скрытые дефекты, либо выявить особенности, влекущие за собой потенциальную неисправность объекта. Эти методы наиболее эффективны для получения диагностической информации о состоянии системы электроснабжения в режиме реального времени, что особенно важно при эксплуатации по техническому состоянию. Дополнительно существует ряд проблем, затрудняющих процесс мониторинга в системы электроснабжения, связанных с отсутствием в литературе по диагностике унифицированных форм представления таких объектов диагностирования или их моделей, пригодных для решения задач мониторинга.

Результаты могут быть применены при организации учета потребления энергетических ресурсов, как отдельных пользователей, так и целого объекта.

Использование всего программно-аппаратного комплекса позволит автоматизировать и сократить временные затраты для системы учета электроэнергии, обеспечить диспетчеризацию системы учета, мониторинг и ведение учета статистических данных о техническом состоянии, считывание данных и об отказах (повреждениях) в технике связи, значительно повысив при этом ее эффективность, за счет использования систематических и эффективных решений.

Список используемых источников

1. Баринов М. А., Будко Н. П., Будко П. А., Виноградeнко А. М., Дорошенко Г. П., Литвинов А. И., Николаев В. А., Чихачев А. В. Программный комплекс мониторинга технического состояния электронного оборудования по дисциплине «техническое обеспечение связи и автоматизации» // Хроники объединенного фонда электронных ресурсов Наука и образование. 2014. № 8 (63). С. 26.

2. Тихонов Б. Н. Техническое обеспечение связи. Часть I. Основы технической эксплуатации средств связи : учебное пособие. Орел : ОВВКУС, 1989. 139 с.

3. Дудник Л. Н. Разработка методического обеспечения для контроля и прогнозирования технического состояния основных блоков компьютерной сети : дис. ... канд. техн. наук : 05.13.01 / Дудник Людмила Николаевна. Краснодар, 2011.

4. Будко П. А., Литвинов А. И. Методика бесконтактного контроля и идентификации технического состояния электрооборудования систем электроснабжения промышленных комплексов // Датчики и системы. 2014. № 8. С. 5–10.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.93

ОПРЕДЕЛЕНИЕ СПОСОБОВ ПОВЫШЕНИЯ КАЧЕСТВА СИСТЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Н. С. Капитонов, Ф. В. Филиппов

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

Выделены современные направления развития систем компьютерного зрения. Обоснована перспективность применения нейросетевого подхода к совершенствованию систем компьютерного зрения. Выбран класс сверточных нейронных сетей в качестве математической основы для систем компьютерного зрения. Представлено параметрическое пространство описания сверточных нейронных сетей в контексте их применения в системах компьютерного зрения. Описаны наборы экспериментов по исследованию способов повышения качества работы систем компьютерного зрения.

компьютерное зрение, сверточная нейронная сеть, распознавание образов.

Компьютерное зрение – активно развивающееся в данный момент направление науки и технологии, занимающееся проблемой создания систем, способных к распознаванию образов. Основной задачей в этой области является инвариантное распознавание изображений. Несмотря на значительный успех, распознавание изображений лишь в немногих случаях способно сравниться или превзойти восприятие у человека. В целом, задача инвариантного распознавания изображения до сих пор не решена. Существуют различные методы для инвариантного распознавания изображений: потенциальные функции, байесовские сети, Марковские сети, искусственные нейронные сети, различные виды ассоциативной памяти и др. Прежде чем переходить к непосредственно исследованию работы сверточных нейронных сетей, необходимо рассмотреть варианты решения проблемы инвариантного распознавания образов другими методами.

Метод потенциальных функций позволяет нелинейно разбивать множества имеющихся объектов, решая задачи, сложно выполнимые другими методами, но при этом сам процесс выбора подходящей потенциальной функции очень трудоемок и требует затратных вычислений и большой выборки [1].

Метод байесовских сетей – это статистический метод описания закономерностей в данных, позволяющий, на основе первичной информации, содержащейся в базах данных, построить сетевую модель, где события описываются множеством вершин, а причинные связи между событиями задаются ребрами. Построенные байесовские сети просто интерпретируются, легко обрабатывают ситуации, когда значения некоторых переменных неизвестны, позволяет естественным образом совмещать закономерности, выведенные из данных, и позволяет избежать проблемы «переподгонки», однако требуют сложных вычислений, которые в некоторых случаях могут привести к потере значимых закономерностей [2].

Метод марковских сетей представляет собой метод графической модели, в которой множество случайных величин обладает Марковским свойством, описанным неориентированным графом. Марковская сеть отличается от другой графической модели, байесовской сети, представлением зависимостей между случайными величинами [3].

Метод ассоциативной памяти в распознавании изображений тесно связан с искусственными нейронными сетями. В целом, ассоциативная память представляет собой особый вид машинной памяти, используемой в системах очень быстрого поиска. В сочетании с искусственной нейронной сетью с обратной связью, метод ассоциативной памяти способен завершать или исправлять образы, с помощью обратной связи стимулировать одни нейроны при поступлении сигнала на другие. Однако, схожих ре-

зультатов можно достичь и рекуррентными нейронными сетями, при этом не накладывая жесткие условия на коэффициенты и не испытывая таких проблем с устойчивостью [4].

Наилучшие результате в решении проблемы инвариантного распознавания образов показал метод искусственных нейронных сетей. Искусственные нейронные сети представляет собой систему соединённых и взаимодействующих между собой искусственных нейронов. Каждый нейрон подобной сети имеет дело с периодически получаемыми им сигналами, которые он, в соответствии с имеющимися у него весовыми коэффициентами, преобразовывает в выходной сигнал, посылаемый к другим нейронам. Будучи соединёнными в достаточно большую сеть с управляемым взаимодействием, такие по отдельности простые нейроны вместе способны выполнять довольно сложные задачи [5].

Свёрточная нейронная сеть – специальная архитектура искусственных нейронных сетей, предназначенная для наиболее эффективного распознавания изображений. Эта технология построена по аналогии с принципами работы зрительной коры головного мозга, в которой были открыты так называемые простые клетки, реагирующие на прямые линии под разными углами, и сложные клетки, реакция которых связана с активацией определённого набора простых клеток. Идея наличия специализированных компонентов внутри системы, решающих конкретные задачи, является основой СНС. В отличие от полносвязной нейронной сети, в СНС имеется гораздо меньшее количество настраиваемых весов, что и является ее главным преимуществом. Так как одно ядро весов используется для всего изображения, сеть при обучении обобщает демонстрируемую информации, а не запоминает ее. Благодаря этому СНС является одним из лучших алгоритмов по распознаванию и классификации изображений. Однако, при меньшем количестве весов, такая сеть имеет большое количество настраиваемых параметров, каждый из которых для каждой новой задачи необходимо подбирать эмпирически, так как это существенно влияет на результат работы сети.

Имеется множество различных параметров сверточной нейронной сети. Некоторые из этих параметров совпадают с параметрами обычных нейронных сетей, как, например, количество слоев в сети, зависящее от сложности задачи, для которой создается сеть. Также существуют параметры, относящиеся только к сверточным нейронным сетям и связанные с особенностями их строения, как было описано выше. Такими параметрами являются, например, размерность рецептивного поля для каждого из слоёв, шаг сдвига рецептивных полей при обработке изображения, наличие и тип функций, упрощающих исходное изображение и т. д. [6]

Существует несколько вариантов увеличения качества распознавания. Наиболее «простым» в плане затраты интеллектуальных усилий является

создание разработчиком предварительной большой выборки, однако, при своей простоте, данный метод фактически не решает проблему улучшения качества, а лишь откладывает ее. Также имеется возможность использовать специальные алгоритмы, которые перед началом процесса обучения сети автоматически расширяют начальную выборку. Такой подход применим, например, когда известно, что все распознаваемые объекты строятся по определенному принципу. Однако, как уже было сказано, такой подход не является качественным решением проблемы. Еще одним способом улучшения качества распознавания, не затрагивающим непосредственно параметры создаваемой сети, является метод регуляризации. Этот метод приведет к более сложному обучению, к тому же, необходимо будет выработать устойчивость сети к требуемым искажениям.

Главным и самым перспективным направлением в улучшении качества распознавания в случае сверточных нейронных сетей можно считать изменение внутренних параметров математической модели. Основным недостатком данного метода можно считать то, что из-за фактического отсутствия единого шаблона при создании сети распознавания, что требует практически для каждой конкретной задачи строить сеть заново, подбирая все параметры вручную и непосредственно наблюдая за их влиянием на качество работы. Такой процесс очень трудоемок и может привести к тому, что после долгих экспериментов и исследований, можно не добиться какого-нибудь значительного увеличения качества или скорости распознавания. Примером изменения внутренних параметров сети можно считать изменения формы рецептивного поля сверточной нейронной сети. Таким образом создаются искажения в отдельном распознаваемом фрагменте, что позволяет расширь обучающую выборку. Также это позволяет создать более узко направленную специализацию данной конкретной распознающей сети, что улучшит качество распознавания при наличии заранее определённых целей. Таким образом, возможно параллельное использование нескольких рецептивных полей, что позволит выделять из одного входящего изображения различные факторы для дальнейшего анализа.

Компьютерное зрение – одно из перспективных направлений развития информационных систем и науки, раскрывающее огромное количество новых возможностей для практического применения в различных областях деятельности. Сверточные нейронные сети являются одной из возможных основ развития данного направления, и совершенствование и улучшение позволит еще больше расширить данные области.

Список используемых источников

1. Сулимова В. В. Потенциальные функции для анализа сигналов и символьных последовательностей разной длины : автореф. дис. ... канд. физ.-мат. наук: 05.13.17 / Сулимова Валентина Вячеславовна. Москва, 2009. 20 с.

2. Дайнеко В. Ю. Разработка модели и алгоритмов обнаружения вторжений на основе динамических байесовских сетей : дис. ... канд. физ.-мат. наук: 05.13.19 / Дайнеко Вячеслав Юрьевич. Санкт-Петербург 2013. 131 с.

3. Чистиков П. Г. Методы и алгоритмы гибридного синтеза естественной русской речи на основе скрытых марковских моделей и метода UNIT SELECTION : автореф. дис. ... канд. техн. наук: 05.13.11 / Чистиков Павел Геннадьевич. Санкт-Петербург 2013. 20 с.

4. Романов М. П. Интеллектуальные системы управления с ассоциативной памятью: модели, алгоритмы и методы исследования : дис. ... д-ра техн. наук: 05.13.01 / Романов Михаил Петрович. Москва, 1999. 386 с.

5. Оганезов А. Л. Применение нейронных сетей в задачах распознавания образов : дис. ... канд. техн. наук: 05.13.11 / Оганезов Алексей Леванович. Тбилиси, 2006. 149 с.

6. Немков Р. М. разработка нейросетевых алгоритмов инвариантного распознавания образов: дис. ... канд. техн. наук: 05.03.18 / Немков Роман Михайлович. Ставрополь, 2015. 162 с.

УДК 004.7:004.422.8

МОДЕЛИРОВАНИЕ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ ДЛЯ ОРГАНИЗАЦИИ КОММУНИКАТИВНЫХ ПРОЦЕССОВ КОНТРАГЕНТОВ

Е. А. Карачинская, Л. К. Птицына

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

Описана значимость коммуникативных процессов контрагентов при усилении влияния глобальной экономики на технологический уклад социума. Проанализировано современное состояние технологического сопровождения коммуникативных процессов контрагентов. Намечены перспективные пути его развития. Представлены преимущества использования сервис-ориентированных систем для организации коммуникативных процессов контрагентов. Предложен базис формализаций для их моделирования. Раскрыты приёмы применения результатов моделирования сервис-ориентированных систем для организации коммуникативных процессов контрагентов в целях их соответствия высокой значимости.

технологический уклад, контрагент, коммуникативный процесс, сервис-ориентированная система, моделирование.

Экономика информационного общества отличается от предшествующих этапов развития социума высокой интенсивностью проявления социальных и технологических нововведений. Одной из важных закономерностей экономики является её непрерывное развитие вследствие по-

следовательного замещения целостных комплексов технологически сопряженных производств – технологических укладов. Технологический уклад социально-экономического развития общества основывается на совокупности технологий определенного уровня развития производства. Современный технологический уклад характеризуется углублением процессов глобализации, развитием интернационализации предпринимательства, увеличением количества транснациональных компаний и созданием международной кооперации в производстве, развитием информационных и инновационных технологий, формированием новых правил сотрудничества в мировом экономическом пространстве.

В соответствии со Стратегией развития информационного общества в Российской Федерации на 2017–2030 гг. реализуется Программа цифровой экономики, ориентированная на поддержку развития как уже существующих условий для возникновения прорывных и перспективных сквозных цифровых платформ и технологий, так и создание условий для возникновения новых платформ и технологий.

Одним из ключевых факторов успешной деятельности предприятия или организации является эффективная профессиональная деятельность в среде информационной инфраструктуры.

При этом объективным залогом успешной деятельности большинства крупных предприятий и организаций является эффективное использование коммуникативных процессов контрагентов, определяющих наукоёмкое ядро цифровой экономики. Предприятиями и организациями предусматриваются задачи, которые требуют усовершенствования, интеграции и дальнейшего развития уже используемых информационных технологий и платформ. Предприятия и организации ориентируются на программные решения, учитывающие специфику их деятельности и обеспечивающие устойчивую конкурентоспособность в условиях интенсивного развития технологических платформ цифровой экономики. Для производств проявляется объективная необходимость интеграции IT-структуры на внешнем и межкорпоративном уровне. При перспективном использовании веб-сервисов расширяются масштабы взаимодействия приложений с разными информационными системами. При выделении независимых сервисов обеспечивается возможность их повторного использования во внутренних и внешних системах, а значит, исключается необходимость разработки дублирующих приложений.

Предлагаемые формализации, связанные с разработкой и исследованием наукоёмкого ядра интеграции веб-сервисов для организации коммуникативных процессов контрагентов с различными профилями, нацеливаются на обеспечение необходимых гарантий качества в изменяющихся условиях рыночной конкуренции.

В условиях цифровой экономики наблюдаются частые изменения в бизнес-процессах, требующие от специалистов предприятий максимально возможной скорости внесения и добавления задач по организации коммуникативных процессов контрагентов. Для обеспечения необходимого уровня интеграции между информационными системами используются сервис-ориентированные системы (*Service Oriented System* – SOA), позволяющие снизить затраты на разработку приложений, увеличить скорости реагирования на изменения требований ведения бизнеса, предусмотреть многократное использование бизнес-сервисов, достичь полной независимости от различного рода технологий. Проблема интеграции становится обязательным аспектом развития IT-технологий. Главными преимуществами использования SOA-систем в профессиональной деятельности являются масштабируемость и гибкая расширяемость существующей информационной инфраструктуры. Сервис-ориентированная архитектура предоставляет клиентам разнообразные возможности по управлению финансами, кадрами, ресурсами, документооборотом через веб-сервисы с помощью удобного интерфейса.

В контексте обеспечения гарантий качества сервис-ориентированная система сопровождается базисом формализаций, ставящих целью построение моделей интеграции сервисов, их анализ посредством соответствующих методов оценивания выбираемых показателей качества и выбор такой интеграции сервисов, которая удовлетворяет требованиям устойчивой конкуренции в профессиональной деятельности [1]. Для обеспечения требуемых гарантий проводится многоэтапное моделирование сервис-ориентированных систем для организации коммуникативных процессов контрагентов.

При формировании базиса формализаций многоэтапного моделирования учитываются стартовые позиции предприятий и организаций в части использования готовых реализаций сервис-ориентированных систем. В связи с этим первые два этапа выбора целевой интеграции сервисов опираются на методики сравнительного анализа и оценки эффективности готовых реализаций сервис-ориентированных систем, доступных для использования на предприятии или в организации.

На первом этапе моделирования активизируется методика ранжирования и выбора претендентов сервис-ориентированных систем.

Предлагаемая $\mathbf{M}_r$ методика ранжирования и выбора претендентов SOA для сопровождения коммуникативных процессов контрагентов описывается следующим кортежем:

$$\mathbf{M}_r = \langle \mathbf{C}, \mathbf{I}, \mathbf{M}_A, \boldsymbol{\lambda}, \boldsymbol{\beta}, \mathbf{W}, \mathbf{K}, \mathbf{L}, \mathbf{R} \rangle,$$

где $\mathbf{C}$ – множество предлагаемых критериев, характеризующих выделенные аспекты поведенческих свойств претендентов SOA для сопровожде-

ния коммуникативных процессов контрагентов; **I** – множество альтернатив в реализации претендентов SOA для сопровождения коммуникативных процессов контрагентов; $\mathbf{M}_A$ – метод преодоления априорной неопределенности относительно метрических характеристик предложенных критериев путем определения значений оценок интенсивности их проявления в сравниваемых реализациях претендентов SOA для сопровождения коммуникативных процессов контрагентов; **λ** – множество интенсивностей проявления предложенных критериев для сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов; **β** – множество значимостей критериев для сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов; **W** – множество матриц результатов попарных сравнений соответствующих оценок интенсивностей проявления предложенных критериев для сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов; **K** – множество векторов коэффициентов предпочтений в выборе альтернативной реализации претендента SOA для сопровождения коммуникативных процессов контрагентов по каждому из предложенных критериев; **L** – множество коэффициентов значимости критериев по результатам попарных сравнений их соответствующих оценок; **R** – множество приоритетов выбора альтернативной реализации претендентов SOA для сопровождения коммуникативных процессов контрагентов.

В предлагаемой методике выбор J альтернативы-лидера среди сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов выполняется на основе следующего предпочтения:

$$J = \arg\left(\max_i R_i\right), \ \ i = 1, 2, \ldots, M.$$

К исходной информации для выбора альтернативы-лидера среди сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов относятся: множество предлагаемых критериев **C**, множество альтернатив **I**, метод преодоления априорной неопределенности $\mathbf{M}_A$, множество интенсивностей проявления предложенных критериев **λ**, множество значимостей критериев **β**.

В результате выполнения вычислительных операций, содержание которых раскрывается в [2], формируются: **W** – множество матриц результатов попарных сравнений соответствующих оценок интенсивностей проявления предложенных критериев для сравниваемых реализаций претендентов SOA для сопровождения коммуникативных процессов контрагентов; **K** – множество векторов коэффициентов предпочтений в выборе альтернативной реализации претендента SOA для сопровождения коммуникативных процессов контрагентов по каждому из предложенных крите-

риев; **L** – множество коэффициентов значимости критериев по результатам попарных сравнений их соответствующих оценок; **R** – множество приоритетов выбора альтернативной реализации претендентов SOA для сопровождения коммуникативных процессов контрагентов; ранжированное множество готовых реализаций сервис-ориентированных систем по каждому из предложенных критериев; *J* идентификатор альтернативы-лидера по интегрированному критерию.

На втором этапе моделирования осуществляется предварительное оценивание эффективности готовых реализаций сервис-ориентированных систем на основе теории нечётких множеств, позволяющей преодолеть неопределённость относительно функционального связывания показателей эффективности и параметров, описывающих специфику профессиональной деятельности. Второй этап моделирования сервис-ориентированных систем для организации коммуникативных процессов контрагентов завершается либо уточнением идентификатора альтернативы-лидера по интегрированному критерию, либо принятием решения о создании новой сервис-ориентированной системы.

При любом исходе второго этапа моделирования сервис-ориентированных систем для организации коммуникативных процессов контрагентов осуществляется переход к третьему этапу, на котором проводится определение и оценивание риска срыва временного регламента профессиональной деятельности при использовании выбранной альтернативы-лидера или создаваемой новой сервис-ориентированной системы. При определении и оценивании риска срыва временного регламента профессиональной деятельности предлагаются расширения формализаций, раскрытых в [3, 4, 5]. Расширения касаются интеграции веб-сервисов. Развитие формализаций для определения и оценивания риска срыва временного регламента профессиональной деятельности осуществляется в рамках расширенных объектно-ориентированных моделей интеграции веб-сервисов.

Научная значимость предлагаемых решений заключается в генерации наукоёмкого ядра жизненного цикла сервис-ориентированных систем для организации коммуникативных процессов контрагентов с гарантиями качества.

Список используемых источников

1. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2011. 105 с.

2. Птицына Л. К., Пашкова Л. С. Выбор эффективной системы биллинга // Международный научно-исследовательский журнал. Часть 1. 4 (11). Сборник по результатам XIV заочной научной конференция Research Journal of International Studies, 2013. С. 111–116.

3. Птицына Л. К., Смирнов Н. Г. Системно-аналитическая основа интеграции сервис-ориентированных средств // Промышленные АСУ и контроллеры. 2011. № 5. С. 31–36.

4. Птицына Л. К., Веселов В. О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоёмкие технологии в космических исследованиях Земли. H&ES RESEARCH. М. : ООО «Издательский Дом Медиа Паблишер», 2015. № 2. С. 42–47.

5. 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.

УДК 004.056

МОДЕЛЬ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

А. В. Карпов

Военная академия связи им. Маршала Советского Союза С.М. Будённого

Моделирование каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. Необходима разработка модели канала утечки информации на объекте информатизации, которая определяет условия их возникновения для данного объекта. Модель используется для проектной оценки защищенности информации от ее утечки либо непрерывного контроля параметров объекта при его эксплуатации.

канал утечки информации, объект информатизации, логико-вероятностный метод, логическая модель, вероятностная функция, система защиты информации.

Защита информации (ЗИ) на объекте информатизации (ОИ) достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам (ТК), несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

Значительное повышение требований к безопасности функционирования ОИ не может быть реализовано только за счет расширения и ужесточения мер контроля за безопасностью без использования количествен-

ных оценок, а они возможны даже при отсутствии вероятностей их нарушения.

Системный подход к проблеме безопасности информации (БИ) на ОИ требует проведения комплексного анализа, классификации угроз, основных поражающих и влияющих факторов, поведения окружающей среды и действий персонала [1]. Для решения этих вопросов необходимы соответствующие методы математического моделирования.

Таким образом, для обоснования распределения сил и средств ЗИ от ее утечки по ТК на ОИ, необходима разработка модели канала утечки информации на данном объекте. Модель позволит получить данные, необходимые для построения системы защиты информации (СЗИ) на ОИ от ее утечки по ТК.

Разработка модели канала утечки информации по ТК на ОИ возможна с помощью логико-вероятностной (ЛВ) теории безопасности и риска, где под степенью риска в данном случае будем понимать угрозу утечки информации по ТК.

Фундаментальными понятиями в ЛВ-теории безопасности и риска являются понятие опасного состояния объекта (в данном случае это утечка информации по ТК на ОИ), характеризующегося ущербом различного масштаба, и понятие опасности – способности системы переходить в опасное состояние [2].

В каждом конкретном случае необходимо дать аналитическое описание этого опасного состояния объекта. В ЛВ-теории безопасности и риска такое описание начинается с составления сценария опасного состояния, которое осуществляется с помощью конъюнкций и дизъюнкций инициирующих событий и условий. В качестве таковых выступают различные внешние и внутренние воздействия, приводящих к утечке информации.

Перейдем к составлению сценария опасного состояния на типовом ОИ. На данном объекте защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Как показывает анализ функционирования типового ОИ, наиболее опасными техническими каналами утечки информации (ТКУИ) на данном объекте являются: акустический, виброакустический и каналы побочных электромагнитных излучений и наводок (ПЭМИН) [3].

Например, утечка информации на ОИ по акустическому каналу (АК) произойдет, если имеют место информативный акустический сигнал (ИАС) ($Z1$), техническое средство разведки (ТСР) в зоне разведдоступности данного сигнала ($Z2$) и отсутствует (либо неисправно) средство защиты информации от утечки по АК ($Z3$) [4]. В данном случае конечное

событие (опасное состояние) – утечка информации по АК на ОИ, а инициирующими событиями и условиями являются соответственно $Z1$, $Z2$, $Z3$.

Для обоснования рационального состава организационно-технических мер защиты, а также варианта структуры СЗИ от утечки по ТК на ОИ, необходима разработка логической модели канала утечки информации (КУИ).

Логическая модель канала утечки информации (Л-функция риска утечки) по ТК на ОИ представляет собой функцию алгебры логики (ФАЛ), включающую в себя операции конъюнкций и дизъюнкций инициирующих событий и условий, приводящих к этой утечке.

В данном случае Л-функция $K1(Z)$ по АК на ОИ имеет вид:

$$K1(Z) = Z1 \cap Z2 \cap Z3 = Z1Z2Z3, \quad (1)$$

где $Z1$ – наличие ИАС; $Z2$ – наличие ТСР акустического сигнала в зоне разведдоступности ИАС; $Z3$ – средство защиты информации от утечки по АК отсутствует или неисправно.

Пусть $K2$, $K3$ – утечка информации по виброакустическому каналу (ВАК) и каналу ПЭМИН соответственно, тогда Л-функция риска утечки информации на ОИ примет вид:

$$Y(Z) = \begin{vmatrix} K1 \\ K2 \\ K3 \end{vmatrix}, \quad (2)$$

где $K1$ – Л-функция риска утечки информации по АК.

Соответственно, Л-функция риска утечки информации по ВАК:

$$K2(Z) = Z1 \cap Z4 \cap Z5 = Z1Z4Z5, \quad (3)$$

где $Z1$ – наличие ИАС (аналогично АК); $Z4$ – наличие ТСР виброакустического сигнала в зоне разведдоступности ИАС; $Z5$ – средство защиты информации от утечки по ВАК отсутствует или неисправно.

Л-функция риска утечки информации по каналу ПЭМИН:

$$K3(Z) = Z6 \cap Z7 \cap Z8 = Z6Z7Z8, \quad (4)$$

где $Z6$ – наличие опасного сигнала (побочного излучения); $Z7$ – наличие соответствующего ТСР сигналов ПЭМИН в зоне разведдоступности опасного сигнала; $Z8$ – средство защиты информации от утечки по каналу ПЭМИН отсутствует или неисправно.

Подставляя (1), (3), (4) в (2), получим:

$$Y(Z)=\begin{vmatrix} Z1Z2Z3 \\ Z1Z4Z5 \\ Z6Z7Z8 \end{vmatrix}, \tag{5}$$

где конъюнкции стоят в строках, а знак дизъюнкции между строками.

Из (5) видно, что существует только 3 способа организации утечки информации на данном объекте и ни одним больше. Анализ Л-функции позволяет также оценить такие характеристики, как структурная значимость и вклад инициирующих событий в обобщенный показатель защищенности информации от утечки по ТК на ОИ, выраженный вероятностной функцией риска утечки на данном объекте. Данный показатель необходим для принятия решения о состоянии защищенности информации на ОИ в соответствии с действующим критерием защищенности [5].

Переход к вероятностной функции риска утечки информации ($B(Z)$) на ОИ возможен путем приведения Л-функции риска утечки информации к дизъюнктивной нормальной форме (ДНФ). Данный переход позволяет получить вероятности истинности логических переменных, отображающих соответствующие события. Данное действие осуществляется путем ортогонализации Л-функции, записанной в ДНФ. После несложных преобразований получим ортогональную ДНФ (ОДНФ) булевой функции $Y(Z)$:

$$Y(Z)=\left(\left[Z1Z2Z3\right]\cup\left[\left(\overline{Z1}\cup Z1\overline{Z2}\cup Z1Z2\overline{Z3}\right)\left(Z1Z4Z5\right)\right]\right)\cup$$

$$\cup\left[\left(\overline{Z1}\cup Z1\overline{Z2}\cup Z1Z2\overline{Z3}\right)\left(\overline{Z1}\cup Z1\overline{Z4}\cup Z1Z4\overline{Z5}\right)\left(Z1Z6Z7Z8\right)\right], \tag{6}$$

где $Y(Z)$ – Л-функция риска утечки информации на ОИ в ОДНФ.

Только для ортогональной ДНФ (6) вместо соответствующих переменных можно подставлять их вероятности, заменяя знаки дизъюнкции и конъюнкции на знаки сложения и умножения соответственно. На основании этого получим вероятностную функцию риска утечки информации на ОИ:

$$B(Z)=p1p2p3+\left[\left(q1+p1q2+p1p2q3\right)\left(p1p4p5\right)\right]+$$

$$+\left[\left(q1+p1q2+p1p2q3\right)\left(q1+p1q4+p1p4q5\right)\left(p1p6p7p8\right)\right], \tag{7}$$

где $B(Z)$ – вероятностная функция риска утечки информации на ОИ; $p1$, $p2\ldots p8$ – прямые вероятности событий $Z1$, $Z2\ldots Z8$; $q1$, $q2\ldots q5$ – инверсные вероятности $Z1$, $Z2\ldots Z5$.

Функция (7) характеризует истинность Л-функции (5) и является обобщенным показателем защищенности информации на ОИ от утечки

по ТК. Другими словами, с помощью вероятностной функции (7) определяют вероятность утечки информации на ОИ при заданных исходных вероятностях инициирующих событий и условий, приводящих к данной утечке.

Разработанная логическая модель канала утечки информации (5) по ТК на ОИ позволяет определить наиболее важные, малозначимые и опасные состояния данного объекта. Также с помощью данной модели возможно выявление наиболее выгодных комбинаций инициирующих условий, защита от которых предотвращает утечку информации на объекте, т. е. объективно устанавливаются приоритеты в разработке соответствующих систем защиты.

Полученная с помощью логико-вероятностного метода вероятностная модель (7) является не просто расчетной формулой вероятности утечки информации на ОИ, а представляет собой важную целевую функцию, с помощью и на основе которой могут быть выработаны действительные, научно обоснованные управленческие решения по функционированию данного объекта.

Список используемых источников

1. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях; Военная академия связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, 2013.

2. Соложенцев Е. Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. Изд. 2-е. СПб. : Издательский дом «Бизнес-пресса», 2006. 530 с.

3. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие. М. : Изд-во МГТУ им. Н.Э. Баумана, 2008. 536 с.

4. Карпов А. В., Лепешкин О. М., Попов Н. А. Структура электромагнитного поля при нелинейной радиолокации // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 1118.

5. Карпов А. В., Лепешкин О. М., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х т. 2017. С. 1198.

Статья представлена научным руководителем, доктором технических наук, доцентом О. М. Лепешкиным.

УДК 004.7

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

С. Х. Киреев, О. С. Лаута

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье описан подход к обнаружению сетевых компьютерных атак на информационно-вычислительные сети, основанный на проведении анализа сетевой активности и выделения признаков аномального поведения с использованием методов машинного обучения и искусственного интеллекта. В качестве математического аппарата для реализации предлагаемого подхода рассматриваются искусственные нейронные сети, позволяющие решать задачи классификации и прогнозирования, и рассматриваются возможные варианты применения искусственных нейронных сетей для обнаружения аномального поведения в информационно-вычислительной сети.

информационно-вычислительная сеть, компьютерные атаки, системы обнаружения атак, искусственный интеллект, машинное обучение, нейронные сети.

Подходы к построению СОА

Задача обнаружения сетевой компьютерной атаки (КА) является нетривиальной и требует серьёзного математического и алгоритмического аппарата. Могут быть выделены два основных направления в данной области: обнаружение злоупотреблений и обнаружение аномальной активности [1]. В реальных системах обнаружения атак эти методы могут использоваться совместно, так как не являются противоречащими друг другу.

В первом случае обнаружение КА сводится к сопоставлению зарегистрированных событий с набором различных «шаблонов» известных компьютерных атак – так называемых «сигнатур». Поэтому данный подход также называется сигнатурным. Схема работы типичной сигнатурной СОА представлена на рис. 1.

Основными задачами, возникающими в процессе создания подобных систем, являются создания языка описания КА и наполнение базы знаний системы сведениями о максимально возможном числе различных КА.

Основным преимуществом сигнатурных СОА является низкое число ложных срабатываний систем на множестве атак, описанных в базе знаний.

Главной проблемой таких систем является невозможность обнаружения атак, отличающихся от имеющихся сигнатур. Данная проблема реша-

ется путём добавления различного рода модификаторов к сигнатурам, а также сочетанием подобных систем с системами других типов.

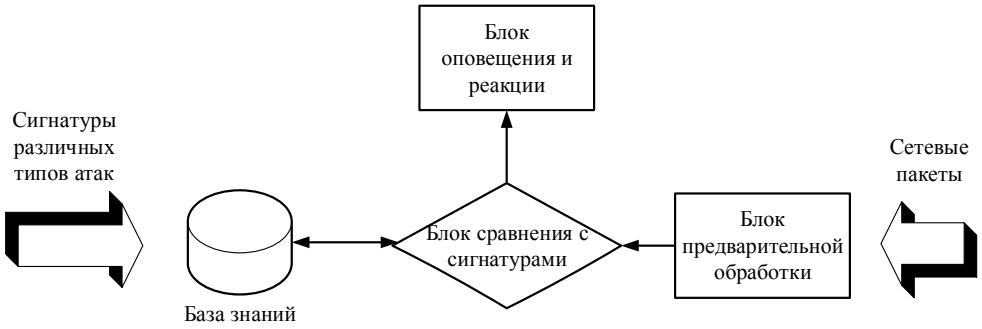


Рис. 1. Схема архитектуры сигнатурной СОА

Второй подход подразумевает построение профиля нормального поведения системы и наблюдения за её характеристиками в процессе эксплуатации. Отклонение от заданного профиля считается аномальным поведением и трактуется как наличие КА на систему. Таким образом, при создании таких систем, основными задачами является:

– построение профиля нормального поведения системы. Эта задача является достаточно сложной, так как требует выбора необходимых параметров системы, которые будут определять её состояние с точки зрения безопасности, а также формализации данных параметров для дальнейшей с ними работы;

– определение граничных значений отклонения для наблюдаемых параметров, превышение которых будет трактоваться как КА.

Схема работы типичной СОА на основе обнаружения аномальной активности представлена на рис. 2.

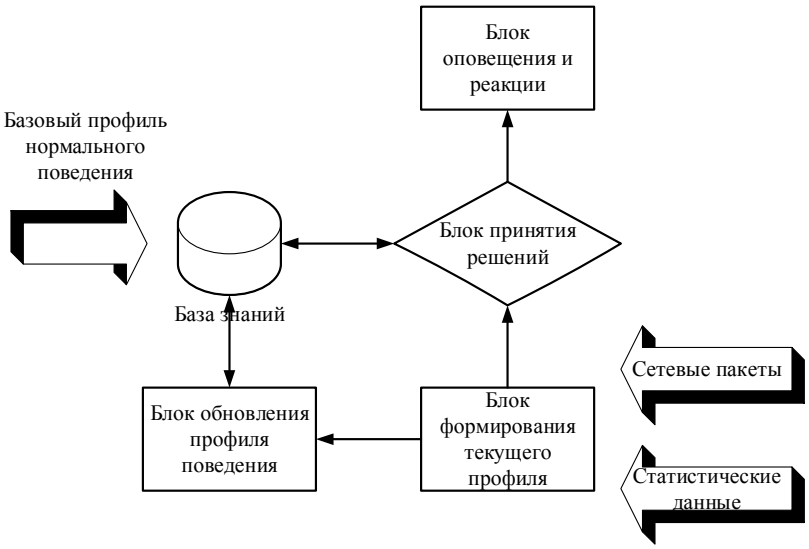


Рис. 2. Схема архитектуры аномальной СОА

Применение ИИ для обнаружения КА

Основной задачей теории ИИ является разработка подходов и алгоритмов, обеспечивающих решение задач, свойственных человеческому мозгу. К таким задачам в общем случае относят [2]:

– накопление знаний;

– применение накопленных знаний;

– извлечение знаний из опыта.

Для решения данных задач системы, основанные на применении ИИ должны обеспечивать выполнение следующих процессов:

1. Представление. В отличие от реального человеческого мозга системы ИИ применяют для описания знаний о предметной области формальный (символьный язык). Символы обычно формируются в уже известных терминах, что делает подобное представление знаний доступным для понимания также и человеку. Знания в данном случае можно отождествить с термином «данные», используемом при описании различных информационных систем.

2. Рассуждение. Согласно [2] систему можно назвать разумной, когда она удовлетворяет следующим критериям:

– система описывает и решает широкий спектр задач;

– система понимает, как явную, так и неявную информацию;

– система имеет механизм управления, определяющий порядок решения тех или иных задач.

Таким образом, рассуждением можно считать способность системы ИИ решать различного рода задачи. Процесс решения произвольной задачи можно рассматривать как некоторую частную задачу поиска, в которой выделяются правила, данные и управляющие воздействия. Правила определяют управляющие воздействия на области данных в соответствии с условиями задачи. Часто системам ИИ приходится работать в условиях неопределённости, когда набор знаний является неполным или неточным. В таком случае, система использует вероятностные рассуждения [2].

3. Обучение. Процесс обучения системы ИИ может включать два различных способа обработки поступающей информации: индуктивный, когда общие шаблоны и правила создаются на основании практического опыта и потоков данных, и дедуктивный, когда для определения конкретных фактов используются общие правила. Информация, на основе которой выполняется обучение, поступает на элемент обучения из внешней среды. Данная информация переводится в символьную форму и попадает в базу знаний, используя которую исполнительный элемент в дальнейшем для выполнения задачи. Результаты выполнения задачи в дальнейшем играют роль обратной связи, которая помогает элементу обучения заполнить пробелы в поступающих знаниях, выбрать наиболее существенные их па-

раметры и отбросить избыточные. Механизм обратной связи позволяет системе проверять рабочие гипотезы и пересматривать их по мере необходимости.

Одним из перспективных направлений применения систем ИИ является их использование в качестве математической основы при построении СОА. Использование систем ИИ в СОА позволяет обеспечить высокую эффективность работы, так как предлагает решение нескольких ключевых проблем, возникающих при разработке СОА: обнаружение ранее неизвестных типов атак, адаптация СОА к поведению элементов ИВС и её пользователей, адаптация СОА к модификациям известных типов атак и др.

Хорошо зарекомендовавшим себя подходом к решению подобных задач с применением методов ИИ является использование искусственных нейронных сетей (ИНС). ИНС представляют математически-формализованную модель естественного мыслительного процесса человека, основанного на передаче информации между простейшими структурными единицами – нейронами. Данный подход является одним из наиболее перспективных и позволяет решать широкий спектр задач: классификация, оптимизация, кластеризация, аппроксимация функций, прогнозирование и др.

Процесс построения профиля нормального поведения в случае с нейронными сетями сводится к созданию обучающей выборки, состоящей из примеров, содержащих данные нормального поведения информационно вычислительной сети (ИВС), и дальнейшего обучения ИНС с использованием этих данных. Алгоритмы обучения, обычно, выбираются на основе выбранного типа ИНС. Параметры ИНС выбираются эмпирическим путём в зависимости от конкретной задачи [3].

В случае, когда профиль нормального поведения строится на основе данных протоколов передачи, в качестве характеристик используются поля заголовков пакетов, а также дополнительные данные, такие как, например, временная метка, если эти данные не предусмотрены протоколом, но являются существенными для обнаружения аномалий.

Также профиль нормального поведения может содержать данные прикладных протоколов, используемых элементами ИВС и статистические сведения о функционировании ИВС за некоторый промежуток времени. Данные профиля могут рассматриваться как отдельные независимые примеры, так и в качестве упорядоченной последовательности. Такой подход является более эффективным, так как анализ закономерностей в последовательностях событий позволяет получить более конкретные сведения о действиях и намерениях пользователей (и других субъектов) ИВС в процессе их взаимодействия с элементами ИВС и более точно произвести обнаружение аномалии при её наличии.

Далее будут рассмотрены различные задачи, решаемые с использованием ИНС, типы ИНС, используемые для решения этих задач и методы применения данных задач к процессу обнаружения аномального поведения ИВС.

1. Задача классификации. Сети прямого распространения

Классической структурой нейронной сети для решения задачи классификации является многослойный персептрон (MLP) – сеть прямого распространения. Пример такой сети изображён на рис. 3.

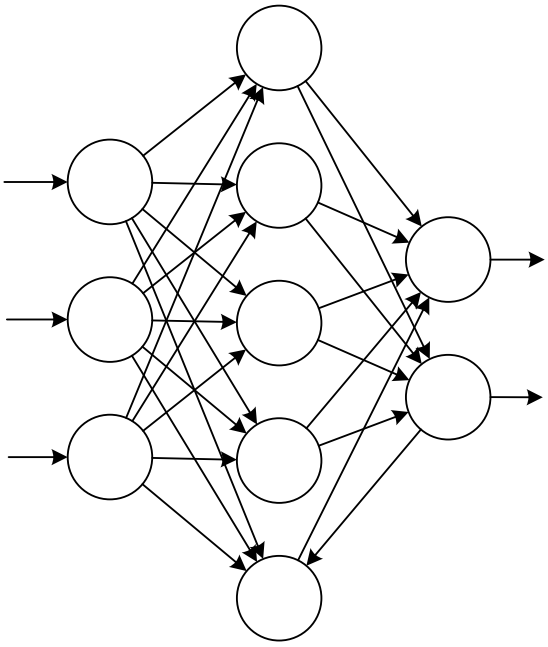


Рис. 3. Многослойный персептрон

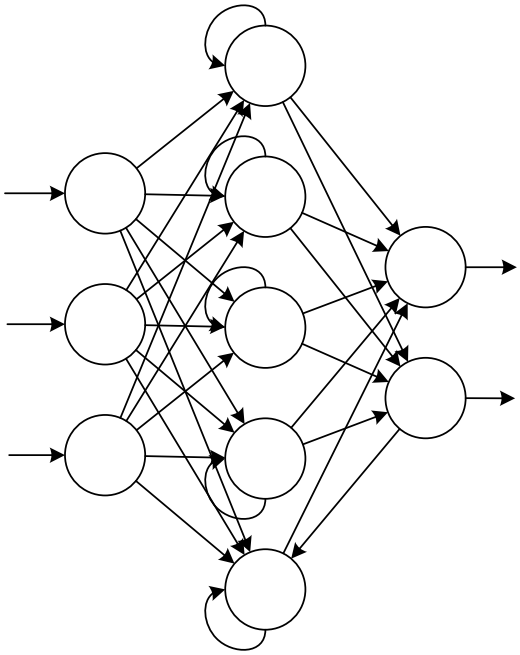


Рис. 4. Сеть Элмана

Персептрон принимает на вход заданный вектор и определяет принадлежность этого вектора к тому или иному классу. В задаче обнаружения аномалий входными данными могут служить поля заголовков пакетов. На выходе ИНС мы можем получать сведения о том, являются ли входные данные «нормальными», либо «аномальными». Существенным недостатком данной топологии ИНС является то, что она не позволяет работать с последовательностями данными, что ограничивает возможности обработки последовательно приходящих команд, т. е. такая сеть способна делать выводы только на основе одного набора входных параметров. Возможным решением данной проблемы является добавление входного поля, содержащего временную метку для каждого пакета, что «упорядочивает» пакеты для ИНС и даёт ей возможность установить закономерности, связанные с последовательностью появления тех или иных входных данных.

2. Задача прогнозирования. Рекуррентные ИНС

Наиболее хорошо зарекомендовавшими себя в решении задач, связанных с прогнозированием, являются так называемые рекуррентные нейронные сети. Отличие данного класса ИНС состоит в том, что в них имеется обратная связь: выходы нейронов скрытого слоя сети соединяются с входами сети, т. е. при обработке нового набора входных параметров учитывается контекст, возникший в процессе обработки предыдущих наборов. Пример такой сети изображён на рис. 4 (Сеть Элмана).

Учитывая динамический и последовательный характер процесса обмена данными в ИВС, такой подход может показаться наиболее подходящим при построении систем обнаружения аномалий, так как возможность учитывать взаимосвязь между различными командами позволит системе более эффективно выполнять свои функции.

Задача прогнозирования в контексте обнаружения аномалий поведения ИВС будет заключаться в определении возможного состояния ИВС на основе информации о предыдущих. При этом, если действительное состояние будет значительно отличаться от возможных прогнозируемых, то можно сделать вывод об аномальном поведении.

Кроме того, рекуррентные нейронные сети могут быть использованы и для решения задач классификации как персептроны, при этом, при анализе потоковых данных, к которым, например, относятся последовательности сетевых пакетов в ИВС, они способны выдавать лучшие результаты [4].

К сожалению, появление обратных связей привносит некоторые сложности, связанные с изменением структуры ИНС. Классические алгоритмы обучения, используемые для сетей прямого распространения, не могут быть использованы для обучения таких ИНС.

Заключение

Становится понятно, что ИНС позволяют эффективно решать задачи, связанные с обнаружением аномального поведения в процессе управления функционирования и информационного обмена в ИВС. Таким образом, использование ИНС позволит повысить защищённость ИВС и обеспечить более высокий уровень обнаружения КА по сравнению с традиционно-используемыми средствами защиты, так как в отличие от сигнатурных СОА способны к обобщению имеющихся знаний и использованию их для обнаружения новых типов КА.

Список используемых источников

1. Лукацкий А. В. Обнаружение атак. 2 изд. СПб. : БХВ – Санкт-Петербург, 2003. 624 с.

2. Хайкин С. Нейронные сети: полный курс. 2-е издание: пер. с англ. М. : Издательский дом «Вильямс», 2006. 1104 с.

3. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы. М. : Горячая линия – Телеком, 2004. 452 с.

4. The Unreasonable Effectiveness of Recurrent Neural Networks [Электронный ресурс]. URL: http://karpathy.github.io/2015/05/21/rnn-effectiveness (дата обращения: 30.05.2017).

УДК 621.391.28

ФОРМАЛИЗАЦИЯ ПРОТОКОЛОВ ПРОСТОЙ АУТЕНТИФИКАЦИИ В МУЛЬТИСЕРВИСНОЙ СЕТИ НА ТЕХНОЛОГИИ IP-QoS

В. В. Кириллов, Р. С. Кокаева, Н. Н. Мошак

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

Построение защищенной национальной мультисервисной сети связи является актуальной задачей современного информационного общества. Использование механизмов защиты требует формализации их работы и оценки влияния на характеристики базовых мультимедийных потоков с учетом поддержания требуемого качества обслуживания. Модели протоколов простой аутентификации равноправного логического объекта и отправителя данных в мультисервисной сети позволяют частично решить эту задачу.

мультисервисная сеть связи, инфотелекоммуникационная транспортная система, протоколы аутентификации, информационная безопасность.

Известно, что механизмы защиты вносят протокольную, временную и потоковую избыточность в информационное окружение сети [1]. В этой связи является актуальным построение моделей механизмов аутентификации и интеграции их в модели процессов передачи базового мультимедийного трафика в мультисервисной сети (МСС) и, в частности, в модели ее инфотелекоммуникационной транспортной системы (ИТС) с учетом поддержания требуемого качества их обслуживания в сессии [1].

Механизм «Аутентификация» реализует в сети одноименную базовую услугу аутентификации разноуровневых элементов [2, 3]. Механизмы аутентификации позволяют проверить подлинность личности участника взаимодействия, а также данных, безопасным и надежным способом. Аутентификация (как и прочие службы безопасности) может быть обеспечена только в контексте выработанной стратегии безопасности. Процедуры ау-

тентификации пользователей задействуются при установлении мультимедийного соединения, а также в сеансе связи, и напрямую связаны с интенсивностью поступления потока мультимедийных вызовов и загрузке сети в сессии.

Протоколы аутентификации можно классифицировать в соответствии со следующими параметрами: типу аутентификации, тип используемой криптосистемы (шифра), вид реализации криптосистемы, количеству обменов служебной информацией между субъектами. Дополнительно они могут различаться наличием диалога и доверия между субъектами, а также использованием в протоколах отметок времени. Обобщенная классификация протоколов аутентификации в соответствии с данными параметрами представлена на рис. 1 [4].

Для обеспечения обмена информацией аутентификации могут использоваться перечисленные ниже методы:

а) использование аутентифицирующей информации, например, паролей, присваиваемых отправителем данных и проверяемых получателем данных;

б) криптографические процедуры;

в) использование характеристик и/или принадлежности объекта.

Рис. 1. Общая классификация протоколов аутентификации

При использовании криптографических процедур они должны сочетаться с протоколами квитирования установления связи, что обеспечивает

защиту от воспроизведения. Процедуры аутентификации участников информационного обмена могут использоваться совместно с:

а) уплотнением времени и синхронизацией;

б) двух- и трехкратным квитированием установления связи (для односторонней и взаимной аутентификации, соответственно);

в) услугами причастности, обеспечиваемыми цифровой подписью и/или процедурами нотаризации.

Как правило, реализация указанных механизмов базируется на установлении дополнительных ассоциаций, описываемых многофазными системами массового обслуживания (СМО), на фазах установления и перед подключением мультимедийного соединения и порождает дополнительный служебный трафик на фазе установления мультимедийной сессии, обслуживаемый, например, с относительным или абсолютным приоритетом по отношению к базовому типу трафика на транзитных маршрутизаторах при аутентификации и/или авторизации соединения (субъекта) объектом доступа в дополнительной транзакции после установления сессии или при аутентификации данных в сессии [1].

Различают простую аутентификацию и строгую аутентификацию.

Простая аутентификация может быть осуществлена различными способами:

1) ***Простая аутентификация без защиты*** (1): а) отправитель *i* передает получателю в открытом (незащищенном) виде свой идентификатор (имя) *IDi* и (необязательно) пароль *Pi* за время $t_{i,j}^{\text{прд}\,IDi,Pi}$; б) получатель *j* передает *IDi* и *Pi* за время $t_{j,CA}^{\text{прд}\,IDi,Pi}$ центру аутентификации (СА) для сопоставления за время $t_{CA}^{\text{обр}\,Pi}$ с *Pi*, который хранится у него в качестве атрибута; в) СА подтверждает или отрицает получателю *j* действительность удостоверений за время $t_{CA,j}^{\text{прд}\,Pi}$; 4) успешность или неуспешность аутентификации может быть сообщена отправителю *i* за время $t_{j,i}^{\text{прд}\,Pi}$.

Время, затрачиваемое на осуществления процесса простой аутентификации можно формализовать аддитивной формой вида:

$$t_{\text{б/з}}^{\text{аут}} = t_{i,j}^{\text{прд}\,IDi,Pi} + t_{j,CA}^{\text{прд}\,IDi,Pi} + t_{CA}^{\text{обр}\,Pi} + t_{CA,j}^{\text{прд}\,Pi} + t_{j,i}^{\text{прд}\,Pi}. \quad (1)$$

2) ***Простая аутентификация с защитой*** (2) с применением хэш-функции *h*(*): а) отправитель *i* формирует за время t_{H1i} защищенную идентифицирующую информацию (хэшкод) $H_1i = h_1(\text{I}Di, Pi, nonce)$ применением хэш-функции $h_1(*)$ от выделенного имени пользователя *IDi*, пароля пользователя *Pi* и одноразовых параметров (*nonce*): случайных чисел r_i, временных меток t_i, номеров последовательностей N_i, формируемых посредством выработки одноразового значения из монотонно возрастающей последовательности (например, меток времени) или случайных чисел со-

ответствующей длины (хэш-функцией называется односторонняя функция $h(M)$, преобразующая сообщение M произвольной длины в выходной хэшкод (дайджест) постоянной длины H с применением или без применения секретных параметров и не позволяющее осуществить обратное преобразование); б) отправитель i передает получателю аутентификатор вида $Aj = IDi, PI, nonce, H_1i$ за время $t_{i,j}^{\text{прд}\,Aj}$. 3) получатель j проверяет хэшкод Hi отправителя. Для этого он генерирует локальную копию хэшкода $(H_1i)j$ за время $t_{(H1i)j}$ и сравнивает с принятым значением хэшкода H_1i за время $t_j^{\text{обр}\,Aj}$.

Процедура может быть усилена применением отправителем повторно однонаправленной функции $h_2(*)$ и формированием хэшкода $H_2i = h_2(IDi, Pi, nonce, H_1i)$ за время t_{H2i}.

Время, затрачиваемое на осуществления процесса простой аутентификации с защитой можно формализовать аддитивной формой вида

$$t_{\text{с/з}}^{\text{аут}} = t_{H1i} + t_{H2i} + t_{i,j}^{\text{прд}\,Aj} + t_{(H1i)j} + t_j^{\text{обр}\,Aj}. \qquad (2)$$

В качестве примеров использования одноразовых паролей можно привести методы аутентификации центрального сервера, конечного пользователя или и того, и другого по протоколу S/Key, механизмы аутентификации в каналах модемного доступа, организованных по протоколу Point-to-Point Protocol (PPP), которые включают использование протоколов Password Authentication Protocol (PAP) или SPAP, Challenge Handshake Protocol (CHAP) или Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Extensible Authentication Protocol (EAP), TACACS+ и Remote Access Dial-In User Service (RADIUS). Эти протоколы используются, в основном, центральными серверами сетевого доступа (NAS) и маршрутизаторами, которые связаны с сервером PPP через коммутируемые каналы или выделенные каналы связи [4].

Для расчета времени передачи трафика безопасности и его обработки можно воспользоваться подходом, изложенным в [5, 6], при условии, что речевые пакеты в МСС обслуживаются с абсолютным приоритетом (с дообслуживанием) по отношению к пакетам данных, а пакеты трафика безопасности обслуживаются аналогично пакетов данных.

Список используемых источников

1. Мошак Н. Н. Формализация и оценка процессов представления механизмов защиты в мультисервисной сети. Общий подход // Электросвязь. 2012. № 3. С. 30–35.

2. Мошак Н. Н. Особенности архитектуры мультисервисных сетей с услугами безопасности // Электросвязь. 2007. № 5. С. 34–40.

3. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть. 2. Архитектура защиты. М. : ИПК Издательство стандартов, 1999.

4. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. СПб. : БХВ-Петербург, 2000. 320 с.: ил.

5. Мошак Н. Н. Теоретические основы проектирования транспортной системы инфокоммуникационной сети: учеб. пос. для вузов. СПб. : Энергомашиностроение, 2006. 159 с. ИА

6. Мошак Н. Н. Метод расчета характеристик транспортной системы инфокоммуникационной сети на технологии IP-QoS // Электросвязь. 2006. № 3. С. 44–47.

УДК 621.391.28

ФОРМАЛИЗАЦИЯ ПРОТОКОЛОВ СТРОГОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ АССИМЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ В МУЛЬТИСЕРВИСНОЙ СЕТИ НА ТЕХНОЛОГИИ IP-QoS

В. В. Кириллов, Р. С. Кокаева, Н. Н. Мошак

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

Использование механизмов защиты требует формализации их работы и оценки влияния на характеристики базовых мультимедийных потоков с учетом поддержания требуемого качества обслуживания. Модели протоколов строгой аутентификации на основе ассиметричных алгоритмов шифрования в мультисервисной сети позволяют решить эту задачу с учетом внесения временной, протокольной и потоковой избыточности в сетевое окружение сети.

мультисервисная сеть связи, инфотелекоммуникационная транспортная система, протоколы строгой аутентификации, информационная безопасность

Строгая аутентификация на основе асимметричных алгоритмов шифрования, как и строгая аутентификация на основе симметричных алгоритмов шифрования, основывается на наличии у пользователей аутентифицирующих их личных (секретных) ключей. Использование асимметричных шифров можно свести к трем аспектам применения [1]: 1) шифрование/дешифрование, при котором отправитель *i* шифрует сообщение *M* (или его сжатое отображение *H*, являющееся функцией *M*) с использованием открытого ключа *Pj* получателя *j*; 2) цифровая подпись $S^i(M)$, когда отправитель *i* «подписывает» сообщение *M* с помощью личного ключа S_i; 3) обмен ключами, при котором происходит обмен сеансовым ключом с применением личных ключей одной и/или обеих сторон.

Процедура аутентификации в этом случае выглядит следующим образом (1) (временем, затраченным на формирование открытого и секретного ключей пользователем, будем пренебрегать). Отправитель шифрует на своем секретном ключе S_i сообщение M за время $t_i^{\text{ш}M(Si)}$ и передает шифрованное сообщение Mi^* за время $t_{ij}^{\text{прд}Mi^*}$. Расшифровав сообщение Mi^* на открытом ключе отправителя P_i за время $t_j^{Mi(Pi)}$ получатель аутентифицирует его. Таким образом, процесс аутентификации в этом случае формализуется следующим выражением:

$$t_{\text{строг,асим ш}}^{\text{аут}} = t^{\text{аут}Pi,Pj} + t_i^{\text{ш}M(Si)} + t_{ij}^{\text{прд}Mi^*} + t_j^{Mi(Pi)} \quad (1)$$

Открытые ключи могут быть получены по запросу из центра *CA* или переданы непосредственно отправителями в процессе аутентификации Формализация процедуры обмена и аутентификации открытых ключей субъектов информационного обмена $t^{\text{аут}Pi,Pj}$ с центром *CA* и без него приведена ниже. Существует три метода выработки парных ключей: 1) пользователь сам генерирует собственные парные ключи; 2) парные ключи генерирует третья сторона; 3) парные ключи генерирует сертификатным руководящим центром *CA*. Мы будем рассматривать только первый метод. В общем случае механизм формирования разделяемого секрета по открытому каналу состоит в следующем. Отправитель вырабатывает разовый личный (секретный) ключ S_i (генерирует случайное число) и вычисляет открытый ключ $P_i = \alpha^{Si} (\text{mod}\, p)$, который отсылает получателю. Получатель аналогичным образом вырабатывает разовый личный ключ S_j, вычисляет открытый ключ $P_j = \alpha^{S_j} (\text{mod}\, p)$ и отсылает его отправителю. Оба корреспондента сейчас могут вычислить общий секретный сеансовый ключ K_{ij}: $K_{ij} = (P_j)^{Si} = (\alpha^{Sj})^{Si} = \alpha^{SjSi} (\text{mod}\, p)$ и $K_{ij} = (P_i)^{Sj} = (\alpha^{Si})^{Sj} = \alpha^{SiSj} (\text{mod}\, p)$. Таким образом, любая транзакция по созданию сеансового ключа в двухключевой криптосистеме в общем случае включает в себя три фазы: а) фазу генерации общего (разделяемого) сеансового секрета K_{ij}; б) фазу взаимного обмена общего сеансового секрета K_{ij} между корреспондентами и в) фазу аутентификации корреспондентов при создании общего сеансового секрета.

а) *Фаза генерации сеансового ключа* K_{ij} включает в себя 1) время, затрачиваемое: на аутентификацию $t_{Pi,j}^{CA\text{аут}}$ открытых ключей пользователей P_i и P_j, получаемых по запросу из центра сертификации *CA* (*Authentification Center*) или без его участия – $t_{Pi,j}^{\text{аут}}$ и 2) собственно время на формирование, общего секрета t_{Kij}. Время $t_{Pi,j}^{CA\text{аут}}$ в свою очередь включает время $t_{i,CA}^{\text{запр}Pj}$, $t_{j,CA}^{\text{запр}Pi}$ на запрос каждой из сторон информационного обмена сертификата партнера из центра сертификации *CA*; время $t_{CA,i}^{\text{отв}Pj}$, $t_{CA,j}^{\text{отв}Pi}$ на ответ *CA* (пересылку

соответствующих сертификатов) каждой из сторон и время $t_j^{\text{аут}\,CA}$, $t_i^{\text{аут}\,CA}$, затрачиваемое на проверку пользователями полученных сертификатов на открытом ключе *CA*.

Если центр сертификации *CA* не участвует в процессе аутентификации, то в этом случае корреспонденты обмениваются открытыми ключами самостоятельно за время $t_{i,j}^{\text{прд}\,Pi}$ и $t_{j,i}^{\text{прд}\,Pj}$.

б) *Фаза взаимного обмена сеансовыми ключам* включает в себя время их передачи в двух направлениях между корреспондирующими парами $t_{Kij}^{\text{прд}}$.

в) *Фаза аутентификации корреспондентов* в зависимости от применяемых протоколов включает себя 1) время на работу протокола простой аутентификации без защиты $t_{\text{б/з}}^{\text{аут}}$ или протокола простой аутентификации с защитой $t_{\text{с/з}}^{\text{аут}}$; 2) время на работу протоколов строгой аутентификации в соответствии со стандартом X.509 с учетом одно-, двух- или трехкратном обмене аутентификационными сообщениями $t_{\text{строг}}^{\text{аут}}$.

Таким образом, транзакции по созданию сеансового ключа K_{ij} в двухключевой криптосистеме могут быть многофазовой моделью формализовать следующими аддитивными формами:

$$\text{а)}\ T_{Kij}^{CA1}=(t_{Pi,j}^{CA\text{аут}}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{б/з}}^{\text{аут}}\ (t_{\text{с/з}}^{\text{аут}})=$$

$$=(t_{i,CA}^{\text{запр}\,Pj}+t_{j,CA}^{\text{запр}\,Pi}+t_{CA,i}^{\text{отв}\,Pj}+t_{CA,j}^{\text{отв}\,Pi}+t_j^{\text{аут}\,CA}+t_i^{\text{аут}\,CA}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{б/з}}^{\text{аут}}(t_{\text{с/з}}^{\text{аут}}),$$

при наличии сертификатного руководящего органа или центра сертификации *CA* с применением протокола простой аутентификации без защиты (с защитой) пользователей;

$$\text{б)}\ T_{Kij}^{CA2}=(t_{Pi,j}^{CA\text{аут}}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{строг}}^{\text{аут}}=$$

$$=(t_{i,CA}^{\text{запр}\,Pj}+t_{j,CA}^{\text{запр}\,Pi}+t_{CA,i}^{\text{отв}\,Pj}+t_{CA,j}^{\text{отв}\,Pi}+t_j^{\text{аут}\,CA}+t_i^{\text{аут}\,CA}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{строг}}^{\text{аут}},$$

при наличии центра сертификации *CA* и с применением протоколов строгой аутентификации пользователей.

$$\text{в)}\ T_{Kij}^{1}=(t_{Pi,j}^{\text{аут}}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{б/з}}^{\text{аут}}(t_{\text{с/з}}^{\text{аут}})=t_{i,j}^{\text{прд}\,Pi}+t_{j,i}^{\text{прд}\,Pj}+2t_{Kij}+2t_{Kij}^{\text{прд}}+t_{\text{б/з}}^{\text{аут}}\ (t_{\text{с/з}}^{\text{аут}}),$$

без центра сертификации *CA* с применением протокола простой аутентификации без защиты (с защитой) пользователей;

$$\text{г)}\ T_{Kij}^{2}=(t_{Pi,j}^{\text{аут}}+2t_{Kij})+2t_{Kij}^{\text{прд}}+t_{\text{строг}}^{\text{аут}}=t_{i,j}^{\text{прд}\,Pi}+t_{j,i}^{\text{прд}\,Pj}+2t_{Kij}+2t_{Kij}^{\text{прд}}+t_{\text{строг}}^{\text{аут}},$$

без центра сертификации *CA* с применением протоколов строгой аутентификации пользователей.

Таким образом, процесс шифрования в двухключевой криптосистеме в общем виде можно формализовать следующей аддитивной формой (2):

$$t_{\text{убш\_асим}} = T_{Kij}^{CA1(2)}(T_{Kij}^{1(2)}) + t_{i,j\,\text{убш}}, \quad (2)$$

где $t_{i,j\,\text{убш}}$ – время шифрования/дешифрования сообщения на симметричном ключе K_e на сторонах участников обмена (временем генерации ключа K_e на стороне отправителя пренебрегаем). Формализация процессов аутентификации $t_{\text{б/з}}^{\text{аут}}$ ($t_{\text{с/з}}^{\text{аут}}$), $t_{\text{строг}}^{\text{аут}}$ приведены ниже. Временная избыточность, вносимая механизмами шифрования в информационное окружение сети при проведении криптографических процедур, должна быть учтена в общем временном балансе передачи пакетов данных по аналогии с задержкой, вносимой механизмами пакетизации [2, 3]. Время, затрачиваемое на формирование общего секрета, должно быть учтено в общем балансе времени длительности мультимедийной сессии [4, 5].

Строгая аутентификация на основе алгоритмов электронной цифровой подписи. ЭЦП – это зашифрованное каким-либо секретным ключом отправителя (не обязательно совпадающего с ключом, использованным для шифрования сообщения) значение хэш-функции $H = h(M)$. Процесс шифрования хэшкода сообщения и называется подписью S^i. Электронная подпись S^i добавляется к сообщению M и может шифроваться вместе с ним при необходимости сохранения данных в тайне.

Симметричная ЭЦП с центром CA. Ключи симметричного шифрования ЭЦП $K_i^{S\text{ЭЦП}}$ вырабатываются и распределяются центром доверия по аналогии с одноключевыми криптосистемами. При этом у каждого из пользователей есть собственный секретный ключ ЭЦП $K_i^{S\text{ЭЦП}}$, копия которого хранится в центре доверия *CA*. Отправитель вычисляет значение хэш-функции $H_i = h(M)$ за время t_i^{Hi} и ЭЦП $S^i = \text{E}_{K_i^S}(h(M))$ за время t_i^{Si}, присоединяет ее к сообщению M и передает файл $Mi^* = (M \,||\, S^i)$ получателю за время $t_{i,j}^{\text{прд}Si}$. Получатель j выделяет ЭЦП S^i и направляет ее в центр доверия *CA* за время $t_{j,CA}^{\text{прд}Si}$. Центр, расшифровывает S^i за время $t_{CA}^{\text{рщ}Si}$ перешифровывает значение хэш-функции H_i с использованием личного ключа ЭЦП получателя $K_j^{S\text{ЭЦП}}$ за время t_{CA}^{Si} и возвращает ЭЦП S_{CA}^j получателю за время $t_{CA,j}^{\text{прд}Sj}$. Последний, расшифровав ЭЦП S_{CA}^j на собственном ключе $K_j^{S\text{ЭЦП}}$ за время $t_j^{\text{рщ}Sj}$, получает значение хэш-функции $H_j^{CA} = D_{K_j^S}(S_{CA}^j)$. Вычислив значение хэш-функции принятого сообщения H_j за время t_j^{Hj} и сравнив его с полученным от центра H_j^{CA} за время $t_j^{\text{сравн}H}$, получатель принимает решение об истинности либо ложности полученного сообщения. Если $H_i^{CA} = H_j$, сообщение истинно, если нет, ложно. В этой схеме невозможность подделки базируется на следующих соображениях: а) ключ $K_i^{S\text{ЭЦП}}$ имеется

только у i и CA, б) сообщение M имеется только у i и j. Поэтому CA не может создать ЭЦП (у CA нет сообщения M). Ни один другой абонент не может создать ЭЦП, так как не имеет ключа отправителя $K_i^{S\text{ЭЦП}}$. Существуют усиления этой схемы, основанные на использовании еще одного центра доверия. Весь процесс создания/проверки ЭЦП можно формализовать следующей формулой (3):

$$t^{\text{аут}}_{\text{строг,сим ЭЦП}(CA)} = t_i^{Hi} + t_i^{Si} + t_{i,j}^{\text{прд}Si} + t_{j,CA}^{\text{прд}Si} + t_{CA}^{\text{рщ}Si} + t_{CA}^{Si} + t_{CA,j}^{\text{прд}Sj} + t_j^{\text{рщ}Sj} + t_j^{Hj} + t_j^{\text{срвавн}H}. \quad (3)$$

*Симметричная ЭЦП без центра CA***.** При получении файла ($M \| S_i$) получатель отделяет ЭЦП S^i, создает ЭЦП $\tilde{S}^i$ на секретном ключе отправителя $K_i^{S\text{ЭЦП}}$ за время $t_j^{\tilde{S}i}$ и сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения) за время $t_j^{\text{срвавн}H}$. Формализация процесса аутентификации в этом случае имеет следующий вид (4):

$$t^{\text{аут}}_{\text{строг,сим ЭЦП}} = t_i^{Hi} + t_i^{Si} + t_{i,j}^{\text{прд}Si} + t_j^{\tilde{S}i} + t_j^{\text{срвавн}H}. \quad (4)$$

Разновидностями симметричной ЭЦП являются контрольные суммы CRC и коды аутентификации сообщений (*message authentication code*, MAC), известные также как коды проверки подлинности данных (*data authentication code*, DAC).

Асимметричная ЭЦП базируется на двухключевых криптографических алгоритмах, в которых предусматривается использование двух ключей – открытого Pi и личного Si. Однако при создании ЭЦП здесь меняются их роли: для подписывания сообщения M используется личный ключ отправителя Si, а для проверки, – его открытый ключ Pi. Двухключевые криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными абонентами (пользователями) криптосистемы. Использование однонаправленных функций в асимметричных системах ЭЦП не позволяет злоумышленнику вычислить личный ключ отправителя, применяемый к хэшкоду. Например, в ЭЦП S^{RSA} RSA – это задача факторизации, а в ЭЦП S^{EGSA} Эль Гамаля – это задача дискретного логарифмирования.

Рассмотрим обобщенную схему формирования и проверки ассиметричной ЭЦП на примере ЭЦП RSA состоит в следующем. Перед отправкой сообщения M (блок данных, файл, таблица) вычисляется его хэш-функция $H_i = h(M)$ за время t_i^{Hi}. Затем вычисляется ЭЦП (например, *RSA*) $S^{iRSA} = \text{E}_{\text{Si}}(H_i)$ с применением личного ключа отправителя Si за время t_i^{SiRSA} и файл ($M \| S^{iRSA}$) отправляется получателю за время $t_{i,j}^{\text{прд}SiRSA}$. При получении пары ($M \| S^{iRSA}$) получатель j вычисляет хэш-значение M двумя разными

способами. Во-первых, он восстанавливает хэшкод $\tilde{H}_i = \mathrm{D}_{P_i}(E_{S_i}(H_i))$, применяя криптографическое преобразование ЭЦП с использованием открытого ключа отравителя P_i за время $t_j^{\tilde{H}i}$. Во-вторых, получатель рассчитывает хэш-значение сообщения $H_j = h(M)$ с помощью аналогичной хэш-функции $h(*)$ за время t_j^{Hj} и сравнивает эти значения за время $t_j^{\text{срравн}H}$. Если эти два значения совпали, получатель считает, что файл подлинный. Невозможность подделки ЭЦП гарантируется сохранением в тайне личного ключа отправителя S_i, т. е. ответственность возлагается на пользователя. Формализация процесса аутентификации в этом случае дается выражением (5):

$$t^{\text{аут}}_{\text{строг,асим ЭЦП}} = t_i^{Hi} + t_i^{SiRSA} + t_{i,j}^{\text{прд}SiRSA} + t_j^{\tilde{H}i} + t_j^{Hj} + t_j^{\text{срравн}H}. \quad (5)$$

Потоковая избыточность, вносимая при аутентификации субъектов мультимедийной сессии на фазе ее установления, должна учитываться при расчете производительности сигнальной системы и ИТС [4, 5], а протокольная и временная избыточность трафика безопасности при передаче его в сессии при аутентификации данных должна быть учтена в задачах анализа ИТС [3, 6].

Список используемых источников

1. Молдовян А. А., Молдовян Н. А. Введение в криптосистемы с открытым ключом. СПб. : БХВ-Петербург, 2005. 288 с.: ил.

2. Мошак Н. Н. Формализация и оценка процессов представления механизмов защиты в мультисервисной сети. Общий подход // Электросвязь. 2012. № 3. С. 30–35.

3. Мошак Н. Н. Теоретические основы проектирования транспортной системы инфокоммуникационной сети: учеб. пос. для вузов. СПб. : Энергомашиностроение, 2006. 159 с. ИА

4. Яшин А. И., Мошак Н. Н., Цветков Д. Б. Модель системы сигнализации пакетной мультисервисной сети военно-морского флота РФ с учетом трафика безопасности // Морская радиоэлектроника. 2016. 2 (56). С. 14–17.

5. Яшин А. И., Мошак Н. Н. Модель протокола Диффи-Хеллмана // Техника средств связи: научно-технический сборник. 2016. Вып. 4 (143). СПб. : Изд-во Политехн. ун-та. С. 6–9.

6. Мошак Н. Н. Метод расчета характеристик транспортной системы инфокоммуникационной сети на технологии IP-QoS // Электросвязь. 2006. № 3. С. 44–47.

УДК 004.93; 004.5

АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ РАЗРАБОТКИ ПРИЛОЖЕНИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

А. В. Козин, Ю. Н. Островский

Военная академия связи им. Маршала Советского Союза С. М. Буденного

«Дополненная реальность» одна из последних достижений науки и техники. К технологиям дополненной реальности относятся те проекты, которые направлены на дополнение реальности виртуальными объектами. Данная технология имеет широкое применение в архитектуре, в маркетинге, в компьютерных играх, военном деле.

дополненная реальность, AR, единое информационное пространство.

Наибольших успехов в этой области на сегодняшний день достигли военные. Они же были основоположниками этой технологии. В военном применении «Дополненная реальность» (англ. *Augmented reality*, AR) (ДР) – это вывод оперативной информации на лобовое стекло, либо дисплей, отображающий тактическую информацию, например, о целях на фоне наблюдаемой обстановки. Военные продолжают проявлять к этой технологии повышенный интерес, рассматривая ее как наиболее перспективную для персональных устройств, входящих в экипировку солдата недалекого будущего. При помощи этих устройств военные планируют интегрировать каждого бойца в единое информационное пространство.

Рассмотрим несколько программных средств разработки приложений дополненной реальности [1].

Vuforia

Vuforia – одна из самых популярных в мире платформ, которая поможет вам разрабатывать дополненную реальность.

Программное обеспечение реализует следующие функции: распознавание различных типов визуальных объектов (куб, цилиндр, плоскость), распознавание текста и окружающей среды, VuMark (комбинация изображения и QR-кода). Кроме того, используя Vuforia Object Scanner, вы можете сканировать и создавать объектные метки. Процесс распознавания может быть реализован с использованием локальной или облачной базы данных. Плагин Unity очень мощный и прост в интеграции.

Все плагины и функциональные возможности платформы бесплатны, но включают водяные знаки Vuforia. Ограничения относятся только к чис-

лу VuMark и количеству взаимодействий с облачной базой данных. Платный план без водяных знаков и с определённым количеством распознаваний через облако стоит $99 в месяц [2].

EasyAR

EasyAR – бесплатная и простая в использовании альтернатива Vuforia. Последняя версия EasyAR (1.3.1) поддерживает только распознавание изображений. Версия 2.0 будет включать следующие функции:

– распознавание 3D-объектов;
– восприятие окружающей среды;
– облачное распознавание;
– работа на смарт-очках;
– облачное развёртывание приложений.

Библиотека полностью бесплатна. Чтобы начать работу с EasyAR, нужно только зарегистрировать учётную запись и сгенерировать ключ плагина вашего Bundle ID. EasyAR легко интегрируется. Документация и примеры интуитивно понятны.

Wikitude

Wikitude – SDK Дополненной Реальности – комплект программ для разработчиков, который позволяет как создавать собственные AR-приложения с нуля, так и интегрировать AR-функционал в уже готовые приложения. Недавно Wikitude выпустила полностью новое мощное SLAM-решение для приложений дополненной реальности Wikitude SDK 6. Последняя версия – 6.1.

Wikitude SDK 6 имеет в арсенале следующие функции: отличное распознавание и отслеживание изображений, технологию трёхмерного слежения на базе SLAM, GEO Data (улучшенная работа с данными с географической привязкой), облачное распознавание (позволяет сохранять базы данных изображений в облаке).

Дополнительные улучшения:

– улучшенная функция Extended Tracking для сохранения положения метки, даже если она за пределами обзора камеры;
– расширенные настройки камеры;
– повышенная стабильность отслеживания изображений (снижения дрожания);

Wikitude предлагает попробовать бесплатную пробную версию с водяным знаком и полной функциональностью платформы. Стоимость SDK 6 Wikitude начинается с €1990.

Плагин Unity предоставляет инструменты для создания базы данных изображений и 3D-объектов. Он не работает с редактором Unity, что усложняет процесс разработки.

ARToolKit

ARtoolKIt – это библиотека трекинга для дополненной реальности с открытым исходным кодом.

ARtoolKit реализует следующие возможности:

– трекинг позиции/ориентации для устройств с обычными и стереоскопическими камерами;

– отслеживание простых чёрных квадратов;

– отслеживание плоских изображений;

– калибровка камеры и стереоскопической оптики;

– плагины для Unity и OpenSceneGraph;

– поддержка оптических шлемов и очков;

– бесплатное программное обеспечение с открытым исходным кодом;

– достаточная скорость для приложений дополненной реальности реального времени.

Разнообразие функций затрудняет интеграцию библиотеки и занимает больше времени для изучения всех параметров и настроек.

Kudan

Согласно различным обзорам и сравнениям эффективности, Kudan является главным конкурентом Vuforia и очень упрощает разработку дополненной реальности.

Используя технологию SLAM, Kudan позволяет распознавать простые изображения и 3D-объекты и обеспечивает лёгкую генерацию базы данных в редакторе Unity.

У Kudan также есть некоторые недостатки: редактор сбоит (иногда это основная причина сбоев приложений на устройствах), есть трудности с установкой лицензионного ключа (он не всегда подходит). Тем не менее, Kudan – это продвинутый коммерческий продукт, поэтому в вашем распоряжении служба поддержки.

Бесплатная версия предназначена только для тестирования приложений. Стоимость платной лицензии составляет $1230. Kudan легко интегрировать, но, с другой стороны, проблемы с редактором Unity усложняют процесс разработки.

Список используемых источников

1. Киргизова Е. В., Шакиров И. Ш., Захарова Т. В., Рубцов А. В. «Дополненная реальность»: Инновационная технология организации образовательного процесса по информатике // Современные проблемы науки и образования. 2015. N 4. С. 25–28.
2. Кирьякиди С. И. Дополненная реальность и перспективы её применения в строительной отрасли. URL: http://isicad.ru/ru/articles.php?article_num=16724 (дата обращения 20.01.2018).

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком

УДК 004.384

МЕТОДЫ И СРЕДСТВА ВИЗУАЛИЗАЦИИ ИНТЕРФЕЙСА ДЛЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «УМНЫЙ ДОМ» НА БАЗЕ UX И UI ДИЗАЙНА

Л. П. Козлова, В. К. Николаенко

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

Рассматривается визуализация данных, как система передачи сложных идей и данных в виде, который обеспечивает наиболее эффективную работу человека. В современном информационном обществе визуализация является важным аспектом представления информации и процесса оптимизации работы различных систем с пользователем и мощным инструментом продуманного насыщения дизайна в любом его виде.

умный дом, интерфейс, информационные технологии, UX дизайн, UI дизайн, экономичность, комфорт.

Невозможно представить жизнедеятельность современного человека без использования девайсов, которые стали частью нашей повседневной жизни, а информационные технологии все глубже внедряются в нее. Стремление человека усовершенствовать свой быт, позволяющего сделать его как можно более комфортным, безопасным и экономичным, способствует постоянному поиску новых возможностей.

Одной из современных технологий является создание умного (интеллектуального) дома, который будет заботиться о своих хозяевах, взяв на себя все бытовые проблемы.

Особенностью «Умного дома» является то, что его можно контролировать различными способами. От традиционных выключателей до современных смартфонов или планшетов. И ничто так не упростит взаимодействие с системой, как интерфейс, адаптированный не под специалиста, а под любого пользователя, понятный и функциональный.

Интерфейс предоставляет самый оптимальный доступ к управлению системой «умный дом» для того, чтобы пользователь мог настроить ее под свои критерии. Поэтому понятному и отлично продуманному интерфейсу отводится важное место в интеллектуальной системе. Он должен отражать основные задачи и не перегружаться излишними функциями и компонентами. Качественный интерфейс умного дома – это непременная составляющая системы, он является гарантом удобного и эффективного управления интеллектуальным домом, с которым легко и просто управляется пользователь [1].

При выборе интерфейса необходимо соблюдать следующие принципы:

– на экран должна поступать только необходимая информация, имеющая легко узнаваемые иконки;

– возможность блокировки некоторых функций для защиты от запуска нежелательной функции, возможность защиты страниц паролем;

– дизайн интерфейса должен быть в едином стиле и красив.

Разработка визуализации интерфейса для системы «умный дом» строится таким образом, чтобы создать его максимально привлекательным и удобным для оптимизации его взаимодействия с пользователем. Поэтому стоит начать с анализа самой системы, для того чтобы иметь представление о возможных комбинациях модулей, с уже существующих систем и интерфейсов для них. Необходимо создать дружественный интерфейс по отношению к пользователю. Однако это не всегда такая простая задача, как может показаться на первый взгляд, и порой требует не малого опыта проектирования. Главными требованиями является удобство, практичность и интуитивная понятность. Именно в этот момент вступают в игру такие понятия как UX и UI дизайн, которые зачастую путаются. Рассмотрим каждое из них по отдельности и определим их ключевые моменты [2].

С одной стороны, понятия UX дизайн и UI дизайн очень тесно связаны между собой, так как оба могут быть применены к (почти) любому продукту, решать задачи, связанные с дизайнерским аспектом продукта, быть ориентированы на комфорт пользователя.

С другой стороны, UX дизайн и UI дизайн имеют важные отличия, многие из которых похожи друг на друга.

UX (*User Experience Design*) дизайн включает в себя такие компоненты как информационную архитектуру, проектирование взаимодействия,

графический дизайн и контент. Основные задачи, которые можно решить с помощью UX дизайна представлены на рис.

UI (*User Interface Design*) дизайн включает в себя определенный набор графически оформленных технических элементов (кнопки, чекбоксы, селекторы и другие поля) и позволяет пользователю организовать взаимодействие с программой / сайтом.

Рисунок. Задачи, решаемые UX дизайном

Таким образом UX дизайн часто ошибочно относят к Визуальному/UI дизайну, потому что для многих людей слово «дизайн» сразу же ассоциируется с цветами и графикой. Но UX дизайн другой.

Пользовательский интерфейс (UI) определяется как средство связи между человеком и системой. С увеличением популярности персональных компьютеров и мобильных девайсов этот термин обычно приравнивают к «графическому пользовательскому интерфейсу (*graphical user interface* (GUI))» – внешний вид и ощущение, презентация и интерактивность продукта [3].

Несмотря на то, что пользовательский интерфейс является очевидно-важной частью опыта взаимодействия, UX дизайнеры не создают вещи, сравнимые по ощущениям с визуальным интерфейсом дизайнера. UX дизайнеры создают функции, которые стоят за визуальной составляющей: процесс, который делает так, чтобы продукт работал хорошо для людей, которые им пользуются. UX соединяет разрыв, между тем как что-то выглядит и как оно работает и чувствуется.

Использование визуализации интерфейса существенно облегчит любым пользователям доступ к системе «умный дом» с последующие настройкой и оптимизацией для себя, и теперь гораздо проще пользоваться набором модулей данной системы. Теперь не нужно иметь большое количество неудобных приложений, оптимизированных под определённые устройства и операционные системы, а достаточно пользоваться одним приложением с оптимизированным интерфейсом, что заметно упрощает пользование такой сложной системой как «умный дом».

Список используемых источников

1. Какие бывают веб-интерфейсы для управления умным домом [Электронный ресурс] // URL: http://videokontroldoma.ru/interfejsy-umnogo-doma/ (дата обращения 24.03.2018).
2. Каспер систем. Что такое UX и UI дизайн – особенности и отличия [Электронный ресурс] // URL: https://www.kasper.by/blog/chto-takoe-ux-i-ui-dizain/ (дата обращения 24.03.2018).
3. Всё, что вам следует знать о UX дизайне [Электронный ресурс] // URL: http://wordyblend.com/chto-takoe-ux/ (дата обращения 24.03.2018).

УДК 004.89

ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ АКАДЕМИЧЕСКИХ ИССЛЕДОВАНИЙ В ОБЛАСТИ АНАЛИЗА ДАННЫХ

О. Ю. Колесниченко[1], Ю. Ю. Колесниченко[1], А. Л. Мазелис[2], Л. С. Мазелис[2], Г. Н. Смородин[3], Д. А. Яковлева[2]

[1]Security Analysis Bulletin
[2]Владивостокский государственный университет экономики и сервиса
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована и практически подтверждена возможность и актуальность проведения исследований в области анализа данных силами сотрудников нескольких вузов – академических партнеров компании Dell EMC. Разработана система корреляции проектных предложений и компетенций академических команд. На основе пилотных проектов выявлены наиболее востребованные тематические направления исследований: глобализация экономических процессов и анализ данных в области медицины. Подтвержден должный уровень полученных результатов путем апробации результатов на англоязычных IEEE конференциях и включении публикаций в международные наукометрические базы.

распределенные академические исследования, анализ данных, глобалистика, академическое партнерство.

По мере лавинообразного роста информационных потоков возрастает интерес к поиску скрытых зависимостей между различными информационными выборками, срезами и потоками. Актуальность исследования данного вида подтверждается появлением новой Науки о Данных (*Data Science*), назначение которой заключается в поиске новых алгоритмов и методов анализа данных с целью моделирования новых соотношений между как уже исследованными, так и неисследованными массивами дан-

ных. При этом данные, как правило, не структурированы, отрывочны, располагаются в различных источниках и обладают большим разнообразием.

Отличительной особенностью проектов по анализу данных является относительно легкая возможность разделения их на независимые этапы, которые могут выполняться отдельными аналитиками или лабораториями. Это позволяет привлекать к проведению исследований команды различных учебных заведений, основывая выбор на наличии соответствующих компетенций и временных возможностей для решения существующих задач. Существенной составляющей является возможное отсутствие финансовых обязательств между различными командами. Результат работы рассматривается как общее достижение и проявляется в виде последовательности публикаций в ведущих научных изданиях и выступлений на международных конференциях.

В рамках Академического партнерства компании Dell EMC были сделаны предложения по участию в некоммерческих распределенных исследованиях по анализу данных для 150 вузов – членов партнерства из России и ряда других стран. В результате сформировалась команда, в которую вошли несколько вузов, в том числе (как проявивших наибольшую активность) Московский государственный университет, Владивостокский государственный университет экономики и сервиса. Тематика исследований определялась потребностями рынка (на основе анализа научных статей), возможностями доступа к массивам исходных данных и наличием компетенций в области анализа данных [1, 2, 3]. Активно использовались сложившиеся отношения с рядом научных и медицинских организаций, а также с рядом коммерческих компаний с целью получения легального доступа к исходным массивам данных.

Сотрудничество с Московским государственным университетом

В результате сотрудничества с факультетом глобальных процессов МГУ в 2014–2015 гг. была проведена серия исследований в области глобальных процессов, поиск скрытых факторов в развитии стран. Были проанализированы «горячие» регионы планеты. Полученные результаты позволили составить рейтинг стран на основе текстовой морфологической аналитики Интернет-ресурсов [1].

Сотрудничество с Владивостокским государственным университетом экономики и сервиса

С учетом опыта сотрудничества ВГУЭС с региональными медицинскими учреждениями проводился анализ медицинских данных. Исходную информационную базу составили данные, регистрируемые медицинской информационной системой qMS компании СП.АРМ, за период с 2013 г.

по 2017 г. – установленные во время госпитализации (несколько разных больниц) коды клинических диагнозов по МКБ-10, отметки о количестве и видах проведенных обследований, процедур и операций [2]. Проанализированы выборки пациентов двух нозологических групп – артериальная гипертензия и сахарный диабет одного типа. Использовались математические методы: кластерный анализ с использованием языка программирования Python, бинарный рефлексивный код Грея, реализованный на языке Java, построение графов [3].

Перспективы развития распределенных академических исследований

Существует потенциальная возможность участия в исследованиях для студентов магистратуры вузов России и СНГ. Подобный подход позволяет студентам принять участие в реальных проектах, завершающихся научными публикациями и использовать результаты исследований для подготовки своих выпускных квалификационных работ (ВКР). Также, это потенциальная возможность для студентов получить опыт непосредственного профессионального взаимодействия с представителями бизнеса и других вузов, что крайне положительно влияет на развитие профессиональных компетенций и формирование портфолио молодого специалиста. В качестве негативного фактора, затрудняющего использование такого подхода, является сложность координации тематики исследований с требованиями к ВКР.

Взаимодействие с вузами Европейского Союза

Данная возможность обсуждалась при посещении вузов Финляндии и Эстонии. Результат обсуждения, к сожалению, не внушает оптимизма. Помимо негативных политических факторов присутствуют также факторы экономической природы, в основе которых лежит различное отношение к вопросам интеллектуальной собственности. Если в российских вузах проведение исследований ассоциируется с написанием научных статей и, по возможности, получением возмещения за потраченные усилия, то вузы ЕС в первую очередь заинтересованы в обсуждении создания и владения интеллектуальной собственностью. Тем не менее, нельзя полностью исключать возможность развития отношений с вузами ЕС, при этом следует учитывать различия ментального характера среди различных стран ЕС.

Можно предположить, что университеты стран Восточной Европы, где помимо учебных программ на местном и английском языках присутствуют также русскоязычные образовательные программы, более открыты для научного взаимодействия с российскими вузами [4].

Выводы

1. Академическое партнерство, как сообщество профессионалов, представляет собой инновационную экосистему, способную в реальном времени формировать творческие команды для проведения распределенных исследований в актуальных направлениях развития экономики, в том числе в области анализа больших данных.

2. Проведенные исследования показали реальную возможность творческого сотрудничества без финансовых обязательств, преследуя цель совместной публикации результатов исследований в ведущих изданиях.

3. Географически распределенные команды имеют преимущества, обусловленные более широкими возможностями для публикации результатов исследований, используя для этого как региональные, так и университетские конференции, при этом гибко решая вопрос участия в конференциях международного уровня в зависимости от места проведения конференций.

4. Существенной составляющей для формирования команды исследователей является новостная лента академического партнерства, использование которой позволяет оперативно распространять информацию о запуске новых проектов в области научных исследований.

Список используемых источников

1. Колесниченко О. Ю., Смородин Г. Н. Большие данные: социальные вызовы // Большая социология: расширение пространства данных. V социологическая Грушинская конференция: материалы конф., 12–13 марта 2015 г. М. : ВЦИОМ, 2015. С. 26–29.

2. Колесниченко О. Ю., Колесниченко Ю. Ю., Минушкина Л. О., Смородин Г. Н., Мартынов А. В., Пулит В. В., Долженков А. Н. Возможности применения бинарного кода Грея для аналитики Больших данных МИС: пациенты с СД 1 типа // Ремедиум. 2017. № 10. С. 38–47.

3. Колесниченко О. Ю., Колесниченко Ю. Ю, Минушкина Л. О., Шахгельдян К. И., Мазелис Л. С., Мазелис А. Л., Николаев А. Э., Мартынов А. В., Пулит В. В., Долженков А. Н. Смородин Г. Н., Авербух В. Л., Михайлов И. О., Григоревский И. Н. Аналитика больших данных [Электронный ресурс] // Национальный Суперкомпьютерный ФОРУМ 2017, 27 ноября – 01 декабря 2017 года. Переславль-Залесский, Россия. URL: http://2017.nscf.ru/TesisAll/ 05_Prikladnoe_PO/928_KolesnichenkoOY.pdf (дата обращения: 15.03.2018)/

4. Education and Training Monitor 2017 Slovakia [Электронный ресурс]. URL: https://ec.europa.eu/education/sites/education/files/monitor2017-sk_en.pdf (дата обращения: 15.03.2018).

УДК 004.416.6

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТЬЮ СОТРУДНИКОВ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ ОРГАНИЗАЦИЙ

М. С. Колмыков, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Применение современных технологий автоматизации и управления служебной деятельностью, как и любой другой процесс автоматизации, в той или иной сфере является одной из основных целей для повышения эффективности, оперативности, работоспособности системы, которой пользуются сотрудники научно-исследовательских организаций.

автоматизация, программное обеспечение, C#, Windows Forms SQL.

Главным элементом любой организации, являются сотрудники, так как они совершенствуют существующие и разрабатывают новые методы и способы проведения научных исследований. Результаты их работы находят практическую реализацию в моделирующих комплексах, моделях и методиках, а также в решениях сложных научных задач.

Результативность работы в целом, базируется на результатах труда сотрудников научно-исследовательских организаций, а также на правильном планировании трудовой деятельности.

Целью этой статьи является выявления текущей проблемы автоматизации рабочего процесса в системе «Портал научной работы» Военной академии связи и её дальнейшее решение.

Чтобы выявить слабое место системы, нужно актуализировать информацию о нужных модулях или отдельных функциях системы, а также получить данные по требующимся функциям для внедрения в систему.

Проведя анализ системы «Портал научной работы» была выявлена потребность пользователей в выводе напоминаний о будущих запланированных мероприятиях на текущий день. Данный процесс необходим для своевременного оповещения пользователей системы о грядущих событиях, чтобы пользователь смог вовремя принять решение и подготовится к нему.

Для реализации модулей была выбрана среда проектирования – Microsoft Visual Studio 2010; язык программирования – C# [1, 2, 3]. Microsoft

Visual Studio – линейка продуктов компании Microsoft, включающих интегрированную среду разработки программного обеспечения и ряд других инструментальных средств. Данные продукты позволяют разрабатывать как консольные приложения, так и приложения с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms. C# – объектно-ориентированный язык программирования. Данная среда и язык были выбраны из-за удобства разработки и поддержки приложения.

Основные требования данного приложения:

– Понятный и не перегруженный интерфейс.
– Вход в приложение по логину и паролю.
– Связь с сервером SQL [4].
– Скрытая работа приложения. Использование минимума ресурсов.

В ходе разработки было выполнено:

– Разработан интерфейс: форма входа и главная форма.
– Разработаны функции и методы для работы приложения.
– Разработаны необходимые серверные хранимые процедуры, функции, триггеры.

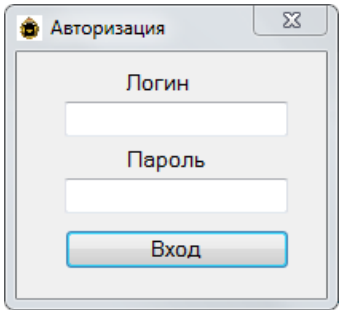


Рис. 1. Форма входа

Форма входа (рис. 1) позволяет пользователю зайти в приложение под своим логином. Затем приложение начнет отслеживание событий, которые находятся на сервере и закреплены за каждым пользователем. Также имеется возможность ввести дополнительные события, на главной форме (рис. 2), не заходя на «Портал научной работы».

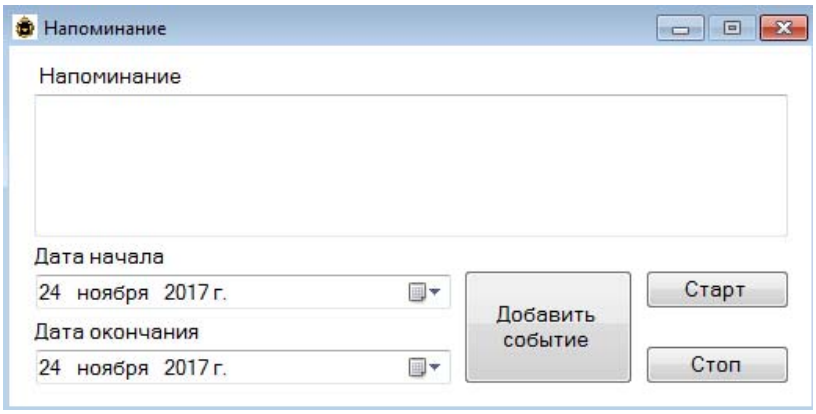


Рис. 2. Главная форма

Во время работы приложения происходит запрос (рис. 3) на получение информации о событиях на текущий день пользователя, под которым работает приложение. Затем идет проверка (рис. 4) полученной информации на совпадения по подходящим критериям. Если событие прошло про-

верку, будет воспроизведен звук оповещения и вывод сообщения об этом событии. Звук и само оповещение будет выводиться до тех пор, пока пользователь не примет решение: окончить отслеживание текущего события, или оповестить пользователя через пять минут.

```
//Метод получения данных из БД
//
ссылка 1
private void GetEvent()
{
    //
    //Очистка массивов с данными перед заполнением
    //
    eventtext.Clear();
    eventstatus.Clear();
    eventtime.Clear();
    try
    {
        //
        //Инициализация соединения с БД
        //
        SqlConnection connect = new SqlConnection(connstr);
        //
        //Вызов хранимой процедуры, передача нужного параметра(GUID)
        //
        SqlCommand cmd = new SqlCommand("EXEC [dbo].[GetStartTime] @userid=@id", connect);
        cmd.Parameters.Add("@id", SqlDbType.UniqueIdentifier);
        cmd.Parameters["@id"].Value = guid;
        connect.Open();
        SqlDataReader reader = cmd.ExecuteReader();
        //
        //Цикл считывания данных из БД
        //
        if (reader.HasRows)
        {
            while (reader.Read())
            {
                if (reader.IsDBNull(2))
                {
                    eventtext.Add(Convert.ToString(reader.GetString(0)));
                    eventtime.Add(Convert.ToDateTime(reader.GetDateTime(1)));
                }
                else if (reader.GetInt32(2) == 0)
                {
                    eventtext.Add(Convert.ToString(reader.GetString(0)));
                    eventtime.Add(Convert.ToDateTime(reader.GetDateTime(1)));
                    eventstatus.Add(Convert.ToInt32(reader.GetInt32(2)));
                }
            }
        }
```

Рис. 3. Метод получения информации о событиях из базы даннных

```
private void CheckDate(object ML)
{
    ManualResetEvent ev = (ManualResetEvent)ML;
    while (ev.WaitOne())
    {
        GetEvent();

        Thread.Sleep(3 * 1000);

        if (eventtime.Count != 0 && DateTime.Now.AddMinutes(30) >= eventtime[0] && eventtime[0] != Convert.ToDateTime("01.01.0001 0:00:00"))
        {
            player.SoundLocation = "Alarm.wav";
            player.PlayLooping();

            //
            //Вывод диалогового окна
            //
            MessageBoxManager.Yes = "Напомнить";
            MessageBoxManager.No = "Принять";
            MessageBoxManager.Register();
            res = MessageBox.Show(eventtext[0] + "\nВремя " + eventtime[0].TimeOfDay, "Напоминание!", MessageBoxButtons.YesNo);
            MessageBoxManager.Unregister();
            //
            //Результат решения диалога
            //
            if (res == DialogResult.No)
            {
                player.Stop();

                SqlConnection connect = new SqlConnection(connstr);
                SqlCommand cmd = new SqlCommand("updateEventStatus", connect);
                cmd.CommandType = CommandType.StoredProcedure;
                cmd.Parameters.AddWithValue("@stdate", eventtime[0]);
                cmd.Parameters.AddWithValue("@userId", guid);
                connect.Open();
                cmd.ExecuteNonQuery();
                connect.Close();
            }
            else if (res == DialogResult.Yes)
            {
                player.Stop();
                Thread.Sleep(3 * 60 * 1000);
            }
        }
    }
}
```

Рис. 4. Метод проверки полученной информации.

Скрытая работа была обеспечена с помощью элементов Windows Forms таких как notifyIcon. По нажатию на кнопку свернуть, главная форма будет свернута с рабочего стола на панель задач, чтобы не отвлекать пользователя лишним окном. В свернутом состоянии все функции приложения работают. Чтобы развернуть приложение нужно нажать на иконку приложения (рис. 5).

Рис. 5. Иконка на панели задач

Данное приложение является аналогом многих других приложений, которые выполняют схожие функции и которые находящихся в общем доступе в интернете, но они не соответствуют поставленным задачам и требованиям. Так же, данное приложение обладает простым, ненагруженным интерфейсом, использует минимум ресурсов и работает с уже существующей базой данных.

Список используемых источников

1. Фримен А. ASP.NET MVC 4 с приемами C# для профессионалов. М. : Вильямс, 2014. 666 с.

2. Шилдт Г. Полный справочник по C#. М. : Вильямс, 2004. 752 с.

3. Шарп, Джон. Microsoft Visual C#. Подробное руководство. СПб. : Питер, 2017. 848 с.

4. Бьюли А. Изучаем SQL. М. : Символ, 2007. 309 с.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Саенко.

УДК 004.7

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИНТЕРПОЛИРОВАНИЯ ДЛЯ НАХОЖДЕНИЯ ПРОМЕЖУТОЧНЫХ ЗНАЧЕНИЙ ИЗМЕРЕНИЙ

М. А. Колташев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Для операции наборами значений, полученных опытным путём, требуется построить функцию, на которую могут накладываться другие получаемые значения. Интерполяция разновидность аппроксимации, при которой кривая построенной функции проходит через имеющиеся точки данных. Если функция слишком сложна для производительных вычислений, следует вычислить ее значение в нескольких точках,

а по ним интерполировать более простую функцию, что позволяет снизить во многих случаях погрешность в результатах вычислений.

интерполяция, функция, метод Лагранжа, метод Эйткена, метод Ньютона.

Интерполяция – способ нахождения промежуточных значений величины по имеющемуся дискретному набору известных значений.

Задачи интерполяции: научиться вычислять значение функции в любой наперед заданной точке.

Интерполяция иногда делится на два вида:

1) $x \in [x_0, x_n]$ – собственная интерполяция.

2) $x \notin [x_0, x_n]$ – экстраполяция [1].

В данной статье демонстрируются принципы работы трех методов интерполирования: Метод Лагранжа, Метод Эйткена, и Метод Ньютона.

Метод Лагранжа

Интерполяционный многочлен Лагранжа – многочлен минимальной степени, принимающий данные значения в данном наборе точек. Для $n + 1$ пар чисел, $(x_0, y_0), (x_1, y_1) \ldots (x_n, y_n)$, где все x_i различны, существует единственный многочлен $L(x)$ степени не более n, для которого $L(x_j) = y_j$.

В простейшем случае ($n = 1$) – это линейный многочлен, график которого – прямая, проходящая через две заданные точки. [2]

Лагранж предложил способ вычисления таких многочленов:

$$L(x) = \sum_{i=0}^{n} y_i l_i(x),$$

где базисные полиномы определяются по формуле:

$$l_i(x) = \prod_{j=0, j\neq i}^{n} \frac{x - x_j}{x_i - x_j} = \frac{x - x_0}{x_i - x_0} \ldots \frac{x - x_{i-1}}{x_i - x_{i-1}} \frac{x - x_{i+1}}{x_i - x_{i+1}} \ldots \frac{x - x_n}{x_i - x_n},$$

$l_i(x)$ обладают следующими свойствами:

- являются многочленами степени n;
- $l_i(x_i) = 1$;
- $l_i(x_j) = 0$, при $j \neq i$.

Отсюда следует, что $L(x)$, как линейная комбинация $l_i(x)$, может иметь степень не больше n, и $L(x_i) = y_i$.

Код метода:

```
double p(double X, int n) // В качестве входных параметров используется
{ // double X – переменная относительно которой
double result = 0, temp = 1; // Нужно найти f(x), а также int n – количество
```

for (int i = 0; i <= n; i++) // точек интерполяции. Матрицы x[], y[] заданы

{ // глобально.
for (int j = 0; j <= n; j++)
if (i! = j)
temp* = (X – x[j]) / (x[i] – x[j]);
result+ = temp*y[i];
temp = 1;
}
return result;
}

Метод Эйткена

Итерационно-интерполяционный метод Эйткена позволяет свести вычисления коэффициентов интерполяционного полинома Лагранжа, с учетом его равенства в узлах интерполяции с исходными данными к вычислению функциональных определителей второго порядка. При этом эффективность метода повышается в тех случаях, когда нет необходимости в получении приближенного аналитического выражения функции $f(x)$, заданной таблично, а требуется лишь определить значение в некоторой точке x*, отличной от узловых точек. Этот метод заключается в последовательной линейной интерполяции. Процесс вычисления $f(x^*)$ состоит в следующем: необходимо пронумеровать узлы интерполяции, например, в порядке убывания их от x*. Затем для каждой узловой точки интерполяции строятся соотношения, которые является интерполяционными полиномами, построенными соответственно по узлам x_i, x_j, x_k. Полученный полином является интерполяционным полиномом, построенный по узлам x_i, x_j, …, x_k, x_m. Это утверждение верное, так как $Pn – 1ij \dots k(x)$ и $Pn – 1j \dots km(x)$ являются интерполяционными полиномами. При его реализации предполагается, что функция гладкая, а также критерием оценки погрешности определяется некоторое значение, определяемое условиями конкретной задачи [2].

Код метода:

Double P(double X, int n) // В качестве входных параметров используется

{ // double X – переменная относительно которой
float l[n + 1], result; // Нужно найти $f(x)$, а также int n – количество
for (int i = 0; i <= n; i++) // точек интерполяции. Матрицы x[], y[] заданы
l[i] = y[i]; // глобально.
for (int i = 1; i <= n; i++)

```
for (int j = 1; j + i <= n; j++)
{
l[j] = (l[j] * (x[ + j] – X) – l[j + 1] * (x[j] – X)) / (x[i + j] – x[j]);
result = l[j];
}
return result;
```

Метод Ньютона

Формула Ньютона:

$$P_n(x) = y_0 + \frac{\Delta y_0}{1!}q + \frac{\Delta^2 y_0}{2!}q(q-1) + \ldots + \frac{\Delta^n y_0}{n!}q(q-1)\ldots(q-n+1), \text{ где } q = \frac{x - x_0}{h}.$$

Конечной разностью функции $y = f(x)$ называется функция $\Delta f(x) = f(x+h) - f(x)$, где h – фиксированный шаг. Конечные разности иногда называются конечными разностями первого порядка [2].

Функция обозначается:

$$\Delta^k f(x) = \Delta(\Delta^{(k-1)} f(x)).$$

Принимаем:

$$\Delta^{(0)} f(x) = f(x).$$

В программе для подсчета конечных разностей мы используем следующую функцию:

```
double Delta(double X, int n, double h) // Где n – порядок, h – шаг
{
if (n > 1)
return (Delta(X + h, n – 1, h) – Delta(X, n – 1, h));
else
return (f(X + h) – f(X));
```

Код метода:

```
double Pn(double X, int h, int n) // В качестве входных параметров используется
{ // double X – переменная относительно которой
double result = y[0], qq, q; // Нужно найти f(x), а также int n – количество
q = (X – x[0]) / h; // точек интерполяции. Матрицы x[], y[] заданы
for (int i = 1; i <= n; i++) // глобально.
{
qq = 1;
```

```
for (int j = 1; j <= i; j++)
qq* = (q – j + 1);
result+ = Delta(x[0], i, h) * qq / fact(i);
}
return result+ 1;
}
{
float l[n + 1], result;
for (int i = 0; i <= n; i++)
l[i] = y[i];
```

Графическое представление

Для графического представления работы методов написана функция graphic (int *n*, int method).

```
void graphic(int n, int method)
{
float X, Y;
initwindow(1000, 640);
line(500, 0, 500, 640); // y
line(490, 20, 500, 0);
line(510, 20, 500, 0);
outtextxy(520, 10, "y");
line(0, 320, 1000, 320); // x
line(990, 310, 1000, 320);
line(990, 330, 1000, 320);
outtextxy(985, 330, "x");
X = – 100;
moveto(500 + X * 20, 160 + (160 – (Y * 3)));
setcolor(4);
for (int i = 0; i <= n; i++) //Отмечаем на графике заданные точки интерполяции
circle(500 + x[i] * 20, 160 + (160 – (y[i])), 5);
setcolor(10);
do
{
if (method==0) //Выбираем метод
{
Y = p(X, 4);
outtextxy(520, 850, "Lagranj");
}
```

```
if (method==1)
{
Y = P(X, 4);
outtextxy(520, 850, "Eytkin");
}
if (method==2)
{
Y = Pn(X, 1, 4);
outtextxy(520, 850, "Newton");
}
if (method==3)
{
Y = S(X, n); // С помощью определенного метода находим у для
outtextxy(520, 850, "Splayn"); // Заданного x
}
lineto(500 + X * 20, 160 + (160 – (Y))); //И проводим к точке (x,y) линию от предыдущей точки
X = X + 0.02;
}
while(X <= 100);
getch();
closegraph();
}
```

Таким образом, например, для метода Лагранжа и значений точек интерполяции:

$x[0] = 1$; $x[1] = 2$; $x[2] = 3$; $x[3] = 4$; $x[4] = 5$;

$y[0] = 1$; $y[1] = 4$; $y[2] = 9$; $y[3] = 16$; $y[4] = 25$.

Получаем график функции (рис.).

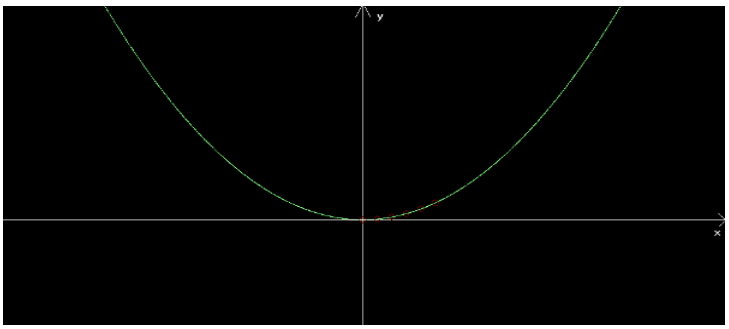


Рисунок. График функции точек по методу Лагранжа

Список используемых источников

1. Макаренко А. А. Специальные вопросы цифровой обработки одномерных и двумерных сигналов : учебное пособие. СПб. : НИИ ИТМО, 2016. 218 с.
2. Шафер Р., Ребайнер Л. Методы цифровой обработки сигналов в задачах интерполяции : учебное пособие. М. : ТИИЭР, 1973. 285 с.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.056.5

РАЗВИТИЕ АСИММЕТРИЧНЫХ АЛГОРИТМОВ В ПРОТОКОЛАХ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ПЕРСПЕКТИВЫ ИХ ДАЛЬНЕЙШЕГО ПРИМЕНЕНИЯ

А. В. Комарова, А. Г. Коробейников, А. А. Менщиков

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В современном информационно-развитом обществе с каждым годом все большее внимание, как со стороны государства, так и со стороны и частных компаний, начинает уделяться шифрованию передаваемой информации, защите персональных данных, аутентификации пользователей в сети Интернет и другим аспектам информационной безопасности. В создании информационно-защищенного современного общества все более широкое применение находят алгоритмы асимметричной криптографии или криптографии с открытым ключом.

асимметричная криптография, электронная цифровая подпись, задача факторизации задача дискретного логарифмирования, постквантовая криптография, протокол безопасности, теория решеток.

Асимметричная криптография на сегодняшний день используется для решения большого количества задач, таких, как проведение финансовых транзакций, электронного голосования, создание защищенной связи по коммутационным каналам, использование на торговых площадках и так далее.

Криптография с открытым ключом применяется не только на межгосударственном уровне, но и в повседневной жизни каждого человека. Обеспечить аутентичность, доступность и конфиденциальность переда-

ваемой информации позволяет электронная цифровая подпись (ЭЦП) [1]. О различных схемах электронной цифровой подписи и их применении пойдет речь в данной работе.

Как известно, существует несколько трудоемких задач, на которых основываются все алгоритмы ЭЦП. Основные из них – это задача факторизации больших чисел (разложение чисел на простые множители) и задача дискретного логарифмирования [2]. На первой задаче базируется первый алгоритм ЭЦП – RSA, изобретенный Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом в 1977 г. На второй задаче основывается схема, предложенная в 1984 г. американским ученым родом из Египта Тахером Эль-Гамалем.

Для усиления стойкости в современных алгоритмах последняя задача решается не в простом конечном поле, а в группе точек эллиптической кривой [3]. Так, действующие стандарты Соединенных Штатов Америки ECDSA и Российской Федерации ГОСТ 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» как раз основываются на этой трудной задаче. В отличие от своих предшественников DSA и ГОСТ 34.10.2001 соответственно, которые базировались на вычислении дискретного логарифма в простом конечном поле. Использование аппарата эллиптических кривых позволяет в значительной степени повысить стойкость алгоритма ЭЦП при одинаковых вводных данных [4]. В новом российском стандарте ЭЦП можно использовать меньшую длину ключа, без понижения безопасности. Но, не смотря на все преимущества в стойкости, новый стандарт требует в несколько раз больше времени и для формирования хэш-функции и для процесса формирования самой подписи.

В 1994 г. американский ученый Питер Шор разработал эффективный полиномиальный алгоритм факторизации для квантового компьютера. Для обычных компьютеров полиномиальный алгоритм разложения больших чисел на множители считается экспоненциально трудной задачей. В связи с этим, в случае появления квантового компьютера, все существующие на рабочие схемы могут подвергнуться взлому, по этой причине созданием алгоритмов, стойких к квантовым вычислениям сейчас занимается такая отрасль криптографии, как постквантовая криптография [5].

К алгоритмам постквантовой криптографии можно отнести схему с использованием блочных шифров, которую предложил Крис Митчел в 2003 г.; схему с использованием псевдослучайных генераторов и теории графов, разработанную Ави Вигдерсоном и Боазом Бараком в 2008 г.; схему на основе квазигрупп (авторы Данило Глигороски, Смайл Марковски и Свейн Кнапског, 2008 г.).

Широкое применение в постквантовой криптографии нашла так называемая теория решеток (с англ. *lattice based cryptography*) [6]. Криптостой-

кость алгоритмов с использованием решеток основана на трудной математической задаче.

К вычислительно трудным задачам криптографии на решетках относятся:

1. Задача поиска наикратчайшего вектора решетки (*Shortest Vector Problem*).
2. Задача поиска ближайшего вектора решетки (*Closest Vector Problem*).
3. Задача поиска кратчайшего расстояния между векторами в базисе решетки (GapSVP).
4. Задача определения минимума длины наикратчайшего вектора решетки (*Shortest Independent Vector Problem*).
5. Задача поиска уникального кратчайшего вектора (unique (*Shortest Vector Problem*) [7].

Задача поиска наикратчайшего вектора решетки (SVP) является NP-полной задачей и считается наиболее перспективной для использования в протоколах ЭЦП [8]. На основе этой трудной задачи в 2003 г., после нескольких неудачных попыток, была разработана схема ЭЦП NTRUSign, которая является стойкой к квантовым вычислениям.

Повышение уровня безопасности существующих асимметричных алгоритмов ЭЦП может быть достигнуто их модификацией с использованием одновременно нескольких независимых вычислительно трудных задач. Такой подход предлагался и был успешно реализован в работах [9, 10, 11]. Для создания схемы, стойкой к квантовым вычислениям, интересным дальнейшим направлением исследований являются схемы ЭЦП, взлом которых требует одновременного решения и трудной задачи асимметричной криптографии (например, задачи дискретного логарифмирования на эллиптических кривых) и трудной задачи постквантовой криптографии (например, задачи поиска наикратчайшего вектора решетки).

Вероятность взлома первой задачи при длине ключа в 256 бит можно оценить по алгоритму p-Полларда как 10^{-154}. Вероятность взлома второй постквантовой задачи при той же длине ключа оценивается как 10^{-216}. В случае комбинирования этих задач в одной схеме ЭЦП, вероятность взлома будет складываться из произведения вероятностей взлома каждой вычислительно трудной задачи в отдельности, то есть будет равна 10^{-370}.

Таким образом, в схемах ЭЦП основанных на двух трудных задачах, может быть существенно увеличен уровень безопасности, а использование в алгоритме подписи постквантовой задачи многократно повысит стойкость к квантовым вычислениям.

Список используемых источников

1. Komarova A. V., Menshchikov A. A., Negols A. V., Korobeynikov A. G., Gatchin Y. A., Tishukova N. A. Comparison of Authentication Methods on Web Resources // Advances in Intelligent Systems and Computing. 2018. Vol. 679, pp. 104–113.

2. Пискова А. В. Разработка алгоритма электронной цифровой подписи, основанного на задачах факторизации и дискретного логарифмирования на эллиптических кривых // Сборник трудов IV Всероссийского конгресса молодых ученых. СПб. : Университет ИТМО, 2015. С. 322–326.

3. Менщиков А. А., Комарова А. В., Коробейников А. Г. Алгоритмы электронной цифровой подписи в информационных системах // Альманах научных работ молодых ученых Университета ИТМО. 2017. Т. 3. С. 135–137.

4. Комарова А. В., Менщиков А. А., Коробейников А. Г. Анализ и сравнение алгоритмов электронной цифровой подписи ГОСТ Р 34.10-1994, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 // Вопросы кибербезопасности. 2017. № 1 (19). С. 51–56.

5. Пискова А. В., Коробейников А. Г. Особенности применения теории решеток в схемах электронной цифровой подписи // Кибернетика и программирование. 2016. № 2. С. 8–12.

6. Комарова А. В., Попов И. Ю., Менщиков А. А., Негольс А. В. Схемы электронной цифровой подписи на решетках // Сборник трудов молодых ученых, аспирантов и студентов научно-педагогической школы кафедры ПБКС «Информационная безопасность, проектирование и технология элементов и узлов компьютерных систем». 2016. С. 123–127.

7. Комарова А. В., Коробейников А. Г., Менщиков А. А., Кляус Т. К., Негольс А. В., Сергеева А. А. Теоретические возможности комбинирования различных математических примитивов в схеме электронной цифровой подписи // Кибернетика и программирование. 2017. № 3. С. 80–92.

8. I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors // In Proc. 39th ACM Symp. on Theory of Computing (STOC), pp. 469–477, 2007.

9. Пискова А. В. Практическое применение теории решеток в схемах электронной цифровой подписи // Альманах научных работ молодых ученых Университета ИТМО. 2016. Т. 4. С. 152–154.

10. Дернова Е. С., Нгуен Ле Минь, Костина А. А., Щербаков В. А. Схемы цифровой подписи, взлом которых требует решения двух трудных задач в одной конечной группе // Региональная информатика–2008 (РИ–2008). XI Санкт-Петербургская международная конф. Санкт-Петербург, 22–24 октября 2008 г. Материалы конференции. СПб, 2008. С. 97–98.

11. Дернова Е. С., Молдовян Н. А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. № 1. С. 22–26.

УДК 004.7

СОВРЕМЕННЫЕ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ И СЕТЕВЫЕ ПРОТОКОЛЫ

Д. М. Кондратьев, М. И. Носов

Военная академия связи им. Маршала Советского союза С. М. Буденного

В статье рассматриваются вопросы систем хранения данных по отношению к предприятиям и организациям военных структур, эксплуатирующим сети связи, входящие в Единое информационное пространство Российской Федерации. Проведен анализ современных устройств хранения данных и сетевых протоколов. Показаны преимущества использования флеш-накопителей в системах хранения данных.

единое информационное пространство, система хранения данных, флеш-накопители, сетевые протоколы.

В России целенаправленно проводится политика по росту информатизации общественной жизни. Решением Президента Российской Федерации (23 ноября 1995 года № Пр-1694) была одобрена Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов [1].

Единое информационное пространство невозможно представить без систем хранения данных, которые непрерывно совершенствуется. Система хранения данных предназначена для организации надежного хранения, а также отказоустойчивого, высокопроизводительного доступа к данным. Доступ к данным невозможен как в случае выхода из строя каналов (доступа) или вычислительных средств, так и в случае отсутствия необходимой производительности для выполнения прикладных задач. Поэтому более подробному рассмотрению будут подвергнуты три составляющих архитектуры информационно-аналитической системы: особенности программно-аппаратных платформ; сетевая инфраструктура (применительно к СХД); управление системой (рис. 1) [2].

Современные телекоммуникационные компании ориентированы на перенос целых массивов данных на флеш-накопители, что обеспечивает высокую производительность и стабильность приложений. В настоящее время, из-за снижения цены, использование флеш-накопителей становится более выгодным, тем самым обеспечивая их широкое применение и рост рынка SSD.

Рис. 4. Типовая архитектура информационно-аналитических систем

Флеш-накопители и жесткие диски изначально были схожи по внешнему виду и по принципу их эксплуатации. Твердотельные диски подключались по интерфейсам SAS и SATA, как и жесткие диски, обеспечивая значительную пропускную способность. Существующая инфраструктура ПК позволяла удобное использование интерфейсов подключения. Но интерфейсы SAS и SATA не смогли раскрыть все преимущества технологии SSD. Флеш-накопители набирают популярность, тем самым, обретая на рынке прочную основу, и имеют все шансы заменить HDD в серверах и СХД. Анализ характеристик устройств хранения данных: HDD Seagate Savvio 10K [3], SSD Intel S3710 [4], SSD Intel P3700 [5] подтверждает эффективность использования SSD (табл. 1).

ТАБЛИЦА 1. Сравнение параметров HDD и SSD

Устройства / Характеристика	SAS HDD (Seagate Savvio 10K)	SATA SSD (Intel S3710)	PCIe NVMe SSD (Intel P3700)
Производительность	200 IOPS	85K IOPS	460K IOPS
Скорость потоковых операций, Мбайт/с	200	550	2800
Задержка доступа чтения (*R*) / записи (*W*)	5/5 мс	55/66 мкс	20/20 мкс

Технологии SSD стремительно развиваются, появляются новые форм-факторы накопителей, совершенствуются интерфейсы. Следуя собственным курсом развития, SSD реализует свой потенциал. В последнее время в качестве интерфейса подключения флеш-накопителей применяется PCI Express. По сравнению с интерфейсами SATA и SAS, PCIe обеспечивает более низкую задержку и лучшую производительность (рис. 2). Для рас-

крытия потенциала SSD, подключенных по шине PCIe, используется логический интерфейс NVMe (*Non-Volatile Memory Express*). Основной целью NVMe является снижение задержки при доступе к носителю и увеличение производительности системы в целом.

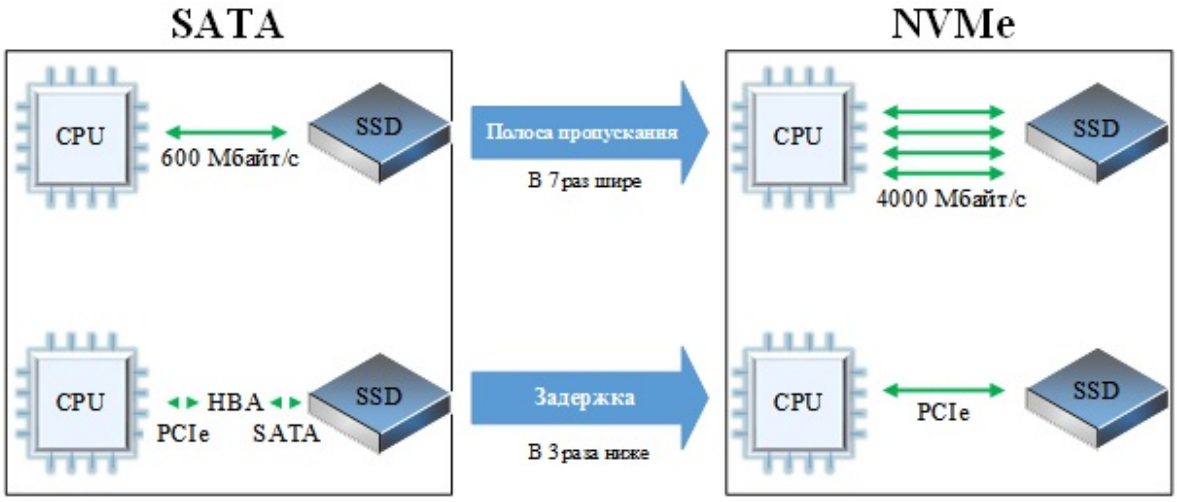


Рис. 5. Сравнение флеш-накопителей SATA и PCI/NVMe

При помощи NVMe можно сократить время доступа к флеш-памяти, не используя интерфейс SCSI. По данным Samsung, если у SATA SSD задержка составляет 40–110 тыс. наносекунд, то у PCIe NVMe SSD она достигает 20–100 тыс. наносекунд, то есть может быть вдвое ниже. Для сравнения, у HDD этот показатель равен 3–10 млн наносекунд [6].

В июне 2016 г. организация NVM Express опубликовала новую спецификацию для стандарта NMVe over Fabrics (NVMeF). Спецификация NVM Express over Fabrics 1.0 позволит расширить область применения NVM Express. По мнению разработчиков, теперь достоинства этой технологии станут доступны не только в рамках стоек, но и на уровне вычислительных центров, включающих тысячи твердотельных накопителей [7]. Основная его задача заключается в обеспечении эффективного удаленного доступа хоста к устройствам NVMe over Fabrics (рис. 3).

Стандарт NVMe over Fabrics реализует всю функциональность NVMe поверх Ethernet и поддерживает RDMA. NVMe over Fabric рассматривается в качестве перспективного протокола SAN, что существенно повышает её производительность. Таким образом, этот протокол способен конкурировать с iSCSI, FCoE, FC и InfiniBand, а в перспективе и с iSER, если NVMe over FC и NVMe over Ethernet получат дальнейшее развитие.

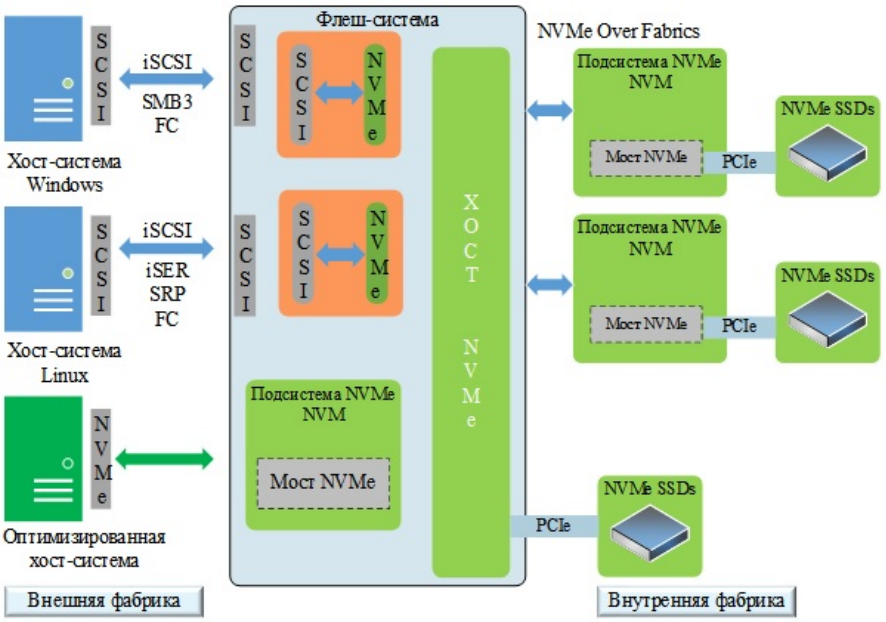


Рис. 3. NVMe over Fabrics при работе с внешними и внутренними фабриками

Компания Mellanox Technologies объявила о предстоящем выходе семейства чипов BlueField на кристалле (SoC) с интегрированным контроллером ConnecX-5 и поддержкой NVMe over Fabric (рис. 4). В чипе реализована поддержка IB EDR на скорости (100Gb/s), а также 10/25/40/50/100Gb Ethernet. Развитие BlueField направлено на использование в серверах для подключения NVMe over Fabric и нацелено на применение в NVMe AllFlash массивах. Использование подобных специализированных устройств позволит повысить эффективность серверов, что очень важно для HPC [8].

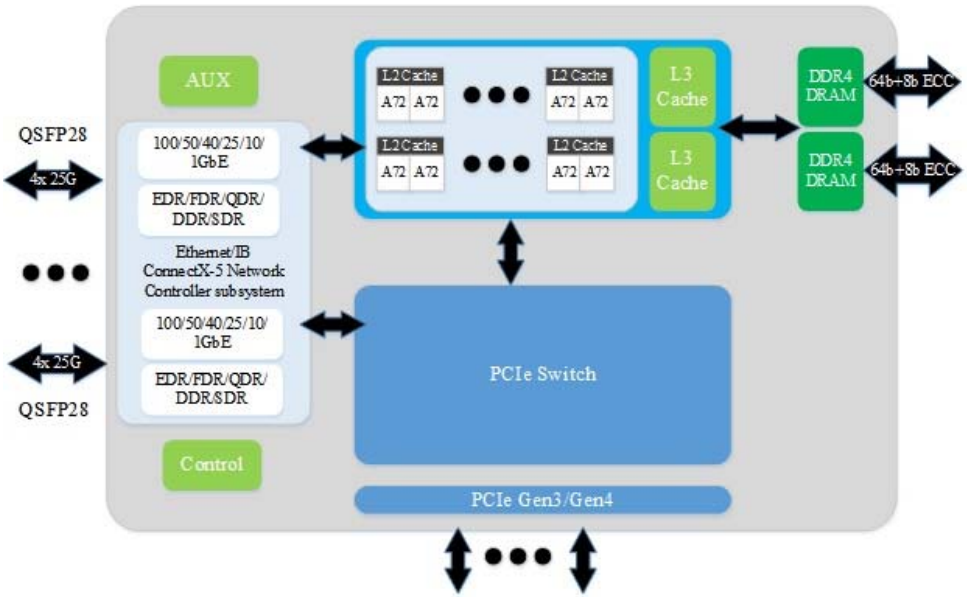


Рис. 4. Архитектура BlueField

Число NVMe систем хранения в ближайшем будущем будет увеличиваться. Подключение серверов через PCI-express коммутатор обеспечивает максимальную скорость, а в качестве транспорта может использоваться FC или RDMA, которую можно реализовать на базе Infiniband, iWARP или RoCE.

Стандарт шестого поколения FC Gen 6 увеличивает максимальную скорость с 16GFC до 32GFC и пропускную способность с 3200 до 6400 Мбайт/с (табл. 2). А стандарт Parallel FC 128GFC позволяет объединить 4 линии FC в один канал с пропускной способностью 25 600 Мбайт/с.

Компания Brocade Communications Systems выпустила коммутатор нового поколения Brocade G620. Он обеспечивает высокую производительность при работе с подключениями на скорости 32 и 128 Гбит/с и показывая производительность 100KK IOPS. Коммутатор содержит от 24 до 64 портов, предоставляя гибкость и масштабируемость по мере роста требований. В максимальной конфигурации (8 слотов) поддерживает до 384 портов 32 GFC + 32 порта 128 GFC с суммарной пропускной способностью 16 Тбит [9].

Таким образом, использование флеш-накопителей и стандарта NVMe over Fibre Channel приводит к низкой латентности и увеличению производительности ввода/вывода в решениях для систем хранения данных. Рассмотренные решения для военных структур в сфере систем хранения данных предоставляют более эффективное использование массивов хранения данных, а также таких сервисов как: резервное копирование, шифрование, репликация, дедупликация, сжатие, SnapShot и т. д.

ТАБЛИЦА 2. Эволюция Fibre Channel

Название продукта	Пропускная способность, Мбайт/с
FC 1G	200
FC 2G	400
FC 4G	800
FC 8G	1600
FC 16G	3200
FC 32G	6400
FC 128G	25600(4x32)
FC 256G	12800
FC 512G	102400
FC 1T	204800

Список используемых источников

1. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов // утв. Президентом РФ (23 ноября 1995 года № Пр-1694).

2. Бабошин В. А., Сиротенко Ф. Ф. Методы построения систем хранения данных в телекоммуникационной сети специального назначения // Вопросы радиоэлектроники. Сер. СОИУ. 2012. Вып. 2. С. 29–44.

3. Seagate Technology [Электронный ресурс] // Enterprise Performance HDD. URL: http://www.seagate.com/ru/ru/support/internal-hard-drives/enterprise-hard-drives/savvio-10k/ (дата обращения 02.02.2018).

4. Intel Corporation [Электронный ресурс] // Intel SSD Data Center S3710. URL: http://www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-dc-s3710-series.html (дата обращения 02.02.2018).

5. Intel Corporation [Электронный ресурс] // Intel SSD DC P3700 Series. URL: http://www.intel.com/content/www/us/en/solid-state-drives/ssd-dc-p3700-spec.html (дата обращения 02.02.2018).

6. Орлов С. Наступление SSD [Электронный ресурс] //Журнал сетевых решений/LAN. 2016. № 09. Режим доступа: http://www.osp.ru/lan/2016/09/13050286 (дата обращения 02.02.2018).

7. NVM Express, Inc. [Электронный ресурс] // NVM Express over Fabrics Specification Released. URL: http://www.nvmexpress.org/nvm-express-over-fabrics-specification-released (дата обращения 02.02.2018).

8. Mellanox Technologies [Электронный ресурс] // Mellanox Introduces New BlueField Family of System-on-Chip Programmable Processors for Storage and Networking Applications. URL: http://www.mellanox.com/page/press_release_item?id=1733 (дата обращения 02.02.2018).

9. Brocade Communications Systems [Электронный ресурс] // Brocade G620 Technical Specifications. URL: http://www.brocade.com/en/backend-content/pdf-page.html?/content/ dam/common/documents/content-types/technical-specification/g620-technicalspecification.pdf (дата обращения 02.02.2018).

УДК 621.396.41

КОМПЬЮТЕРНАЯ МОДЕЛЬ КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ

Д. И. Коньков

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Рассматриваются теоретические и практические вопросы разработки компьютерной модели канала передачи информации.

передача непрерывной и дискретной информации по каналу связи.

В сетях связи в интересах передачи данных широко используются непрерывные каналы – каналы ТЧ и широкополосные каналы (ШК) систем передачи с частотным разделением каналов (ЧРК). В этих каналах нормируются следующие характеристики:

– эффективно-передаваемая полоса частот (для канала ТЧ она определена в границах 0,3–3,4 кГц) [1];

– амплитудно-частотная характеристика (АЧХ) или неравномерность остаточного затухания;

– фазо-частотная характеристика (ФЧХ), которая для удобства измерения оценивается не значением фазы, а ее производной – групповым временем прохождения (ГВП);

– нормируемые значения средней мощности модулированного сигнала и шума в канале связи;

– амплитудная характеристика и коэффициенты нелинейности;

– изменение частоты сигнала, передаваемого по каналу;

– фазовое дрожание;

– импульсные помехи и кратковременные перерывы сигнала.

Указанные характеристики оценивают влияние как устройств формирования канала связи (фильтры, корректоры, усилители, автоматические регуляторы уровней, генераторы), так и внешних помех (собственные шумы, переходные помехи импульсные помехи, кратковременные перерывы сигнала и др.).

Канал связи можно представить моделью, изображенной на рис. 1, и раздельно учитывать воздействие каждого влияющего фактора [1].

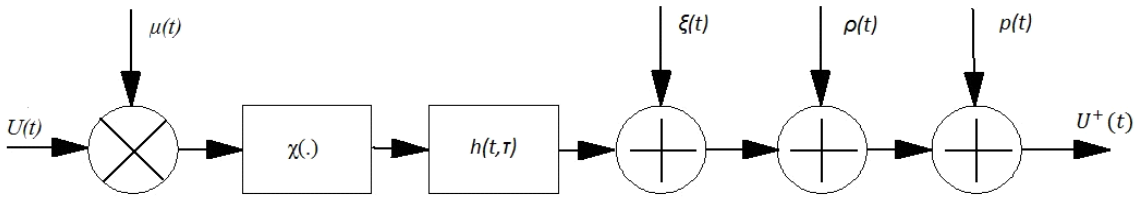


Рис. 1. Модель канала связи

В модели отображены:

$h(\tau)$ – импульсная характеристика канала, связанная с комплексной передаточной функцией канала $K(j\omega)$ преобразованием Фурье:

$$K(j\omega) = \int_0^{\infty} h(\tau) e^{-j\alpha I} dt = |K(j\omega)| e^{-j\varphi(\omega)},$$

где $|K(j\omega)| = K(\omega)$ – амплитудно-частотная характеристика (АЧХ), $\varphi(\omega) = \arg K(j\omega)$ – фазочастотная характеристика (ФЧХ) непрерывного

канала связи. Заметим, что канал связи считается стационарным, т. е. не изменяющим свои параметры во времени, что при передаче данных вполне реально;

$\chi(.)$ – звено, учитывающее нелинейные искажения сигнала;

$\xi(t)$ – аддитивные шумы гауссова типа, источников которых много и которые практически невозможно подавить;

$\mu(t)$ – мультипликативные помехи, вызывающие изменение передаточной функции канала. В их число входят кратковременные перерывы, возникающие в проводных каналах связи, нелинейные искажения и замирания на радиолиниях;

$\rho(t)$ – аддитивные импульсные помехи;

$p(t)$ – аддитивные помехи [1].

Учитывая множество факторов, влияющих на передаваемый сигнал, актуальна идея создания компьютерной модели имитирующей прохождение сигнала по каналу связи. Помимо имитации непрерывного канала данная модель позволит воспроизводить дискретные каналы связи. В связи с этим в компьютерной модели необходимо реализовать процессы, происходящие в реальных каналах передачи.

Входной сигнал поступает на вход имитатора работы согласующего удлинителя, устанавливаемого на входе канала ТЧ. Имитатор канала ТЧ выполняет имитацию следующих искажений передаваемого сигнала:

– искажения частотных характеристик затухания и группового времени прохождения;
– нелинейное искажение;
– задержка распространения;
– остаточное затухание;
– изменение частоты;
– дрожание фазы;
– скачки фазы.

Кроме того, имитатор канала ТЧ обеспечивает генерацию следующих аддитивных помех:

– равномерный шум,
– гармоническая помеха,
– импульсные помехи [2].

Сигнал с выхода канала ТЧ поступает на вход второго имитатора работы согласующего удлинителя, устанавливаемого на выходе канала ТЧ.

Компьютерная модель дискретного канала передачи информации повторяет функции аппаратной модели AnCom Canal-5. Имитатор телефонных каналов AnCom Canal-5 предназначен для проведения испытаний телекоммуникационного оборудования путем воспроизведения электрических характеристик выделенного канала тональной частоты (ТЧ) в четы-

рех- и двухпроводном окончании, а также канала коммутируемой телефонной сети. Структурная схема блоков приведена на рисунке (рис. 2) [2].

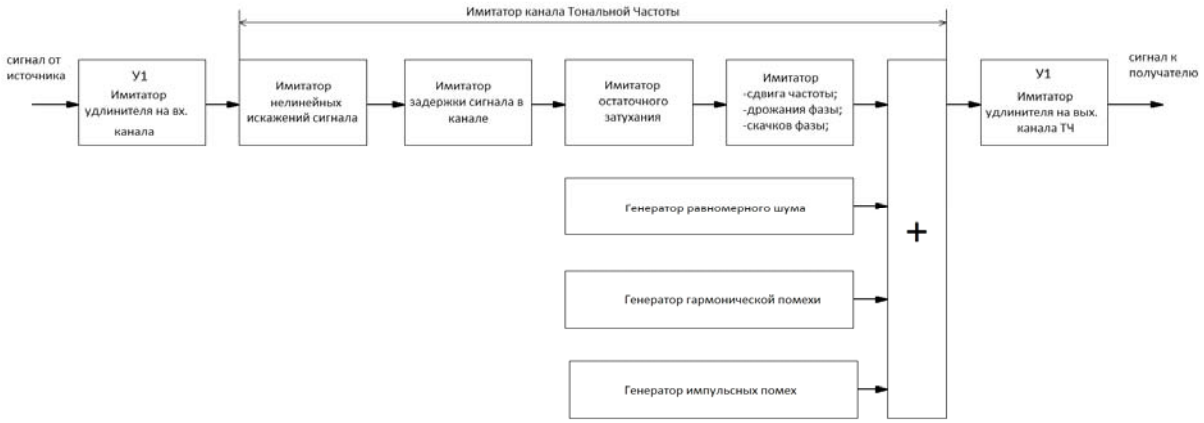


Рис. 2. Структурная схема имитаторов канала ТЧ и удлинителей

Преимущества компьютерной модели заключается в её существенно низкой стоимости по сравнению с аппаратной моделью и невозможности дальнейшей модернизации последней под современные требования. Также компьютерная модель может выступать в качестве лабораторной работы для студентов радиотехнических специальностей.

Модель реализована на базе программной оболочки MatLab. Блок-схема модели имеет вид, показанный на рис. 3 (см. ниже). Все операции преобразования сигналов реализованы программным путём. Частотные свойства канала (в том числе различные фазовые искажения и временная задержка) изменяются с помощью пары прямого и обратного быстрых преобразований Фурье (БПФ и ОБПФ). При таком подходе изменение частотных характеристик канала легко реализуется путём умножения спектра входного сигнала на соответствующую комплексную функцию с заданной формой амплитудной и фазовой характеристик. Нелинейные искажения имитируются путём передачи отсчётов сигнала через нелинейное звено, форму амплитудной характеристики которого можно изменять программно.

Влияние помех имитируется путём прибавления к выходному сигналу канала ТЧ соответствующих сигналов от генератора помехи.

Для проведения исследования на вход системы подается произвольная последовательность 0 и 1, формируемая с помощью датчика равномерно распределённых чисел. Далее эта последовательность модулируется с помощью использования различных видов модуляции. В данной работе используются следующие виды:

– частотная модуляция;
– фазовая модуляция;

– квадратурная амплитудная модуляция.

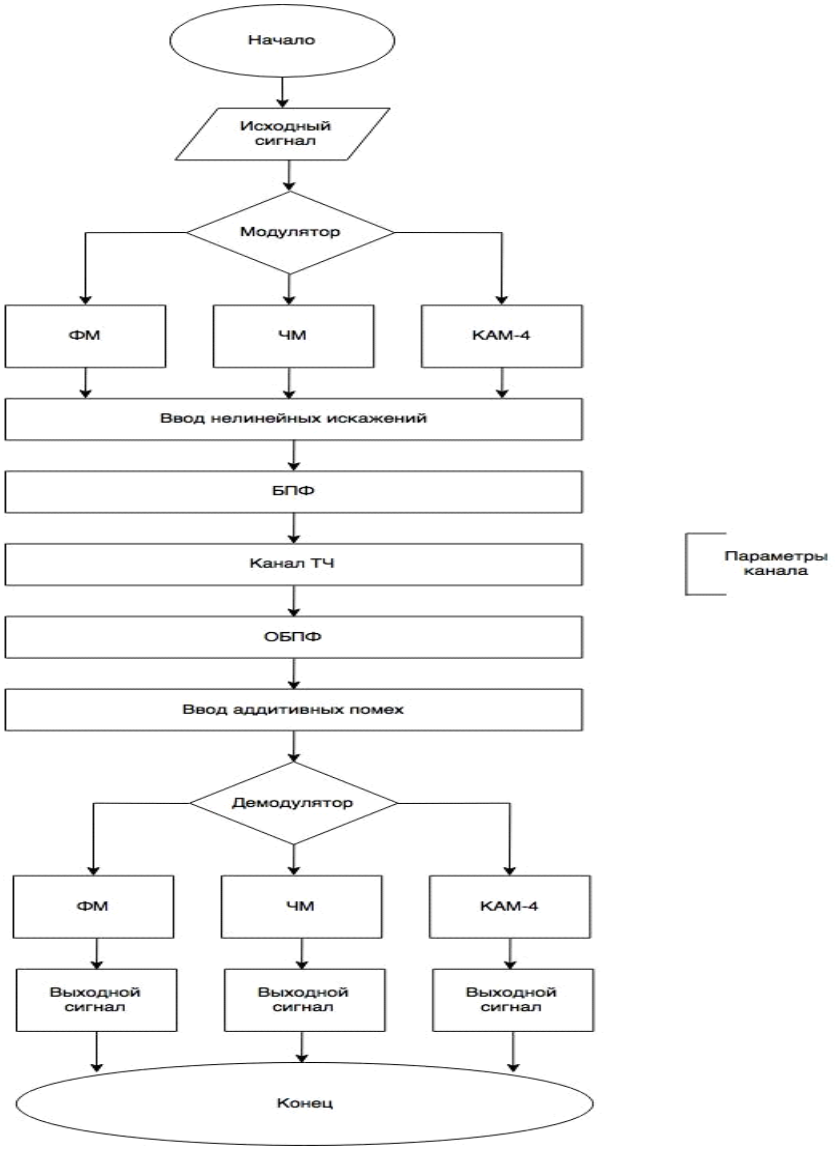


Рис. 3. Блок-схема модели

Модулированный сигнал поступает на вход канала тональной частоты, параметры которого задаются отдельно в зависимости от требуемой задачи. Параметры канала ТЧ задаются путём изменения характеристик. Кроме этих параметров, можно исследовать действие на канал шумов и помех. После этого, сигнал поступает на демодулятор. На выходе демодулятора наблюдается сигнал, отличный от исходного сигнала. Выходной блок оценки качества передачи производит сравнение полученного сигнала с переданным сигналом и подсчитывает вероятность ошибки. С этой целью на него передаётся последовательность входных сигналов.

Интерфейс программной модели оформлен с помощью графического интерфейса пользователя GUI в виде последовательности окон, позволяю-

щих задавать основные параметры модели и запускать соответствующий режим моделирования.

В дальнейшем планируется использовать в компьютерной модели более современные методы модуляции, а также помехоустойчивое кодирование, уделить большее внимание факторам, влияющим на сигнал в канале связи. С этой целью программа модели допускает дальнейшее расширение путём добавления соответствующих модулей в текст программы и в графическую оболочку.

Список используемых источников

1. Теория передачи сигналов : учебное пособие // Библиотека сайта АНО «Радиочастотный Центр МО». Режим доступа: http://window.edu.ru/resource/848/57848

2. Имитатор телефонных каналов AnCom Canal-5. Техническое описание и инструкция по эксплуатации ЭД 4221-008-11438828-99ИЭ. ООО «Аналитик-ТС», 2000. 63 с. Режим доступа: https://docplayer.ru/51914844-Ooo-analitik-ts-imitator-telefonnyh-kanalov-tehnicheskoe-opisanie-i-instrukciya-po-ekspluatacii-ed-ie.html

Статья представлена преподавателем ВАС, доктором технических наук, профессором И. Б. Саенко.

УДК 004.85

ИССЛЕДОВАНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ТОНАЛЬНОСТИ ТЕКСТА В СОЦИАЛЬНЫХ МЕДИА-РЕСУРСАХ

М. И. Короткова, В. Л. Литвинов, К. В. Соколова

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

В статье рассмотрены алгоритмы машинного обучения, которые позволяют проводить анализ тональности текста в социальных медиа-ресурсах. Рассматриваются различные виды классификаций тональности текста. Показаны особенности некоторых подходов к классификации тональности текста. Предложены методы и алгоритмы машинного обучения для анализа контента социальных медиа-ресурсов, такие как машинное обучение с учителем и без учителя.

алгоритмы машинного обучения, тональность текста, социальные медиа-ресурсы, контент, машинное обучение с учителем.

В настоящее время активное развитие социальных медиа-ресурсов ведет к увеличению интереса к задаче анализа контента этих ресурсов. Основной проблемой при анализе мнений, новостей или комментариев в социальных медиа-ресурсах является классификация текста по тональности. Тональность – это эмоциональная оценка, которая выражается в тексте к какому-либо объекту и определяется тональностью его лексических единиц и правил их сочетания. Традиционно, текст классифицируется по тональности на позитивные и негативные эмоциональные оценки.

Целью данного исследования является анализ методов и алгоритмов машинного обучения в задачах анализа тональности текста в социальных медиа-ресурсах.

Социальные медиа-ресурсы представляют собой новый вид коммуникации, позволяющий участникам электронного общения делиться различным контентом в режиме реального времени. Под контентом следует понимать информационное содержание медиа-ресурсов, включающее текстовую, графическую, звуковую и другие виды информации. На основании этого контента можно выделить такие медиа-ресурсы, как блоги, форумы, социальные сети или wiki-проекты, относящиеся к медиа-ресурсам, которые выстраивают взаимодействие около этих видов контента [1].

Особого внимания в социальных медиа-ресурсах заслуживает текст, поскольку именно с помощью него пользователи обмениваются большей частью информации. Существует множество подходов к автоматической классификации текста по тональности:

- на основе словаря;
- правила, использующие шаблоны;
- машинное обучение без учителя;
- машинное обучение с учителем.

Подход, основанный на словарях, чаще всего использует лексические словари тональности для анализа текста. В простом виде этот словарь представляет собой список слов с числовым значением тональности для каждого слова. Пример такого словаря представлен ниже в таблице.

ТАБЛИЦА. Лексический словарь тональности

Слово	Валентность (1–9)
счастливый	8,21
хороший	7,47
скучный	2,95
сердитый	2,85
грустный	1,61

Анализ тональности текста в данном подходе предполагает использование следующего алгоритма: в первую очередь, каждому слову в тексте присваивается его значение тональности по словарю, и только после этого вычисляется общая тональность всего текста. Вычисление общей тональности текста можно осуществить самыми различными способами, начиная со среднего арифметического всех значений, и заканчивая обучением классификатора с помощью нейронной сети.

Подход, основанный на использовании правил с шаблонами заключается в генерации этих самих правил, посредством которых и определяется тональность всего текста. В первую очередь, текст разбивается на слова или последовательности слов (*N-grams*), после этого, данные, полученные после разбиения, используются для выделения шаблонов, которые чаще всего встречаются, и уже им присваивается положительная или отрицательная оценка. Выделенные шаблоны, в свою очередь, применяются уже при создании правил, например, следующего вида: «если условие, то заключение».

Наибольшая точность в определении тональности теста достигается подходами, основанными на машинном обучении (*Machine Learning*), которое находится на стыке прикладной статистики, численных методов оптимизации, дискретного анализа, и уже давно оформившееся в самостоятельную математическую дисциплину.

Метод обучения (*learning algorithm*) – это отображение:

$$\mu: (X \times Y)^{\ell} \to A,$$

которое произвольной конечной выборке $X^{\ell} = (x_i, y_i)^{\ell}$ ставит в соответствие некоторый алгоритм $a \in A$. Говорят также, что метод μ строит алгоритм a по выборке X^{ℓ}. Метод обучения должен допускать эффективную программную реализацию.

На этапе обучения метод μ по выборке X^{ℓ} строит алгоритм $a = \mu(X^{\ell})$. На этапе применения алгоритм a для новых объектов x выдаёт ответы $y = a(x)$.

Алгоритм принято считать алгоритмом машинного обучения, если он способен улучшать своё поведение по мере приобретения опыта. Это означает, что алгоритм способен обучать параметры модели либо на основе подготовленных тестовых примеров, либо на основе собственных ошибок, со временем лучше и лучше решая поставленную задачу [2].

Машинное обучение без учителя (*unsupervised learning*) – подход, в основе которого лежит идея о том, что наибольший вес в тексте имеют термины, чаще всего встречающиеся в тексте и при этом присутствующие в небольшом количестве текстов всей коллекции. Вывод о тональности всего текста можно сделать, определив лишь тональность выделенных терминов.

Подход, основанный на машинном обучении с учителем (*supervised learning*), предполагает наличие обучающего набора текстов в рамках его эмотивного пространства, и уже на базе этого набора строится статический или вероятностный классификатор.

Наивный байесовский классификатор является вероятностным классификатором, который основывается на применении теоремы Байеса со строгими предположениями о независимости. Отличительной особенностью «наивного» байесовского классификатора является малое количество данных, которые необходимы для оценки параметров, требующихся для классификации [3].

Алгоритм SVM или метод опорных векторов представляет собой набор схожих алгоритмов, использующихся для задач классификации. Достоинством алгоритма SVM является непрерывное уменьшение эмпирической ошибки классификации и увеличение зазора.

При анализе тональности текста особого внимания заслуживает оценка точности и качества системы, насколько хорошо она согласуется с мнением пользователей относительно эмоциональной оценки анализируемого текста. Точность и полнота – характеристики, которые используется при оценке качества анализа тональности. Полнота вычисляется по следующей формулы:

$$R = \frac{\text{correctly extracted opinions}}{\text{total number of opinions}},$$

где correctly extracted opinions – это верно определенные мнения, а total number of opinions – общее количество мнений. Точность вычисляется по следующей формуле:

$$R = \frac{\text{correctly extracted opinions}}{\text{total number of opinions found by system}},$$

где correctly extracted opinions – это верно определенные мнения, а total number of opinions found by system – общее количество найденных системой мнений. Точность выражает количество анализируемых текстов, в оценке которых мнения системы анализа и эксперта, в конечном итоге, совпадают. Как правило, оценка системы сопоставима с мнением эксперта, если тональность текста определена с точностью 70 % [4].

Таким образом, социальные медиа-ресурсы получили широкое распространение в современном информационном обществе, представляя собой совершенно новый вид коммуникации, который позволяет пользователям обмениваться различного рода контентом, в том числе, содержащем текстовую информацию. При автоматическом анализе тональности текста в социальных медиа-ресурсах целесообразно использовать методы и алгоритмы машинного обучения, поскольку их результат сопоставим с результатом ручного анализа эксперта.

Список используемых источников

1. Борченко И. Д. Социальные медиа как инструмент массовой коммуникации // Наука и образование в XXI веке. Международная научно-практическая конференция : сб. науч. тр., 30 сентября 2013 г. Часть 7. Тамбов, 2013. С. 35.

2. Литвинов В. Л., Румянцева В. О. Интеллектуальный профиль среды машинного обучения Azure Machine Learning // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 2-х т. 2016. Т 2. С. 133–136.

3. Субботин С. В., Большаков Д. Ю. Применение байесовского классификатора для распознавания классов целей // Журнал Радиоэлектроники. 2006. № 4. URL: http://jre.cplire.ru/iso/oct06/2/text.html (дата обращения 30.03.2017).

4. Айсина Р. М. Обзор средств визуализации тематических моделей коллекций текстовых документов. Машина релевантных тегов // Машинное обучение и анализ данных. 2015. № 11. С. 1584–1618.

УДК 004.85

ПРИМЕНЕНИЕ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ ИНТЕРНЕТ-МАРКЕТИНГА

М. И. Короткова, В. Л. Литвинов, К. В. Соколова

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

В статье сформулировано понятие Интернет-маркетинга, приведены основные положения интеллектуальной маркетинговой политики. Рассмотрены основные инструменты и стратегии Интернет-маркетинга, выявлены ключевые компоненты и его главные преимущества. Приведены понятия нейронной сети и машинного обучения. Рассмотрены основные направления развития машинного обучения в задачах Интернет-маркетинга. Описаны возможные инструменты для осуществления этих задач.

машинное обучение, обучение по прецедентам, дедуктивное обучение, искусственные нейронные сети, Интернет-маркетинг, инструменты Интернет-маркетинга, стратегии Интернет-маркетинга.

Машинное обучение (МО) – раздел искусственного интеллекта, изучающий методы построения алгоритмов, способных на обучение выполнению конкретных задач путем анализа заведомо верных входных данных [1].

Машинное обучение подразделяют на два типа: обучение по прецедентам, или индуктивное обучение, и дедуктивное обучение. Обучение по прецедентам основано на выявлении закономерностей в эмпирических данных. Дедуктивное обучение предполагает формализацию знаний экспертов и их перенос в компьютер в виде базы знаний. Данный вид обучения принято относить к области экспертных систем, поэтому термины машинное обучение и обучение по прецедентам можно считать синонимами.

Рассмотрим подробнее обучение по прецедентам. В задачах такого типа дано конечное множество объектов и множество возможных ответов (реакций). При этом существует некоторая зависимость между объектами и ответами, но эта зависимость заранее неизвестна. Известна только конечная совокупность прецедентов – пар «объект, ответ». Такая совокупность называется обучающей выборкой. Требуется по этим данным выявить общие зависимости, закономерности, взаимосвязи, присущие не только этой конкретной выборке, но вообще всем прецедентам, в том числе тем, которые ещё не наблюдались [1].

Основное ожидание, связанное с МО, заключается в реализации потребности в гибких, адаптивных, обучаемых алгоритмах или методах вычислений [2].

Главная задача, решаемая алгоритмами машинного обучения, заключается в отнесении наблюдаемого объекта к тому или другому классу для принятия последующего решения автоматически или человеком. Такие задачи распространены очень широко.

Маркетинговая деятельность включает в себя планирование ассортимента продукции, ценообразование, транспортировку, хранение и складирование продукции, оптовую торговлю, розничную торговлю, обслуживание потенциальных покупателей в торговом зале, кредитование, рекламу, маркетинговые исследования. Каждый из этих видов деятельности нередко смешивают с маркетингом в целом. Однако маркетинг, включая в себя все эти виды, шире любого из них в отдельности. Соответственно, интеграция всех этих действий в единый процесс называется маркетинговой программой.

Современный подход к маркетингу, диктуемый складывающейся экономической конъюнктурой, можно выразить понятием RPB (*Research Planning Branding*), которое включает в себя три основных составляющих: поиск, планирование и брэндинг.

Практически все современные коммерческие компании имеют представительство в Интернете в виде полноценного ресурса, блога, страницы. Однако, просто создав сетевой ресурс и даже заполнив его информационным контентом, невозможно обеспечить автоматическое увеличение продаж и рост популярности компании. Необходима более целенаправленная работа с сайтом специалистов по Интернет-маркетингу.

Интернет-маркетинг (*internet marketing*) – это совокупность приемов в Интернете, направленных на привлечение внимания к товару или услуге, популяризацию этого товара (сайта) в сети и его эффективное продвижение с целью продажи [3].

Можно выделить три основных преимущества современного Интернет-маркетинга: информативность, высокая результативность в сравнении с традиционной рекламой, а также большой охват целевой аудитории, так как в Интернете количество потенциальных покупателей ничем не ограничено.

Выделяют следующие инструменты Интернет-маркетинга: контекстная реклама, баннерная или медийная реклама, E-mail рассылка, SEO-оптимизация, социальные сети, видеоролики, арбитраж трафика.

Контекстная реклама – разновидность сетевой рекламы, при которой рекламное объявление соответствует контенту просматриваемой страницы.

E-mail рассылка – один из самых эффективных и проверенных инструментов Интернет-маркетинга. Позволяет установить доверительные отношения между заказчиками и клиентами.

Социальные сети, как инструмент интернет-маркетинга, обладают рядом неоспоримых преимуществ. Клиент продолжает пользоваться привычным для себя интерфейсом, а компании действуют на безопасной и комфортной для пользователя зоне.

SEO-оптимизация представляет собой комплекс мер и средств, направленных на улучшения позиции сайта в популярных поисковых системах (*Yandex*, *Google*, *Bing*, *Yahoo*). Не важно какую направленность имеет ресурс: основная его задача – привлечение клиентов. Обычно для этих целей используется платная реклама, но получать новый контингент пользователей можно напрямую используя возможности поисковых сервисов.

Арбитражем называют скупку и продажу интернет-трафика по более выгодной стоимости. Посредник покупает баннерную или контекстную рекламу на более популярных ресурсах, в результате чего поток пользователей этих ресурсов направляется на необходимый сайт.

Рассмотрим стратегии Интернет-маркетинга, которые используют представленные выше инструменты: комплексный интернет-маркетинг, интернет-PR и вирусный маркетинг.

Стратегия комплексного интернет-маркетинга представляет собой продуктивное полноценное использование возможностей web-маркетинга и применение их в соответствии с общими стратегиями развития бизнеса в сети. Использование комплексного подхода позволяет достичь так называемого синергетического эффекта (усиления взаимного действия всех компонентов) [3].

Интернет-PR, так же, как и традиционный, повышает узнаваемость бренда и создает «эффект присутствия» компании в информационном пространстве. Наибольший эффект PR достигается путем размещения какой-либо рекламы в авторитетных изданиях с большой аудиторией.

Вирусный маркетинг предполагает создание необычного и запоминающегося контента, а также распространения её по сети. Это могут быть популярные видео или фото материалы, приложения или анимации, а также статьи с кричащими заголовками.

Все рассмотренный методы, инструменты и стратегии бывают настолько же успешными, насколько и затратными. Причем подразумеваются не только финансовые издержки, но и потраченные часы работы специалистов. В эпоху развития технологий, в частности электронных вычислений и искусственного интеллекта, процессы Интернет-маркетинга можно если не полностью, то частично оптимизировать, доверив анализ ситуации и ресурсов компьютеру. С этой проблемой успешно справятся искусственные нейронные сети.

Искусственная нейронная сеть (ИНС) – математическая модель, а также её программное воплощение, построенная по принципу организации и работы биологических нейронных сетей, состоящих из нервных клеток живого организма (рис.).

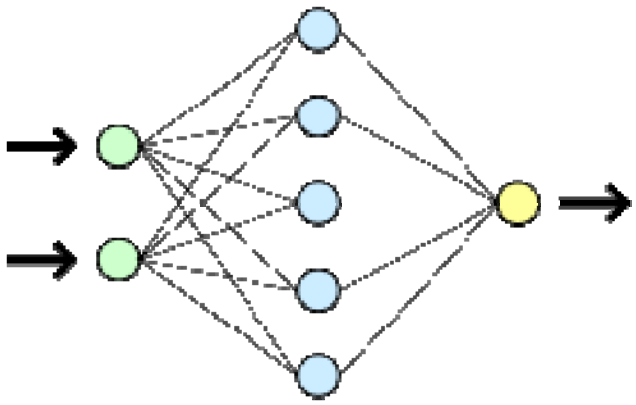


Рисунок. Схема простой нейронной сети

Возможность обучения ИНС – главное преимущество перед традиционными алгоритмами. Технически, весь процесс заключается в нахождении коэффициентов связей между нейронами. В процессе обучения такая сеть выявляет сложные зависимости между исходными и выходными данными, исходя из чего способна выполнять обобщение. Итогом является возможность сети вернуть верный результат на основании данных, которые отсутствовали в изначальной выборке [4].

Правильно обученная нейронная сеть способна, анализируя контент сайта, выделить общую направленность деятельности конкретного ресурса, создать список ключевых слов, которые позволят произвести SEO-

оптимизацию. Понимание контекста также позволит в автоматическом режиме подставлять баннерную или контекстную рекламу. Анализируя новости в интернете, ИНС может прогнозировать, что будет популярно в определенный момент времени, а это позволит маркетологам верно выстроить свой план действий.

На данный момент существует очень богатый инструментарий для создания искусственных нейронных сетей и их машинного обучения. Почти для каждого языка программирования существуют специализированные пакеты и библиотеки по данной тематике. На данный момент наиболее выделяются такие языки как Python и R. Оба языка широко используются для работы с большими объемами данных, обладают высокой степенью гибкости, имеют открытый исходный код и отзывчивых пользователей, которые ежедневно делятся со всеми полезной информацией, а также помогают друг другу. Оба языка имеют продвинутые инструменты для выполнения проектов в сфере науки о данных. Язык программирования Python разрабатывался для создания программных продуктов, упрощения процесса разработки, так как является весьма дружественным для начинающих программистов. Python является лидером в разработке приложений. В то же время R создавался в основном для разработки проектов в области анализа данных, которые сфокусированы на статистике и визуализации.

Методы машинного обучения не имеют ограничений на природу описываемых с их помощью явлений. Для применения алгоритмов не важно, идет ли речь о данных с датчиков технологического процесса, данных продаж интернет-магазина или словах для перевода на другой язык. Перевод – та область, в которой машинное обучение совершило революцию. Перевод в поисковых системах основан на огромной базе текстов. Здесь не нужно выводить правила, согласовывать члены предложения: текст в выдаче будет определен на основании статистических показателей.

Другие области, в которых машинное обучение не только получило применение, но и вывело решения на новый уровень – это сам поиск, обработка результатов научных исследований, прогнозирование загруженности дорог, выявление фактов мошенничества, медицинские исследования. Там машинное обучение дает уникальные по ценности результаты.

В то же время маркетинговые данные имеют весьма существенные отличия. Данные о конкретных пользователях, их поведении и действиях, полезны не во всех маркетинговых каналах. Они хорошо подходят для персонализации сайта, E-mail-рассылок, рекламных моделей.

В других каналах индивидуальная персонализация невозможна или бесполезна: SEO, контекстная реклама, в которых в лучшем случае можно мыслить и работать с сегментами пользователей, а также реклама в офлайне, которая по-прежнему составляет главную строку бюджета маркетинговых затрат.

Список используемых источников

1. Литвинов В. Л., Румянцева В. О. Интеллектуальный профиль среды машинного обучения AzureMachineLearning / Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 3-х т. 2016. Т. 2. С. 133–136.
2. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. М. : ДМК Пресс, 2015. 400 с.
3. Вольфсон М. Б., Соловьева Ю. И. Прогнозирование и оценка эффективности рекламной кампании фирмы в сети Интернет // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 2-х т. 2015. Т. 1. С. 730–735.
4. Хайкин С. Нейронные сети: полный курс = Neural Networks: A Comprehensive Foundation. 2-е изд. М. : Вильямс, 2006. 1104 с.

УДК 004.75

АНАЛИЗ ГИБРИДНЫХ ОБЛАЧНЫХ РЕШЕНИЙ ДЛЯ УПРАВЛЕНИЯ СИСТЕМАМИ ХРАНЕНИЯ ДАННЫХ

М. В. Котлова, Л. К. Птицына

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

В статье рассмотрены идеи формирования дата-центров. Проанализирована специфика функционирования систем, обеспечивающих надежность распределенного хранения информации. Проведен анализ современной инфраструктуры многоуровневого хранения данных и определены основные проблемы синергии между различными уровнями. Рассмотрена интеграция облачных технологий в системы хранения данных.

центр обработки данных, система хранения данных, облачное решение, распределённая файловая система, консенсусный алгоритм.

Согласно Программе цифровой экономики, утверждённой Распоряжением Правительства Российской Федерации № 1632-р от 28.07.2017, данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности. Одна из основных целей базового направления развития цифровой экономики, касающегося информационной инфраструктуры, ориентируется на развитие системы российских центров обработки данных, которая обеспечивает предоставление государству, бизнесу и гражданам доступных, устойчивых, безопасных и экономически эффективных услуг по хранению и обработке данных

на условиях и позволяет экспортировать услуги по хранению и обработке данных.

Центр обработки данных (*data-center* – дата-центр) предназначается для выполнения функций обработки, хранения и распространения по сетям информации в интересах некоторого сообщества клиентов. Дата-центр создаётся как специализированный комплекс интеграции серверного и сетевого оборудования, предусматривающий эффективное использование технических средств за счёт сокращения расходов на администрирование при решении бизнес-задач путём предоставления информационных услуг.

В инфраструктуре типового центра обработки данных различаются: информационная инфраструктура, телекоммуникационная инфраструктура и инженерная инфраструктура, обеспечивающая функционирование образующих систем.

Одна из ключевых задач инженерной инфраструктуры заключается в поддержании постоянной низкой температуры. В настоящее время акцентируется внимание исследователей на оригинальных решениях указанной задачи:

– размещение оборудования центра обработки данных в горной выработке;

– размещение оборудования центра обработки данных в глубине океана;

– создание гигантской цилиндрической материнской платы с полой сердцевиной, обеспечивающей естественную циркуляцию воздуха для охлаждения аппаратуры.

По мере повышения степени интеграции оборудования в центрах обработки данных расширяются преимущества построения современных IT-инфраструктур на базе коммуникационной технологии Infiniband, обеспечивающей высокую доступность, упрощение администрирования, повышение надежности и увеличение утилизации ресурсов. Преимущества обуславливаются благодаря иерархической приоритизации трафика, низкой латентности, масштабируемости, возможностям резервирования и вариациям выбора скоростей передачи. Расширение преимуществ технологии Infiniband достигается на основе её использования совместно с низкоуровневыми универсальными программно-аппаратными интерфейсами и высокоуровневыми программными интерфейсами и протоколами.

С развитием информационных технологий усложняется современная инфраструктура хранения данных, ориентированная на хранение больших массивов данных в распределенных системах. Представленные системы разделяются на два класса: распределенные файловые системы (например, *Google File System*, *Hadoop Distributed System*) и распределенные хранилища структурированных данных (например, *Google BigTable*, *HBase*).

Расширение разнообразия программных продуктов и поставщиков услуг становится основной причиной введения нескольких уровней хранения данных, требующих синергии между ними. Для решения этой задачи может использоваться файловая система с перекрестным облаком.

Легкость интеграции кросс-облачной масштабируемой файловой системы заключается в том, что используется программное обеспечение, устанавливаемое и запускаемое в облаке или на компьютерах организации, а не на удаленном объекте, таком как ферма серверов. Кроме того, распределенная файловая система является встроенным решением и применяется для обеспечения максимальной производительности и улучшения срока службы дата-центров.

Для создания облачных или гетерогенных платформ с изменяемой рабочей нагрузкой при минимальном аппаратном управлении требуется новая файловая система. Подобная система, разработанная без использования открытых программных кодов или существующих файловых систем, анонсируется корпорацией Elastifile. В распределенной файловой системе используется новый консенсусный алгоритм Bizur для согласования состояния данных [1].

Благодаря отсутствию необходимости подключения схемы распределенного журнала, новый алгоритм Bizur отличается преимуществами от других распределенных логических консенсусных алгоритмов, поскольку он характеризуется большим количеством операций ввода-вывода в секунду и более низкими задержками во время нормальной работы, а также во время сбоев [1]. За счёт интеграции технологии гибридного облака обеспечивается быстрое распространение облачных инфраструктур.

Система Elastifile Cloud File System (ECFS) является уникальным программным обеспечением, определенным инфраструктурным решением, которое ориентируется на управление динамическими нагрузками в гетерогенных средах с последовательным масштабированием производительности [2]. Представленная файловая система является первым решением, разработанным для эффективного удовлетворения следующих ключевых критериев:

– унифицированный доступ к данным;

– легкая масштабируемость облака;

– беспрепятственная передача данных между локальным и облачным хранилищем.

В рассмотренной архитектуре данного решения предусматриваются гибкие режимы организации работ, позволяющие развернуть систему локально или в облаке, или применить гибридное решение, сочетающее оба подхода. На рис. представляются типовые варианты развертывания системы ECFS.

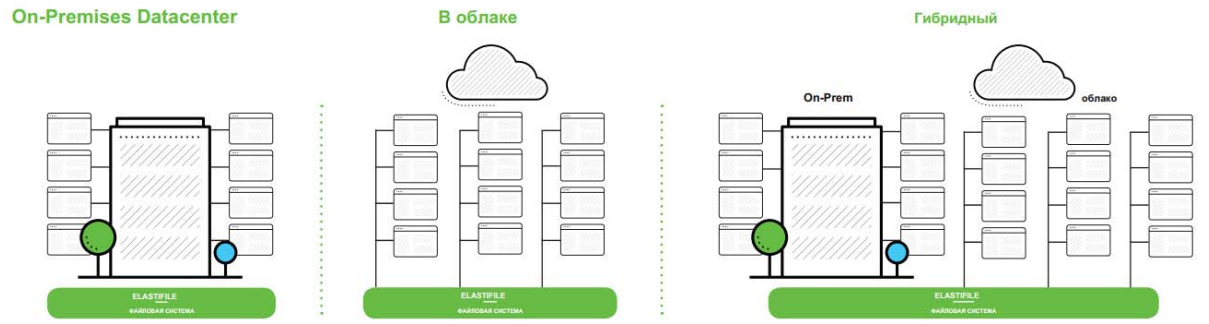


Рисунок. Варианты развертывания системы ECFS

Применение гибридных облачных решений для дата-центров предоставляет возможность организовать простой и объединенный доступ к профилированным данным.

Технология, разработанная компанией Elastifile, позволяет предприятиям размещать данные и приложения в облачном хранилище без какой-либо модификации и беспрепятственно управлять ресурсами распределенной файловой системы.

Список используемых источников

1. Hoch E. N., Ben-Yehuda Y., Lewis N., Vigder A. Bizur: A Key-value Consensus Algorithm for Scalable File-systems. URL: https://pdfs.semanticscholar.org/d48a/0c8db425d817ec45cf5ae8ea b29414464eeb .pdf (дата обращения 15.02.2018).

2. Frank S., Cohen A. The Elastifile cross-cloud data fabric. URL: http://www.elastifile.com/wp-content/uploads/epub/pdf/White-Paper-Lift-Shift-and-Go.pdf (дата обращения 27.01.2018).

УДК 004.75

СОВРЕМЕННЫЕ МЕТОДОЛОГИИ ОРГАНИЗАЦИИ ДОЛГОСРОЧНОГО ХРАНЕНИЯ АРХИВНЫХ ДАННЫХ

М. В. Котлова, Л. К. Птицына

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

Проведен анализ современного состояния и тенденций развития технологических процессов по организации длительного хранения информации. Рассмотрены основные проблемы и сформированы требования к методологиям сохранения архивных данных. Представлены основные компоненты наукоёмкого ядра методологий. Описаны архи-

тектурные решения долгосрочного хранения информации. На основе проведенного анализа определены тенденции развития технологий хранения архивных данных.

система хранения данных, стандарты хранения информации, форматы хранения данных, архитектура систем хранения данных.

По мере расширения сфер профессиональной деятельности, выполняемых с использованием цифровых технологий, возрос практический интерес к хранилищам данных и их оперативной аналитической обработке. Традиционные хранилища данных и инструменты оперативной аналитической обработки поддерживают архивы, но рассматривают их как любые другие данные. В целях развития экономики знаний появилась объективная необходимость в объединении функциональности инструментов оперативной аналитической обработки и технологий долгосрочного хранения.

С развитием информационных технологий возрастают и объемы информации, нуждающиеся в долгосрочном хранении. В исследовании EMC Digital Universe, проведенном совместно с IDC, приведена оценка объемов цифровой вселенной: в 2013 г. насчитывалось всего 4,4 ЗБ, а к 2020 г. это значение по прогнозам увеличится до 44 ЗБ (1 ЗБ = 1 000 000 000 ТБ) [1].

IT-специалисты выделяют три основных класса информации, которые составляют большую часть объема архивных данных, подлежащих долгосрочному хранению:

1) метаданные (данные, которые позволяют описывать содержание, объем, положение в пространстве, качество и другие характеристики пространственных данных и пространственных объектов);

2) цифровые копии музейного наследия (образы предметов, артефактов, представляющих научную, историческую и культурную ценность, библиотечные и архивные фонды);

3) массивы данных, сохранение которых регламентировано законодательными и локальными актами.

Для формирования методологии хранения архивных данных определяют основные требования, предъявляемые к системам хранения:

– безграничное время хранения в системе и доступа к её данным;

– устойчивость системы к физическому воздействию;

– полезность сохраняемой в системе информации;

– целостность архивных данных системы;

– защищенность информации системы;

– оптимальная совокупная стоимость хранения и доступа к данным системы;

– возможность интеграции системы с технологиями построения информационной инфраструктуры.

Непрерывное развитие информационных технологий стимулирует регулярное изменение форматов и протоколов доступа к данным. К основным угрозам, связанным с потерями информации, относят чрезвычайные и форс-мажорные ситуации, проблемы с физическими носителями, устаревание программного и аппаратного обеспечения, утрата контекста или метаинформации.

Ключевыми компонентами методологии сохранения данных считают стандарты архитектур и функций архивов, форматы хранилищ данных и программное обеспечение, позволяющее обеспечить сохранность и организовать доступ к информации.

Стандарт OAIS (*Open Archival Information System*) описывает типовую архитектуру и функции электронного архива. Система, построенная согласно стандарту OAIS, использует понятие пакет передаваемой информации (SIP-архив с информационными объектами). На рис. 1 представлены функциональные объекты стандарта OAIS.

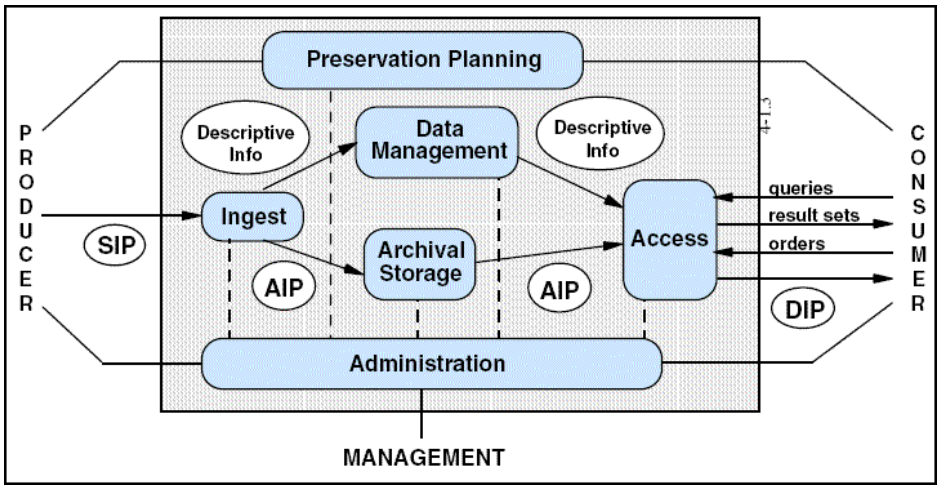


Рис. 1. Функциональные объекты по стандарту OAIS

Стандарт VERS (*Victorian Electronic Records Stra*tegy) направлен на поддержку агентств в управлении и сохранении полных, документированных и достоверных цифровых записей.

Спецификация MoReq (*Model Requirements for the management of electronic records*) представляет собой основополагающий документ, регламентирующий требования к системам электронного документооборота.

Автономный формат хранения информации (SIRF) обеспечивает долговременным физическим и облачным хранилищам эффективные способы сохранения и защиты цифровой информации на протяжении многих десятилетий в условиях постоянно меняющегося технологического сопровождения.

Стандарт eXchange (AXF) определяет архивный формат инкапсуляции для общего содержимого на основе файлов, который позволяет сохранять и переносить архивные данные на различные носители без учета применяемой технологии и типа операционной системы.

Технология AXF абстрагирует базовую технологию файлов и операционной системы, облегчающую долгосрочную переносимость и доступность файлов, содержащихся в контейнере, при одновременном добавлении нескольких характеристик сохранения открытых архивных информационных систем, соответствующих стандарту OAIS, для обеспечения долгосрочной защиты файловых активов [2].

Спецификация Baglt представляет собой набор иерархических условных обозначений файловой системы, предназначенных для поддержки дискового хранения и сетевой передачи произвольного цифрового контента.

Для управления системами хранения данных существует представительное разнообразие программного обеспечения.

Система LOCKSS позволяет организациям с разрешения издателя собирать, сохранять и распространять копии материалов, а также предоставлять доступ к открытым данным.

Программный пакет DSpace поддерживает создание репозиториев открытого доступа для научного и/или опубликованного цифрового контента.

Компания Arkivum является ведущим поставщиком программного обеспечения для долгосрочного мониторинга данных и обеспечения удобства их использования. Предлагаемые решения помогают организациям защищать и сохранять ценнейший цифровой контент на высшем уровне, поддерживать усиленное регулирование управления цифровыми отчетами, экономично отслеживать увеличение объема данных и предоставлять доступ к архивным данным.

Программное обеспечение iRODS предназначают для управления данными и метаданными, хранящимися на серверах, объединенных в конфедерации. Представленный продукт используют в исследовательских целях и для правительственных организаций.

Значительное возрастание производительности вычислительных ресурсов за последнее десятилетие обуславливает объективную необходимость совершенствования механизмов хранения информации. На рис. 2 представлен один из перспективных вариантов изменения архитектуры систем хранения архивных данных.

Представленный вариант предусматривает использование оптических носителей. Профессиональные оптические накопители не только обеспечивают надежное хранение на протяжении 100 лет, но и поддерживают методологии многоуровневого и многослойного хранения данных.

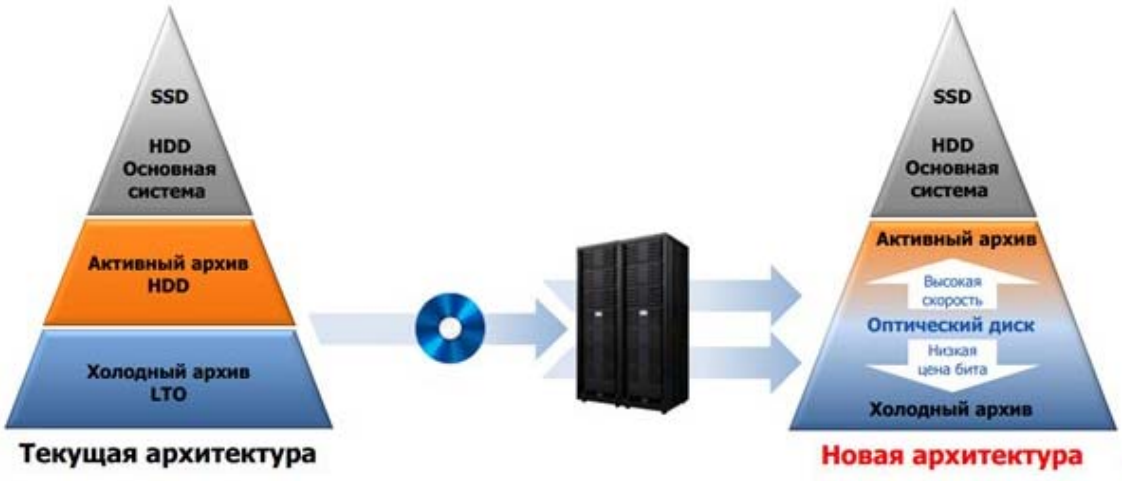


Рис. 2. Изменение архитектуры систем хранения данных

Список используемых источников

1. The Digital Universe of Opportunities. URL: https://russia.emc.com/collateral/ analyst-reports/idc-digital-universe-2014.pdf (дата обращения 10.02.2018).

2. Ковалев А. Д., Никифоров И. В., Котляров В. П. Разработка распределенной системы архивации данных на основе стандарта OAIS с использованием технологии APACHE HADOOP // Информатика и кибернетика (ComCon – 2016) : сборник докладов студенческой научной конференции Института компьютерных наук и технологий, 4–9 апр. 2016 г. СПб. : Изд-во Политехнического ун-та, 2016. С. 250–252.

УДК 004.62

К ПРОБЛЕМЕ ПЕРЕХОДА НА СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

А. А. Кузькин, М. А. Куцакин, А. Н. Лапко, В. В. Рябоконь

Академия Федеральной службы охраны Российской Федерации

Политика государства, направленная на импортозамещение в том числе и в информационной сфере, подразумевает развитие и внедрение свободного программного обеспечения отечественного производства во все сферы деятельности человека. Особенно остро этот вопрос рассматривается в рамках государственных организаций и служб. При этом важной остается проблемы, связанные с затратами материальных и временных ресурсов, с быстрым и эффективным обучением персонала первичным навыкам работы в подобном программном обеспечении или операционных системах семейства Unix. Также особо остро стоит вопрос о переносе всех информационных процессов организации в Unix-системы. В данной работе коротко представлен порядок приобретения первичных навыков работы в операционных системах

семейства Unix, а также состав и вариант стенда для отработки практических заданий.

операционные системы, Unix, Linux, обучение персонала.

Концепция свободного программного обеспечения (СПО) (*free software*) заключается в том, чтобы разрешить каждому использовать, копировать и распространять ПО, как в точности, так и с модификациями, безвозмездно или за плату [1].

На данный момент времени, зачастую, выделяют четыре основных критерия, используемых для оценки степени свободы ПО [1]:

1. Свобода запускать программу в любых целях (свобода 0).
2. Свобода изучения работы программы и адаптация ее к нуждам конкретного пользователя или организации (свобода 1).
3. Свобода распространять копии ПО (свобода 2).
4. Свобода улучшать программу и публиковать произведенные изменения для использования их другими пользователями (свобода 3).

ПО считается свободным, если пользователи располагают всеми четырьмя свободами. Однако доступ к исходным текстам программ является обязательным условием, которое позволяет производить сертификацию подобного ПО и, впоследствии, использовать его в рамках обработки конфиденциальной информации (например, операционная система Astra Linux SE). Это положение легло в основу современной стратегии развития информационных технологий, в том числе и программного обеспечения отечественного производства, направленного на импортозамещение.

Современные источники информации [2] говорят о том, что по данным на середину 2016 г. всего около 23 % всех закупок ПО приходится на отечественные продукты. При этом абсолютное большинство (90–95 %) базового ПО, используемого органами власти, разработано зарубежными ИТ-компаниями. Также в [2] говорится о приблизительных затратах, связанных, например, с обеспечением организации с 16 тысячью рабочих мест свободным ПО, таким как GosLinux. Разница в денежных средствах составляет порядка 40 раз в пользу использования СПО, в том числе и относящихся к нему операционных систем.

Однако существует проблема, касающаяся не только материальных ресурсов, но и временных. Она вытекает из необходимости переподготовки и переобучения персонала организации или компании. Это позволяет сделать вывод об актуальности разработки специальных учебных курсов, программ, практических стендов и т. д., способствующих в кратчайшие сроки приобрести пользователям первичные навыки работы в различных версиях операционных систем семейства Unix, необходимые в рамках решаемых организацией задач.

В данной работе предлагается следующий порядок приобретения навыков работы в операционных системах семейства Unix каждым из сотрудников организации:

1. Изучение теоретических основ, связанных с архитектурой операционных систем семейства Unix (ядро операционной системы *Linux*, компоненты операционной системы *Linux*, дистрибутивы операционной системы *Linux*).

2. Установка дистрибутива Linux (виды установки *Linux*, принципы регистрации в пользовательских сеансах, пользовательский сеанс *Fly*).

3. Основы работы с командным интерпретатором bash (синтаксис команд *bash*, справочная система *man*, базовые команды для работы с файлами, механизм глобальной подстановки, перенаправление стандартного ввода-вывода, основы языка сценариев *bash*).

4. Объединение команд и поиск данных в операционной системе Linux (механизмы объединения команд, поиск файлов в файловой системе).

5. Поиск и фильтрация данных в операционной системе Linux (базовые регулярные выражения, расширенные регулярные выражения).

6. Управление пользователями и модели разграничения доступа (пользователи и группы пользователей, владение объектами файловой системы, дискреционная модель разграничения доступа, мандатная модель разграничения доступа).

7. Администрирование пользователей и групп (управление пользовательскими учетными записями, управление групповыми учетными записями, механизмы повышения привилегий).

8. Управление пользовательскими учетными записями (базовые списки доступа, смена режимов доступа для базовых списков, расширенные списки доступа).

9. Мандатная модель разграничения доступа в операционной системе Linux (мандатная модель разграничения доступа, команды управления мандатной моделью разграничения доступа, управление мандатной моделью с помощью графической оснастки).

10. Управление процессами (принцип порождения процессов, системные структуры для управления процессами, алгоритм планирования процессов, приоритеты процессов).

11. Управление работами и процессами (управление работами, команды мониторинга процессов, передача процессам сигналов и управление их приоритетами, управление сервисами).

12. Управление запоминающими устройствами и файловыми системами (принцип именования устройств ввода-вывода, динамическое именование запоминающих устройств, принцип монтирования файловых систем).

13. Управление дисковыми разделами и файловыми системами (управление дисковыми разделами, создание файловых систем, монтирование файловых систем).

14. Управление сетевым взаимодействием (основы сети с коммутацией пакетов на базе протоколов TCP/IP, принципы планирования и управления сетью TCP/IP, доменная инфраструктура).

15. Администрирование сетевых инфраструктур (использование утилит net tools и iproute, настройка статической маршрутизации в подсетях, настройка сетевых сервисов, настройка домена).

16. Конфигурирование доменной инфраструктуры в Linux (доменная инфраструктура, команды управления доменной инфраструктурой, методика администрирования домена).

Предложенный порядок сопровождается наличием множеством практических заданий для каждого вопроса, что позволит, затратив порядка 40–50 часов, обучить сотрудников любой организации особенностям и первичным навыкам работы в операционных системах семейства Unix.

Наличие практических заданий вызывает необходимость разработки и настройки практического стенда. Его примерный состав и вариант реализации представлен на рис.

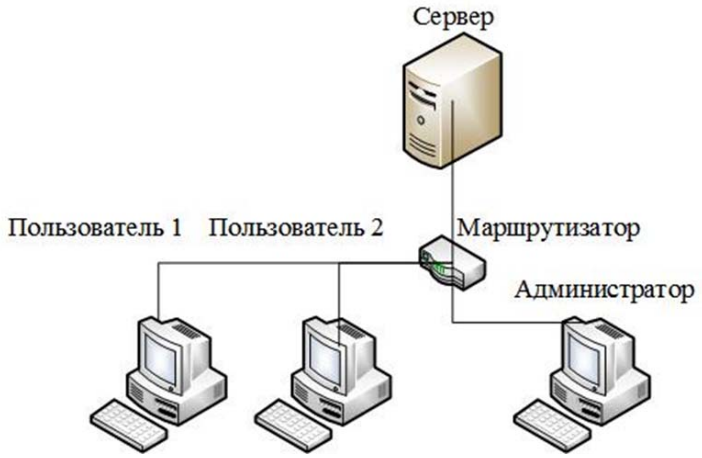


Рисунок. Пример практического стенда на базе операционной системы Linux

Данная конфигурация практического стенда также пригодна для первичной настройки и тестирования сетевых сервисов на базе операционной системы Linux и проверки их работоспособности.

При этом важным моментом в процессе обучения персонала является наличие программ, позволяющих создавать и использовать виртуальные образы операционных систем. Это объясняется необходимостью работы с правами суперпользователя, а также возможностью деструктивного воздействия на аппаратную составляющую ЭВМ.

Однако, в рамках предложенной темы остается нераскрытым важный вопрос, связанный с быстрым переносом всех информационных процессов организации в Linux-системы [3].

Здесь под переносом процессов подразумевается следующее: прекращение выполнения процесса на одном узле системы; сохранение его состояния, в том числе информации об используемых ресурсах, памяти, регистрах процессора, используемых файлах и связях с другими процессами; перенос этих данных на другой узел и, наконец, на основе этих данных создание нового процесса на новом узле, идентичного ранее выполняемому, будто прежний и не прекращал выполняться [3].

Выполнение перечисленных процедур требует от сотрудников углубленных знаний и навыков по организации и администрированию операционных систем Linux. Таким образом, направлением дальнейших исследований в рамках озвученной выше проблемы является проверка разработанного порядка приобретения первичных навыков работы в операционных системах семейства Unix на группе обучающихся. Это позволит подтвердить указанные временные рамки для освоения предложенного материала и скорректировать наполнение предложенного плана переподготовки сотрудников для решения более сложных задач.

Список используемых источников

1. Что такое свободное ПО? [Электронный ресурс]. Режим доступа: http://www.4stud.info/oss/lecture1.html (дата обращения: 22.01.2018).

2. Сменят ли чиновники Windows на Linux? // Сделано в России. 2016. № 04 (57). С. 4–6.

3. Гилев В. А. Новый подход к переносу процессов В Linux-системах // Вестник НГУ. Серия: Информационные технологии. 2007. Т. 5. Вып. 1. С. 3–11.

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ СВЯЗИ

В. И. Курносов, Ю. Ю. Поляков

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

Представлен анализ проблемы защиты информации от несанкционированного доступа в локальной вычислительной сети. Рассмотрена концептуальная модель разграничения доступа к информационным ресурсам. Дана оценка эффективности решений по защите от несанкционированного доступа к информационным ресурсам.

Сформулированы предложения по организации защиты информации в ЛВС предприятия связи.

защита информации, вероятный злоумышленник, несанкционированный доступ, локальная вычислительная сеть, разграничение доступа.

В связи со стремительным развитием информационных технологий в современном мире и стремлением Российской Федерации (РФ) находиться в этой сфере на должном уровне возникает необходимость обращения более серьезного внимания на вопросах защиты информации. Крайне остро в современных условиях стоит проблема защиты информации от несанкционированного доступа на предприятиях связи. Одним из основополагающих организационных принципов обеспечения защиты информации от несанкционированного доступа является ограничение и стабилизация состава допущенных лиц, их тщательная предварительная проверка и сохранение определенного контроля за их деятельностью после прекращения контакта с конфиденциальной информацией. Анализ угроз безопасности информации в вычислительных средах (ВС) на предприятии связи показывает, что основным нарушителем и источником преднамеренной угрозы является санкционированный пользователь.

Вероятный злоумышленник будет использовать эти нарушения в своих целях, при этом осуществляя преднамеренные и случайные угрозы ВС. Поэтому чрезвычайно важным является вопрос разграничения доступа к информационным ресурсам в вычислительной среде и недопущение угрозы нарушения конфиденциальности информации со стороны злоумышленника.

В свою очередь, в дополнение к вышесказанному следует отметить, что комплекс мероприятий по защите информации в автоматизированных системах (АС) управления производственными процессами на предприятиях связи (ПС) позволяет значительно повысить оперативность процессов управления и приводит к значительному увеличению обоснованности принимаемых решений, обеспечивает выполнение требований по устойчивости и непрерывности управления. Разветвленная структура ВС порождает множество разнородных информационных потоков, циркулирующих между управляемыми объектами, объектами управления и взаимодействующими объектами. Локальные вычислительные сети (ЛВС), составляющие основу ВС, строятся на основе современных сетевых технологий и коммуникационного оборудования. Данное обстоятельство позволяет полностью использовать средства обеспечения безопасности информации, реализуемые в них, такие как, например, технология виртуальных ЛВС (ВЛВС). Технология ВЛВС является технологией разграничения доступа к информационным ресурсам. Методический аппарат использования ВЛВС, в силу новизны данной технологии, еще слабо развит. Однако со-

вместное использование технологии ВЛВС с другими средствами и механизмами разграничения доступа, применяющимися в ВС, представляется достаточно эффективным в плане комплексной защиты информации от несанкционированного доступа (НСД).

Вопросы по защите информации от НСД в АС в различных аспектах рассматривались в работах Зегжды П. Д., Доценко С. М., Буйневича М. В., Бушуева С. Н., Бочкова М. В., Саенко И. Б. [1], Авраменко В. С., Копчака Я. М., Супруна А. Ф. [2], Матвеева В. В. Однако вопросы защиты конфиденциальной информации на технологии ВЛВС в данных работах не нашли должной проработки. Этими обстоятельствами предопределяется актуальность инженерной задачи: разработать модель разграничения доступа к информационным ресурсам в локальных вычислительных сетях предприятий связи и на ее основе разработать методику защиты информации от НСД ВЛВС.

Решение данной задачи возможно посредством решения следующих частных подзадач:

анализа механизмов реализации угроз конфиденциальности сведений, используемых на предприятии связи;

анализа возможностей наиболее существенных средств и методов защиты информации от НСД, используемых на ПС, в частности, технологии ВЛВС;

разработки модели к информационным ресурсам ЛВС ПС, построенных на основе концепции ВЛВС;

разработки методики защиты информации от НСД в ВС ПС, позволяющей использовать разработанную модель для решения многокритериальной задачи синтеза требуемой схемы разграничения доступа к информационным ресурсам;

разработка предложений по организации защиты информации от НСД в ВС ПС, охватывающих наиболее важные вопросы практической реализации разработанных модели и методики.

С этой целью необходимо:

конкретизировать модель нарушителя в ВС ПС;

обосновать структуру системы защиты информации (СЗИ) от НСД в ВС ПС;

предложить и детально разработать алгоритм оптимизации;

разработать методику защиты информации от НСД в ВС ПС, позволяющую комплексно использовать традиционные средства и методы защиты с технологией ВЛВС.

При этом должны быть обеспечены:

применение апробированных общенаучных и специальных методов исследования;

подтверждение непротиворечивости полученных частных количественных оценок практики функционирования существующих элементов систем защиты.

Основное содержание инженерной разработки должно содержать описание процесса функционирования ПС. На основе его анализа определяются роль и место, а также обосновывается структура системы обеспечения информационной безопасности ВС. Определяются информационные ресурсы, которые требуют особой защиты. Анализируются пути реализации угроз и обеспечения информационной безопасности, производится классификация угроз и рассматривается номенклатура отечественных и зарубежных средств их реализации и защиты. Выявляются основные проблемы защиты информации, возникающие при переходе на автоматизированные способы управления производственными процессами (ПП). Устанавливаются противоречия между существующими ресурсами и высокими требованиями к информационной защищенности ПП. На основе концепции построения защищенной информационной среды осуществляется постановка задачи инженерной разработки.

В ходе разработки модели разграничения доступа к информационным ресурсам в ЛВС необходимо учитывать специфику ее построения на концепции ВЛВС и обеспечить синтез сети по критериям конфиденциальности и доступности информации. При этом важно осуществить анализ возможных методов решения поставленной задачи синтеза, на основе которого могут быть предложены и детально разработаны решения по синтезу структуры ВЛВС с помощью генетических алгоритмов оптимизации.

В свою очередь, методика защиты информации от НСД в ВС ПС должна базироваться на исследовании экспериментальных зависимостей между показателями и параметрами в задаче синтеза схемы разграничения доступа, что позволит выработать предложения по организации защиты информации и осуществить оценку эффективности решений по защите информации от НСД в ВС ПС путем экспериментальных испытаний.

Список используемых источников

1. Бочков М.В., Логинов В.А., Саенко И.Б. Активный аудит действий пользователей в защищенной сети // Защита информации. Конфидент. 2002. № 4–5. С. 94–98.

2. Супрун А. Ф. Комплексное обеспечение информационной безопасности. Моделирование процессов реализации угроз : учеб. пособие. Часть 1. СПб. : СПбГПУ, 2012. 50 с.

УДК 004.62

ОБНАРУЖЕНИЕ ДЕФЕКТОВ КОММУНИКАЦИОННЫХ ПРОТОКОЛОВ С ИСПОЛЬЗОВАНИЕМ ФАЗЗИНГА

М. А. Куцакин, А. Н. Лапко, В. В. Рябоконь

Академия Федеральной службы охраны Российской Федерации

Сетевое тестирование методом фаззинга является эффективным механизмом для обеспечения безопасности и надежности реализации коммуникационных протоколов. Однако, такое тестирование по-прежнему проводится экспертами практически вручную из-за отсутствия формальных моделей протоколов. В этой статье представлен подход к разработке автоматизированного способа тестирования, в котором используется синтезированная приблизительная спецификация протокола для управления процессом тестирования. Также приведены предварительные результаты использования разработанного подхода к реализациям клиентов pidgin и aMSN.

фаззинг, тестирование безопасности, сетевой протокол.

Фаззинг (*fuzzing, fuzz testing*) – это метод тестирования программного обеспечения, часто автоматизированный или полуавтоматический, который включает в себя подачу недействительных, неожиданных, или случайных данных на вход компьютерной программы [1]. Программа затем контролируется на появление исключительных ситуаций, сбоев или возможных утечек памяти.

Тестирование коммуникационных протоколов методом фаззинга направлено на повышение надежности и безопасности систем вследствие раннего обнаружения дефектов реализации и своевременного их исправления [2]. С этой целью на входной интерфейс тестируемого компонента подается измененный трафик для выявления нарушения конфиденциальности информации, а также любого другого нежелательного или неопределенного поведения. Обнаружение таких недостатков чрезвычайно важно, поскольку они могут быть использованы злоумышленниками для реализации сетевых атак. Для современных сложных программных продуктов и сетевых протоколов эти недостатки повсеместны из-за некорректной обработки входных данных. Тестирование методом фаззинга по принципу «черного ящика» не подразумевает наличие априорных знаний о структуре использующегося коммуникационного протокола, что затрудняет измерение полноты тестирования и автоматизацию процесса в целом. Знание формата сообщений протокола несколько упрощает ситуацию, однако часто возникает ситуация различного обслуживания сообщений одного типа,

выполняющих разные роли в сеансе протокола, что следует учитывать при тестировании.

Ключевой возможностью метода фаззинга является его способность автоматизировано формировать тестовые входные данные. Увеличение доли автоматизированных операций положительно влияет на воспроизводимость при проведении тестирования методом фаззинга. Достоинства этого свойства можно объяснить двумя ключевыми факторами:

1) Тесты, созданные для одной версии коммуникационного протокола, могут успешно использоваться для последующих версий того же или другого похожего протокола.

2) В случае ошибки в тестируемом протоколе необходимо как можно более точно воспроизвести последовательность событий целиком, чтобы определить причину ошибки.

Основная идея автоматизации для улучшения качества тестирования и его измеримости состоит в формальном синтезе приблизительной модели протокола и последующем ее использовании для выбора тестов с целью наилучшего покрытия возможных дефектов. Такая модель основана на предполагаемом знании протокольных сообщений и ее основной функцией является описание состояний и переходов в сеансе протокольного взаимодействия. В случае, когда формальные спецификации протокола недоступны для реальных систем, построение подобной модели существенно усложняется, поскольку необходимо изначально методом проб и ошибок частично подобрать подходящую для описания спецификацию.

Для моделирования коммуникационного протокола можно адаптировать аппарат взаимодействующих конечных автоматов (CEFSM, *Communicating Extended Finite State Machine*), при этом поведение каждого элемента протокола описывается детерминированным конечным автоматом, который имеет переменные состояния и параметры входа/выхода с символической областью значений [3]. Такой автомат представляет собой кортеж $<S, s_0, I, O, f_{next}, f_{output}>$, включающий конфигурацию состояний, входной и выходной алфавит, функции перехода и выхода. Трассой конечного автомата является последовательность пар входа/выхода $tr = \{<I_1, O_1>, <I_1, O_1>,\ldots,<I_k, O_k>\}$, образуемая конкретным тестовым случаем, т. е. последовательностью входных данных. Целью тестирования является поиск такой последовательности длины L: $\{<I_k, O_k>, 0 \le k \le L\}$, которая приведет реализацию протокола к наблюдаемому сбою.

Поскольку тестировщик полностью контролирует вход и выход пока абстрактного автомата, очевидным способом получить его модель является активное обучение. Генератор тестов выполняет роль «учителя» в процессе обучения, обеспечивает трассировку результатов и сравнение трасс. Этот итерационный процесс начинается с небольшого подмножества входного алфавита и заканчивается, когда учитель больше не может найти

подходящие примеры для обучения. Из работы [3] можно сделать вывод, что при наличии N состояний автомата и P различных входов, для приближенного моделирования достаточно $(N + P)$ предположений. Вычислительная сложность процесса при этом будет определяться как стратегией, используемой учителем, так и самим обучающим алгоритмом, и для наихудшего случая она составит $O(T \cdot P^2 \cdot N^2 + T \cdot P \cdot N^3)$, где T определяет сложность вычисления примера на каждой итерации. На практике для получения приблизительной модели можно ограничиться небольшим количеством итераций обучения.

Второй подход к получению модели требует большего количества наблюдений, но потенциально меньшего количества вычислений. При этом сначала собирается значительное количество трасс путем пассивного мониторинга, а затем строится и минимизируется граф конечного автомата. Построение начинается с пустого графа, в который добавляется по одной трассе за раз. При этом находится самый длинный префикс трассы, которая предварительно заканчивается в состоянии s и уже находится в текущем графе, создается новая ветвь от состояния s до окончания трассы. Одной из практических проблем на данном этапе является обработка полей данных, связанных с сеансом. Типичными примерами полей, значение которых не влияет на переходы между состояниями в сеансе, являются имя пользователя, идентификатор сеанса и т. п. Идентификация этих полей уменьшает избыточность графа конечного автомата, но при этом является нетривиальной задачей, требующей индивидуального подхода. После построения конечного автомата его граф минимизируется путем слияния совместимых наборов. Подобная задача минимизации конечных автоматов – хорошо изученная проблема класса NP-hard, для решения которой существует множество эвристических решений, например, алгоритм Бьермана [4]. Вычислительная сложность подобных алгоритмов в наихудшем случае является экспоненциальной, но при введении определенных ограничений можно получить полиномиальный субоптимальный алгоритм, а в крайнем случае и с линейной сложностью.

После синтеза приблизительной спецификации протокола M_x она может использоваться для управления экспериментами по тестированию методом фаззинга. Метрика покрытия тестами может быть определена для измерения полноты набора тестовых последовательностей. Для мутационного фаззинга требуется определение места внесения искажений, поскольку беспорядочное искажение данных, как правило, приводит к игнорированию тестов. Для применения генерационного фаззинга требуется формальное описание структур данных, которое не всегда возможно выполнить. Пусть в M_x задана последовательность $I_0 I_1 \ldots I_L$, тогда тестовая последовательность фаззинга имеет общий вид $I_0 I_1 \ldots I_k \, f_{fuzz}(I_{k+1} \ldots I_L)$, где префикс длины k является ведущей последовательностью, которая приводит

граф B в определенное состояние, а остаток – результат применения функции фаззинга f_{fuzz}: $I^* \rightarrow I_B{}^*$ к оригинальному окончанию последовательности.

При заданном наборе из K тестовых последовательностей $\{SEQ_i = PREFIX_i\, f(LAST_i) | \; 0 \le i \le K,\; PREFIX_i \in I^*,\; LAST_i \in I\}$ приведенная ниже формула вычисляет полноту покрытия как число переходов, охваченных последним входным сообщением к общему числу переходов в M_x:

$$\mathrm{TR}_{\mathrm{Cov}} = \frac{\left|\{< s', LAST_i > | \; s' = f_{next}(s_0, PREFIX_i) \wedge f_{next}(s', LAST_i)\downarrow\}\right|}{\left|\{< s, i > | \; f_{next}(s,i)\downarrow, s \in S, i \in I\}\right|}.$$

Другие метрики могут быть аналогичным образом разработаны в соответствии с использующимися функциями f_{fuzz} над входной последовательностью, например, повтором, стиранием и т. д. Фактически, генератор тестов должен быть сконструирован таким образом, чтобы отдавать предпочтение последовательностям, которые увеличивают выбранную метрику.

Обе стратегии синтеза модели и некоторые типовые функции фаззинга были протестированы на MSN клиентах мгновенной передачи сообщений Gaim (*pidgin*) и aMSN. С целью контроля входа/выхода между клиентом и сервером был установлен прокси-сервер (рис.). Целью тестирования был поиск входных последовательностей, которые приводили к критическим ошибкам клиента. Модель кодера/декодера протокольных сообщений MSN содержала около 50-ти состояний и 70-ти переходов, некоторые типичные функции фаззинга были разработаны и добавлены вручную, чтобы примерное покрытие тестами приблизилось к 100 %.

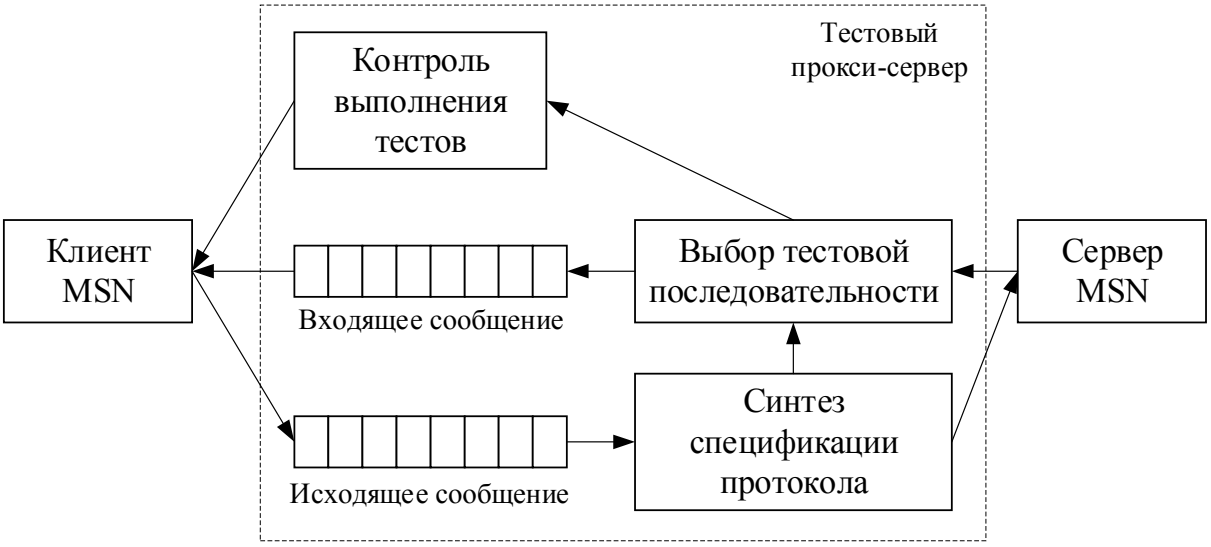


Рисунок. Схема тестового стенда фаззинга

Функции фаззинга при этом либо изменяли поля данных сообщения для формирования неверного входа, либо изменяли тип сообщения для формирования неверного перехода из текущего состояния. В результате были обнаружены некоторые ранее неизвестные дефекты:

– неверный код статуса. Клиент aMSN завершает работу при получении кода статуса не из заранее сформированного списка в ILN-сообщении, передающем текущий статус клиента (свободен, занят, отошел);

– удаление поля адреса электронной почты. Сбой происходит в обоих клиентах при удалении любых полей, связанных с почтой (которая используется как имя учетной записи);

– пропуск сообщения списка контактов. Для получения пользовательских списков клиент обменивается с сервером цепочкой сообщений LST (список контактов) и ILN (информация о присутствии). Если отбросить сообщение LST, то при приеме сообщения ILN в мессенджере aMSN происходит сбой;

– случайная мутация типа сообщения. Сбой проявляется периодически при изменении типа входного сообщения на случайный, неопределенный для данного состояния. Например, при изменении сообщения CVR или VER (используются для согласования версии протокола) на тип LST, оба клиента аварийно завершают свою работу.

Предложенный подход к тестированию сетевых приложений и протоколов показал неплохой потенциал к практическому применению. Ключевой проблемой и направлением дальнейших исследований является улучшение качества синтезированной модели в части, касающейся интеграции плоскости управления и плоскости данных протокольных трасс, что даст больше информации о направлении мутации входных данных, приводящему к сбою. С другой стороны, построение даже приближенной модели протокола может быть полезно в других областях, например, реверсной инженерии протокола [5] и проведении сетевого тестирования.

Список используемых источников

1. Fuzz testing [Электронный ресурс]. Режим доступа: http://en.wikipedia.org/wiki/fuzz_testing (дата обращения: 13.12.2017).

2. Dolev, D., Yao, A.: On the security of public-key protocols // IEEE Transaction on Information Theory 29, 1983 С. 198–208.

3. Lee, D., Yannakakis, M.: Principles and methods of testing finite state machines // A survey. In: Proceedings of the IEEE, 1996. С. 1090–1123.

4. Gören, S., Ferguson, F.J.: On state reduction of incompletely specified finite state machines // Computers and Electrical Engineering 33(1), 2007. С. 58–69.

5. Cui, W., Kannan, J., Wang, H.: Discoverer: Automatic Protocol Reverse Engineering from Network Traces // The 16th USENIX Security Symposium, 2007.

УДК 004.65

РАЗРАБОТКА БАЗЫ ДАННЫХ УЧЕТА ДАННЫХ РАДИОЧАСТОТНЫХ ЗАЯВОК В ЗАДАЧЕ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ РАДИОЧАСТОТНОГО СПЕКТРА

М. А. Куцакин, А. Н. Лапко, В. В. Рябоконь

Академия Федеральной службы охраны Российской Федерации

Статья посвящена вопросам разработки базы данных учета данных, представленных в радиочастотных заявках. Раскрыто место учета данных в общей задаче управления использованием радиочастотного спектра. Детально описаны результаты анализа радиочастотных заявок на предмет наличия функциональных зависимостей. Представлена схема логической структуры базы данных, предусматривающая взаимосвязь выделенных объектов учета. Раскрыты вопросы обеспечения согласованности данных базы данных.

база данных, учет данных, радиочастотная заявка, управление использованием радиочастотного спектра.

Построение информационного общества на основе внедрения новейших систем телекоммуникаций является актуальной государственной задачей. В настоящее время большим спросом пользуются услуги, предоставляемые на основе использования радиочастотного спектра (РЧС). Ограниченность и особенности РЧС, как государственного природного ресурса, обладающего экономической ценностью и социальной значимостью, и возрастающая потребность в нем обуславливают необходимость управления использованием РЧС. Главная цель такого управления заключается в обеспечении функционирования как можно большего количества радиоэлектронных средств (РЭС) в условиях электромагнитной совместимости (ЭМС) на определенной частоте в конкретном месте. На практике с учетом постоянного увеличения количества РЭС и усложнения электромагнитной обстановки достижение такой цели может оказаться достаточно сложной задачей.

Один из подходов решения описанной задачи заключается в аккумулировании информации о РЭС, предоставляемых заявителями в радиочастотных заявках (РЧЗ) на этапах выделения полос радиочастот и присвоения (назначения) радиочастот, и расчете ЭМС заявленных РЭС с действующими [1]. Данный подход предполагает использование различных средств автоматизации (рис. 1):

– автоматизированной системы (АС) управления использованием РЧС, предназначенной для ведения и поддержания в актуальном состоянии базы данных (БД) РЭС;

– программного комплекса ITDI, применяемого для расчета электромагнитной совместимости РЭС;

– БД Международного союза электросвязи (МСЭ) таких как TerRaBase, SRS и GIMS, содержащих информацию о РЭС иностранных государств, расположенных в приграничных зонах или на орбитальных спутниках.

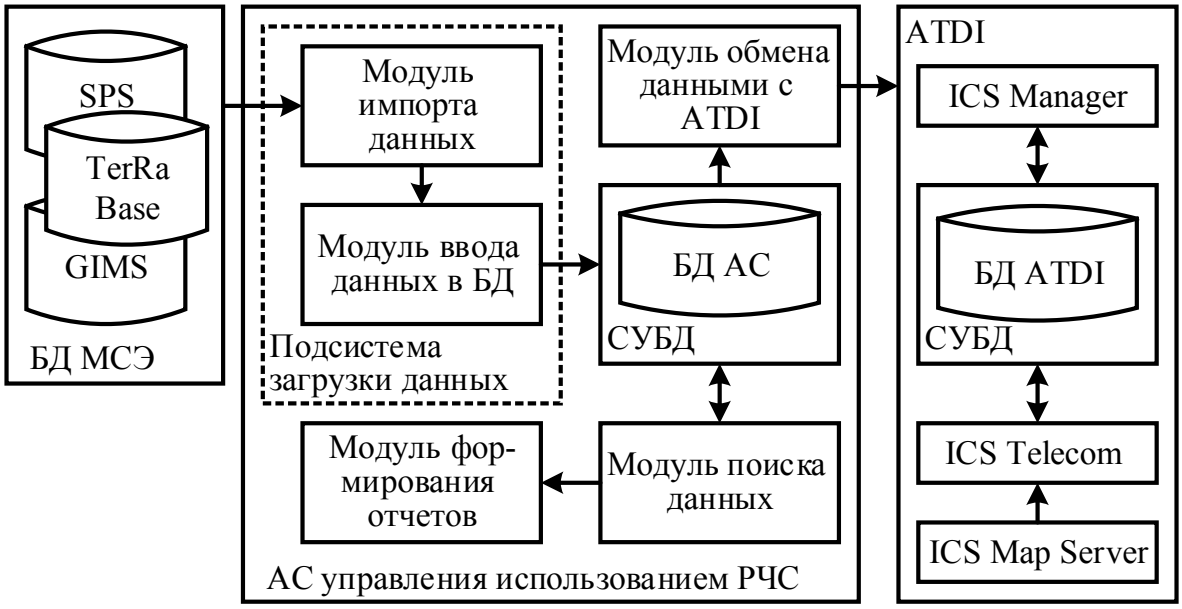


Рис. 1. Структурная схема АС управления использованием РЧС

Ключевым компонентом АС управления использованием РЧС, посредством которого обеспечивается взаимосвязь всех остальных компонентов, является БД. С целью разработки логической структуры БД проведен анализ данных, учитываемых в радиочастотных заявках, на предмет наличия функциональных зависимостей (табл.).

ТАБЛИЦА. Функциональные зависимости

Детерминант (таблица)	**Набор зависимых атрибутов (*домен*)**
Идентификатор типа (Тип РЭС)	Название радиослужбы (*символьный*); Наименование типа РЭС (*символьный*)
Идентификатор РЭС (РЭС)	Наименование РЭС (*символьный*); Шифр РЭС (*символьный*)
Идентификатор решения (Решение ГКРЧ)	Регистрационный номер (*символьный*); Дата (*дата*)
Идентификатор аппарата (Космический аппарат)	Наименование (*символьный*); Описание орбиты (*символьный*); Тип орбиты (*символьный*)

Детерминант (таблица)	Набор зависимых атрибутов (*домен*)
Идентификатор РЧЗ (РЧЗ)	Исходящий номер (*символьный*); Дата отправки (*дата*); Цель представления (*символьный*); Этап состояния РЭС (*символьный*); Место установки РЭС (*символьный*); Функциональное назначение РЭС (*символьный*); Пользователи РЭС (*символьный*); Необходимость международно-правовой защиты (*булев*); Шифр системы РЭС (*символьный*); Меры по повышению ЭМС (*символьный*); Структурная схема РЭС (*BLOB*)
Идентификатор полосы (Полоса частот РЭС)	Номер полосы частот (*целочисленный*); Минимальная частота (*численный*); Максимальная частота (*численный*); Прием/передача (*булев*)
Идентификатор режима (Режим работы РЭС)	Номер режима (*целочисленный*); Номера полос частот (*символьный*); Номер элементарного РЭС 1 (*численный*); Номер антенны 1 (*символьный*); Номер элементарного РЭС 2 (*символьный*); Номер антенны 2 (*символьный*)
Идентификатор передатчика (Передатчик)	Номер передатчика (*целочисленный*); Рабочие частоты (*символьный*); Тип выходного прибора (*символьный*); Способ перестройки частоты (*символьный*); Нестабильность частоты (*численный*); Уровень побочных излучений до 3 гармоники (*численный*); Уровень побочных излучений выше 3 (*численный*); Уровень шумовых излучений (*численный*)
Идентификатор передатчика; Идентификатор класса излучения (Параметры передатчика)	Вид мощности (*символьный*); Тип модуляции (*символьный*); Ширина полосы излучения на уровне –3 дБ (*численный*); Ширина полосы излучения на уровне –30 дБ (*численный*); Ширина полосы излучения на доп. уровне (*численный*); Минимальная мощность (*численный*); Максимальная мощность (*численный*); Спектральная плотность (*численный*)
Идентификатор приемника (Приемник)	Номер приемника (*целочисленный*); Рабочие частоты (*символьный*); Тип приемника (*символьный*); Нестабильность частоты (*численный*); Избирательность по соседнему каналу (*численный*); Избирательность по зеркальному каналу (*численный*); Избирательность по блокированию (*численный*); Избирательность по интермодуляции (*численный*); Шумовая температура (*численный*)
Идентификатор приемника; Идентификатор класса излучения (Параметры приемника)	Пороговая чувствительность (*численный*); Реальная чувствительность (*численный*); Защитное отношение (*численный*); Ширина усилителя высокой частоты (УВЧ) на –3 дБ (*численный*); Ширина УВЧ на –30 дБ (*численный*); Ширина УВЧ на доп. уровне (*численный*)
Идентификатор приемника; Идентификатор класса излучения; Идентификатор гетеродина (Гетеродин)	Вид настройки (*символьный*); Промежуточная частота (*численный*); Ширина усилителя промежуточной частоты (УПЧ) на –3 дБ (*численный*); Ширина УПЧ на –30 дБ (*численный*); Ширина УПЧ на дополнительном уровне (*численный*)

Детерминант (таблица)	Набор зависимых атрибутов (*домен*)
Идентификатор антенны (Антенна)	Номер антенны (*символьный*); Назначение антенны (*символьный*); Тип антенны (*символьный*); Длина антенны (*численный*); Диаметр антенны (*численный*); Высота антенны (*численный*); Количество витков (*численный*); Угловая точность наведения (*численный*); Зона обслуживания (*символьный*)
Идентификатор антенны; Идентификатор луча (ДНА)	Наименование луча (*символьный*); Положение луча (*символьный*); Рабочая частота (*численный*); Коэффициент усиления (*численный*); Ширина ДНА в горизонтальной плоскости (*численный*); Ширина ДНА в вертикальной плоскости (*численный*)
Идентификатор антенны; Идентификатор луча; Идентификатор сектора (Сектор антенны)	Нижняя граница сектора (*численный*); Верхняя граница сектора (*численный*); Уровень боковых лепестков (*численный*)
Идентификатор антенны; Идентификатор АТФ (АФТ)	Тип фидера (*символьный*); Тип поляризации (*символьный*); Критическая частота (*численный*); Волновое сопротивление (*численный*); Затухание (*численный*); Прием/передача (*булев*)
Идентификатор станции; Идентификатор РЭС (Станция)	Заводской номер (*символьный*); Номер станции в сети (*символьный*); Адрес установки станции (*символьный*); Широта (*символьный*); Долгота (*символьный*)
Идентификатор станции; Идентификатор антенны станции (Антенна станции)	Высота подвеса от Земли (*численный*); Высота подвеса от моря (*численный*); Угол места (*численный*); Азимут (*численный*)
Идентификатор станции; Идентификатор частоты станции (Частоты станции)	Нижняя частота (*численный*); Верхняя частота (*численный*); Прием/передача (*булев*)
Идентификатор организации (Организация)	Наименование (*символьный*); Адрес (*символьный*); Номер телефона (*символьный*); Адрес электронной почты (*символьный*)
Идентификатор сотрудника (Сотрудник)	Должность (*символьный*); Фамилия инициалы (*символьный*)

В результате проведенного анализа выделены объекты учета БД и распределены между ними характеристики, учитываемые в РЧЗ. На основе результатов анализа разработана схема логической структуры БД, предусматривающая взаимосвязь выделенных объектов учета (рис. 2, см. ниже). Схема выполнена в виде модели, основанной на ключах, т. е. в ней представлены только те атрибуты БД, которые выступают в роли первичных или внешних ключей.

Согласованность данных БД обеспечивается за счет использования словарей и ограничений предметной области [2]. Словарь представляет со-

бой таблицу БД, состоящую только из двух атрибутов: первичного ключа и непосредственно значения словаря. Использование словарей позволяет исключить ошибки при вводе данных в БД.

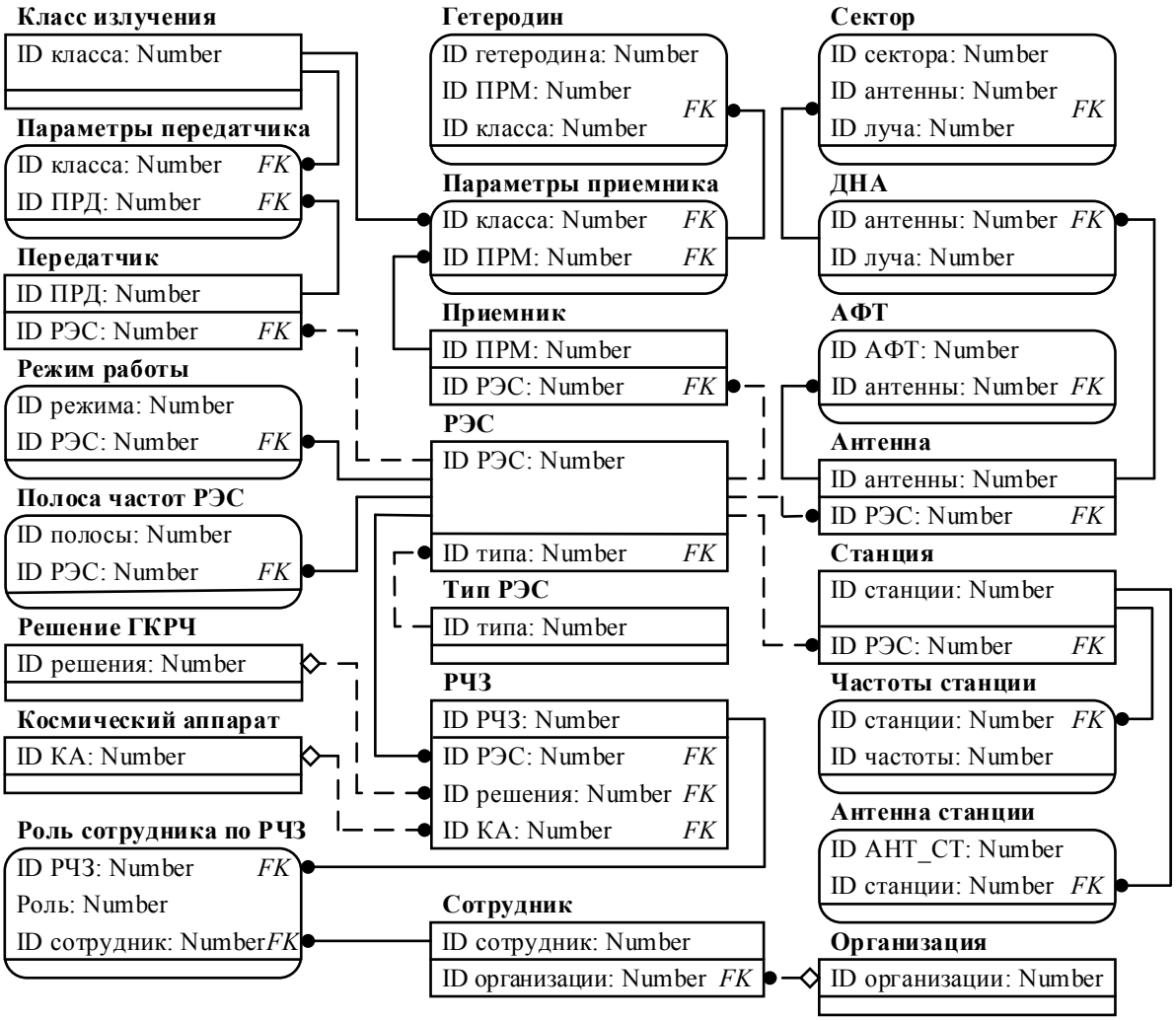


Рис. 2. Схема логической структуры БД

Ограничения предметной области представляют собой формализованные правила, определяющие набор допустимых значений для некоторого атрибута таблицы БД, исходя из специфики предметной области. Такие ограничения могут быть реализованы в виде триггеров БД (хранимых процедур, срабатывающих на определенные события БД) или предложения CHECK конструкции CREATE TABLE.

На основе представленной модели разработана физическая модель БД, которая доведена до практической реализации в СУБД Microsoft SQL Server 2008, которая позволяет решить задачу учета и согласованного хранения данных, представленных в РЧЗ. В качестве направлений дальнейших исследований в данном направлении можно отметить задачи по автоматиза-

ции ввода исходных данных РЧЗ, проверки их полноты и корректности, а также задачи импорта данных из БД в программный комплекс ATDI для проведения расчетов ЭМС РЭС.

Список используемых источников

1. Lapko A., Egorov A. Developing the automated system of radio frequency spectrum management // Modern informatization problems in the technological and telecommunication systems analysis and synthesis / Editor in Chief Dr. Sci., Prof. O. Ja. Kravets. Yelm, WA, USA: Science Book Publishing House, 2017. PP. 245–368.

2. Лапко А. Н. Системы баз данных: учебно-методическое пособие. Орел : Академия ФСО России, 2017. 255 с.

УДК 004.7:004.422.8

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ПРИОБРЕТЕНИЯ ЗНАНИЙ О ВЛИЯНИИ АКТИВНОСТИ ИНФРАСТРУКТУРЫ НА КАЧЕСТВО ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ АГЕНТОВ

А. А. Лебедева, Л. К. Птицына

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

Обоснована актуальность создания системы приобретения знаний о влиянии активности инфраструктуры на качество функционирования интеллектуальных информационных агентов. Выделен типовой профиль их качества. Определены функциональные задачи рассматриваемого математического обеспечения. Формализовано проявление активности инфраструктуры в критических ситуациях функционирования агентов. Представлены классы функциональных моделей интеллектуальных информационных агентов и методы их анализа. Раскрыта система аналитических соотношений для определения и вычисления значений выбранных показателей качества в активной инфраструктуре.

информационный интеллектуальный агент, объектно-ориентированная модель, активная инфокоммуникационная среда.

Усложнение современных информационных инфраструктур, требования к обработке больших информационных потоков с заявленным уровнем качества, обеспечение защиты информации от влияния различных инфор-

мационных угроз обуславливают необходимость совершенствования подсистемы управления функциональными процессами.

Одно из перспективных направлений интеллектуализации функциональных процессов базируется на введении в информационную инфраструктуру интеллектуальных информационных агентов. Корректное функционирование агента поддерживается системой планирования действий, отвечающей за составление планов действий агентов в соответствии с поставленными целями, а также модельно-аналитическим интеллектом, с помощью которого агент способен самостоятельно оценить эффективность спланированных действий и спрогнозировать их успешное достижение.

Очевидно, что влияние активной инфокоммуникационной среды, в которой функционирует агент, способно повлиять на качество его работы и вызвать угрозу невыполнения, либо несвоевременного выполнения решаемой задачи. Накопление знаний о влиянии активной инфраструктуры на характеристики функционирования агента позволит проанализировать возможные тенденции и спрогнозировать степень влияния инфраструктуры на качество его работы. В таком случае при прогнозе потенциального сбоя в работе агента и срыва временного регламента становится возможным своевременное устранение вероятной проблемной ситуации до наступления нежелательного последствия.

Указанное обстоятельство актуализирует необходимость приобретения и сохранения знаний о влиянии активности инфраструктуры на качество работы интеллектуальных информационных агентов. Для разрешения представленной проблемной ситуации предлагается расширенное математическое обеспечение модельно-аналитического интеллекта интеллектуального информационного агента.

В качестве основы для формирования математического обеспечения выбран объектно-ориентированный подход. Из обширного множества методических решений агентных технологий формируется опорный базис для разработки системы приобретения знаний. Указанный базис включает следующие составляющие:

– методика формирования модельно-аналитического интеллекта информационных агентов, позволяющего обеспечить гарантии качества их функционирования [1];

– методика формирования модельно-аналитического интеллекта информационных агентов с динамической синхронизацией их действий [2];

– методика формирования модельно-аналитического интеллекта информационных агентов, выполняющих действия в условиях активной инфокоммуникационной среды [3].

В расширенном математическом обеспечении модель системы приобретения знаний о влиянии активности инфраструктуры на качество функ-

ционирования интеллектуальных информационных агентов представляется кортежем:

$$\mathbf{M} = \langle \mathbf{G}, \mathbf{DB}, \mathbf{C} \rangle,$$

где **G** – метод достижения цели интеллектуальным информационным агентом в активной инфокоммуникационной среде; **DB** – база знаний, в которой сохраняются изменения состояний среды и динамических характеристик; **C** – метод анализа зависимостей динамических характеристик информационных агентов от состояний среды для прогнозирования критических ситуаций.

Согласно [3] достижение цели интеллектуальным информационным агентов в активной инфокоммуникационной **G** среде описывается кортежем:

$$\mathbf{G} = \langle f_s(k_s), f_f(k_f), \mathbf{P}_{Ia}, \mathbf{C}, \mathbf{P}_I, \mathbf{F}_A, \mathbf{F}_B, \mathbf{F}_N, \mathbf{F}_0 \rangle,$$

где $f_s(k_s)$ – вектор плотностей распределения вероятностей дискретного времени k_s успешного выполнения запросов интеллектуального агента к информационным источникам. Вектор $f_s(k_s)$ составляют плотности распределения вероятностей дискретного времени k^s_{0ia} успешного запроса к i-му (i = 1, 2, …, I) информационному источнику в активной среде: $f_{1sa}(k^s_{01a})$, ..., $f_{Isa}(k^s_{0Ia})$, а также плотности распределения вероятностей дискретного времени $k^s_{0iн}$ успешного запроса к i-му информационному источнику в пассивной среде: $f_{1sн}(k^s_{01н})$, …,$f_{1sн}(k^s_{01н})$; $f_f(k_f)$ – вектор плотностей распределения вероятностей дискретного времени k_f неуспешного выполнения запросов интеллектуального агента к информационному источнику. Вектор $f_f(k_f)$ составляют плотности распределения вероятностей дискретного времени k^f_{0ia} выполнения неуспешного запроса к i-му (i = 1, 2, …, I) информационному источнику в активной среде: $f_{1fa}(k^f_{01a})$, …, $f_{Ifa}(k^f_{0Ia})$, а также плотности распределения вероятностей дискретного времени $k^f_{0iн}$ неуспешного запроса к i-му информационному источнику в пассивной де: $f_{1fн}(k^f_{01н})$, …, $f_{Ifн}(k^f_{0Iн})$; $\mathbf{P}_{Ia}$ – вектор вероятностей влияния активной среды на достижение целей агентом при запросе к источникам, $\mathbf{P}_{Ia} = \langle p_{isa}, p_{ifa} \rangle$, где p_{isa} – вероятность влияния активной инфокоммуника-ционной среды на достижение целей агентом при успешном запросе к i-му источнику, p_{ifa} – при неуспешном запросе к i-му источнику (i = 1,2, …, I); **C** – матрица инцидентности, описывающая вырожденный граф, узловые вершины которого соответствуют запуску, завершению, объединению или распараллеливанию действий информационного агента; $\mathbf{P}_I$ – матрица вероятностей переходов между неузловыми вершинами, соответствующих выполняемым действиям информационного агента; $\mathbf{F}_A$ – вектор функций объединения по-

следовательно выполняемых действий информационного агента; $\mathbf{F}_B$ – вектор функций разветвления последовательных действий, характеризуемых вероятностями успешного выполнения запроса $p_1, p_2, ..., p_I$ к i-му информационному источнику (i=1, 2, …, I). Неуспешное выполнение запроса к i-му источнику описывается вероятностями: $(1 - p_1)$, $(1 - p_2)$, ..., $(1 - p_I)$; $\mathbf{F}_N$ – вектор функций объединения распараллеленных действий агента; $\mathbf{F}_0$ – вектор функций распараллеливания действий агента.

Выделяются следующие типовые случаи достижимости целей интеллектуальными информационными агентами при априорно неопределенном механизме синхронизации подпроцессов параллельного процесса опроса:

– I реплицированных информационных источников;

– I нереплицированных информационных источников.

В первом случае вероятности $f_s(k_s)$ и $f_f(k_f)$ определяются с помощью следующих соотношений:

$$f_f(k_f)=(1-p_1)(1-\mathrm{p}_2)\ldots(1-p_I)\times$$

$$\left[\begin{array}{c} f_1^f\left(k_{01}^f=k_f\right)\sum_{k_{02}^f\le k_f}\ldots\sum_{k_I^f\le k_f}f_2^f\left(k_{02}^f\right)\ldots f_I^f\left(k_I^f\right)+f_2^f\left(k_{02}^f=k_f\right)\times \\ \times\sum_{k_{01}^f<k_f}\sum_{k_{03}^f\le k_f}\ldots\sum_{k_I^f\le k_f}f_1^f\left(k_{01}^f\right)f_3^f\left(k_{03}^f\right)\ldots f_I^f\left(k_I^f\right)+\ldots+f_I^f\left(k_I^f=k_f\right)\times \\ \times\sum_{k_{01}^f<k_f}\sum_{k_{02}^f<k_f}\ldots\sum_{k_{I\text{-}1}^f<k_f}f_1^f\left(k_{01}^f\right)f_2^f\left(k_{02}^f\right)\ldots f_{I\text{-}1}^f\left(k_{I\text{-}1}^f\right) \end{array}\right] \quad (1)$$

$$k_f=\max\{\min(k_{01}^f),\min(k_{02}^f),\min(k_I^f)\},\ldots,\max\{\max(k_{01}^f),\max(k_{02}^f),\max(k_I^f)\} \quad (2)$$

$$f_s(k_s)=p_Ip_2\ldots p_I\times$$

$$\times\left[\begin{array}{c} f_1^s(k_{01}^s=k_s)\left(1-\sum_{k_{02}^f\le k_s}f_2^s(k_{02}^s)\right)\ldots\left(1-\sum_{k_I^s\le k_s}f_I^s(k_I^s)\right)+ \\ +f_2^s(k_{02}^s=k_s)\left(1-\sum_{\mathrm{k}_{01}^s<k_s}f_1^s(k_{01}^s)\right)\left(1-\sum_{k_{03}^s\le k_s}f_3^s(k_{03}^s)\right)\ldots\left(1-\sum_{k_I^s\le k_s}f_I^s(k_I^s)\right)+ \\ +f_I^s(k_I^s=k_s)\left(1-\sum_{k_1^s<k_s}f_1^s(k_{01}^s)\right)\left(1-\sum_{k_{02}^s<k_s}f_2^s(k_{02}^s)\right)\ldots\left(1-\sum_{k_{I\text{-}1}^s<k_s}f_{I\text{-}1}^s\left(k_{I\text{-}1}^s\right)\right) \end{array}\right] \quad (3)$$

$$k_s=\min\{\min(k_{01}^s),\min(k_{02}^s),\ldots,\min(k_I^s)\},\ldots,\min\{\max(k_{01}^s),\max(k_{02}^s),\max(k_I^s)\} \quad (4)$$

Во втором случае при параллельном опросе I нереплицированных источников выражения для анализа вероятностей $f_s(k_s)$ и $f_f(k_f)$:

$$f_s(k_s)=p_1p_2\ldots p_I\times$$

$$\left[\begin{array}{c} f_1^s(k_{01}^s=k_s)\sum_{k_{02}^s\le k_s}\ldots\sum_{k_I^s\le k_s}f_2^s(k_{02}^s)\ldots f_I^s(k_I^s)+f_2^s(k_{02}^s=k_s)\times \\ \times\sum_{k_{01}^s<k_s}\sum_{k_{03}^s\le k_s}\ldots\sum_{k_I^s\le k_s}f_1^s(k_{01}^s)f_3^s(k_{03}^s)\ldots f_I^s(k_I^s)+\ldots+f_I^s(k_I^s=k_s)\times \\ \sum_{\mathrm{k}_{01}^s<k_s}\ldots\sum_{k_{I\text{-}1}^s<k_s}f_1^s(k_{01}^s)f_2^s(k_{02}^s)\ldots f_{I\text{-}1}^s\left(k_{I\text{-}1}^s\right) \end{array}\right] \quad (5)$$

$$k_s=\max\{\min(k_{01}^s),\min(k_{02}^s),\ldots,\min(k_I^s)\},\ldots,\max\{\max(k_{01}^s),\max(k_{02}^s),\max(k_I^s)\} \quad (6)$$

$$f_f(k_f)=(1-p_1)(1-p_2)\ldots(1-p_I)\times$$

$$\times\begin{bmatrix} f_1^f(k_{01}^f=k_f)\left(1-\sum_{k_{02}^f\le k_f} f_2^f(k_{02}^f)\right)\ldots\left(1-\sum_{k_I^f\le k_f} f_I^f(k_I^f)\right)+ \\ +f_2^f(k_{02}^f=k_f)\left(1-\sum_{k_{01}^f<k_f} f_1^f(k_{01}^f)\right)\left(1-\sum_{k_{03}^f\le k_f} f_3^f(k_{03}^f)\right)..\left(1-\sum_{k_I^f\le k_f} f_I^f(k_I^f)\right)+..+ \\ +f_I^f(k_I^f=k_f)\left(1-\sum_{k_{01}^f<k_f} f_1^f(k_{01}^f)\right)\left(1-\sum_{k_{02}^f<k_f} f_2^f(k_{02}^f)\right)\ldots\left(1-\sum_{k_{I-1}^f<k_f} f_{I-1}^f\left(k_{I-1}^f\right)\right)\end{bmatrix} \quad (7)$$

$$k_f=\min\{\min(k_{01}^f),\min(k_{02}^f),\min(k_I^f)\},\ldots,\min\{\max(k_{01}^f),\max(k_{02}^f),\max(k_I^f)\} \quad (8)$$

На основе соотношений (1)–(8) оцениваются вероятности успешного и неуспешного решения задачи агентом за ограниченное время $N_{\max}$, а также математические ожидания времени достижения агентом цели:

$$P(k_s\le N_{\max})=\sum_{k_s\le N_{\max}} f_s(k_s);\ \mathrm{MO}[k_s]=\sum_{k_s} k_s f_s(k_s),$$

$$P(k_f\le N_{\max})=\sum_{k_f\le N_{\max}} f_f(k_f);\ \mathrm{MO}[k_f]=\sum_{k_f} k_f f_f(k_f).$$

Научная новизна результатов исследований заключается в расширении модельного пространства агентных технологий и предоставлении опорной базы для создания системы приобретения знаний о качестве функционирования интеллектуальных информационных агентов в активных средах.

Практическая значимость обусловлена возможностью анализа влияния состояний инфокоммуникационной среды на достижимость запланированных целей и, соответственно, прогнозирования вероятных изменений качества функционирования интеллектуальных информационных агентов.

Список используемых источников

1. Птицына Л. К., Лебедева А. А. Аналитические компоненты информационной технологии формирования динамических характеристик запросов интеллектуальных агентов с подтверждением // Наукоемкие технологии в космических исследованиях Земли. 2015. N 1. С. 32–36.

2. Птицына Л. К., Лебедева А. А. Разработка системно-аналитического ядра информационных интеллектуальных агентов с динамической синхронизацией их действий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. науч. ст. 2014. С. 505–509.

3. Лебедева А. А., Птицына Л. К. Методика формирования динамических характеристик интеллектуальных информационных агентов в условиях активной инфокоммуникационной среды // Информация и Космос. 2017. С. 105–111.

УДК 681.3.81

ПОДСИСТЕМА КОНТРОЛЯ ОБЪЕМА ПОМЕЩЕНИЙ НА ОСНОВЕ ТЕХНОЛОГИИ WISEE

А. И. Ликарь, С. К. Морозов

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

Наиболее часто в качестве объёмных извещателей для помещений закрытого типа используются пассивные инфакрасные извещатели благодаря сочетанию их относительно низкой стоимости и, вместе с тем, хороших функциональных характеристик. Однако, данным извещателям присущ ряд известных характерных недостатков, вытекающих из принципов работы.

Для компенсации этих недостатков используются извещатели комбинированного типа, включающих в себя два независимых метода детекции: пассивный ИК и микроволновый. Но стоимость извещателей комбинированного типа намного больше, чем пассивных ИК, что затрудняет их массовое применение.

В качестве решения данной проблемы предлагается использование штатных пассивных ИК извещателей в сочетании подсистемой обнаружения нарушителя на основе технологии WiSee.

объемный детектор, WiSee.

Наиболее часто в качестве объёмных извещателей для помещений закрытого типа используются пассивные инфакрасные (ИК) извещатели благодаря сочетанию их относительно низкой стоимости и, вместе с тем, хороших функциональных характеристик [1]. Однако, данным ИК-извещателям присущ ряд известных характерных недостатков, вытекающих из принципов работы [2, 3]:

1. Для обнаружения движения нарушитель должен явно отличаться по температуре от окружающих предметов. При температуре окружающей среды близкой к средней температуре человеческого тела к (36,6ºС) объект обнаружения практически сливается с фоновой обстановкой.

2. ИК-извещатель не различает малые и медленные возмущения на уровне фона (использование теплоизолирующей одежды при должной пластике движений).

3. Проблемы, связанные с маскированием оптической системы ИК-извещателя (блокируется любым предметом комнатной температуры, выполняющим функцию экрана, например, листом картона, непрозрачной плёнкой лакокрасочного материала и т. п.).

Для компенсации этих недостатков используются извещатели комбинированного типа, включающих в себя два независимых метода детекции: пассивный ИК и микроволновый.

Пассивная часть извещателя анализирует разницу температур в ИК диапазоне, а микроволновая реагирует на разницу частот переданного и отраженного сигналов. Использование двух принципов обнаружения значительно снижает число ложных тревог, поскольку влияние вызывающих их факторов практически исключается.

Существенно большая стоимость извещателей комбинированного типа затрудняет их массовое применение.

В качестве решения данной проблемы предлагается использование штатных пассивных ИК извещателей в сочетании подсистемой обнаружения нарушителя на основе технологии WiSee.

WiSee представляет собой технологию распознавания жестов, которая использует беспроводные сигналы (в данном случае Wi-Fi) для сканирования помещения и выявления кинематических особенностей движения человека [4, 5]. Поскольку микроволновые излучатели не требуют определённого угла обзора, а радиоволны могут проходить даже сквозь стены, не говоря о тонких перегородка, использование нескольких беспроводных источников способно покрыть контролируемую зону помещений больших размеров.

Так как эта технология не относится к системам передачи, требующих линии прямой видимости (между передатчиком и приёмником сигналов не должно быть никаких физических препятствий), и может проходить сквозь стены, для покрытия больших территорий достаточно единичных точек доступа WiFi. Работа WiSee основывается на определении и анализе едва заметных доплеровских смещений и искажений, обусловленных многолучевым распространением, которые происходят с этими беспроводными сигналами от движений человека в окружающей среде.

WiSee использует принцип эффекта Допплера, который заключается в разнице между частотами принятого и излучённого сигналов, пропорциональной скорости взаимного сближения (удаления) источника и приёмника. Если рассматривать многократные отражения излучений от человеческого тела как источник, то движение человека приводит к доплеровским сдвигам. Так, перемещение руки от приёмника приведёт к отрицательным доплеровским смещениям, а перемещение к приёмнику, соответственно, к положительным смещениям. Движения человеческого тела изменяют фазы и амплитуды, принимаемых сигналов.

Опубликованы доказательства работоспособности технологии WiSee, в частности, её реализации с помощью программного обеспечения GNURadio в сочетании с использованием оборудования USRP-N210. Оценка функционирования WiSee проводилась на пяти людях, как в офис-

ном помещении, так и в трёхкомнатной квартире. Прорабатывались несколько сценариев: передвижения в пределах линии прямой видимости, вне линии прямой видимости, а также движения за стеной от приёмника. В общей сложности было выполнено и зафиксировано 900 жестов разных людей в разных точках, предусмотренных сценариями.

Из опубликованных результатов проведённого тестирования технологии WiSee можно сделать следующие выводы о работе системы:

– WiSee может распознавать движения любых частей тела со средней точностью до 94 % при расчётной погрешности около 11,1 %;

– используя четыре антенны для приёма электромагнитных волн и одну антенну для их распространения и разместив устройство, например, в гостиной, можно покрыть всю площадь квартиры. Но способность к точному обнаружению всех людей, находящихся в квартире, и их жестов, падает до 60 %. Эту ситуацию исправляет добавление ещё одного источника WiFi в квартире. Таким образом, если использовать WiSee с поддержкой точки доступа WiFi как приёмник и несколько мобильных устройств как источники в разных частях комнаты, можно обеспечить распознавание телодвижений во всех частях даже больших помещений;

– среднее количество ложных срабатываний системы WiSee за отчётный период (сутки) составляет 2,63 неправильных распознаваний жестов в час при условии создания преамбулы путём двух повторений разных движений одним человеком. Данное значение уменьшается до 0,07 ложных срабатываний в час при условии создания преамбулы с помощью четырёх повторений движений;

– используя 5 антенн для приёма сигналов и одну как источник WiSee может успешно распознавать мельчайшие жесты одного человека, который находиться в окружении трёх активно жестикулирующих людей. Однако, точность идентификации движений снижается, если число интерферирующих людей возрастёт. С учетом фиксированного количества передающих и принимающих сигнал антенн, точность уменьшается с увеличением числа людей в сканируемой зоне.

Для обеспечения применения данной WiSee технологии в целях контроля объема помещений не требуется детального анализа характера перемещений нарушителя, что позволит свести программный анализ скорости изменения фазы и амплитуды принимаемых отражённых сигналов к сопоставлению с пороговыми значениями.

Предлагаемая дополнительная подсистема контроля объема помещений на основе технологии WiSee потенциально может быть реализована на основе уже имеющихся WiFi точек доступа существующей в организации информационной сети.

Такая дополнительная подсистема контроля объема помещений может быть хорошим дополнением к уже установленным пассивным ИК-извеща-

телям охранных систем, компенсируя их недостатки без значительных затрат, как это может быть в случае замены пассивных ИК-извещателей на извещатели комбинированного типа.

Список используемых источников

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступам. М. : Горячая линия – Телеком, 2010. 272 с.

2. Стасенко Л. А. Чем умней система, тем изобретательнее взломщик [Электронный ресурс]. URL: http://www.secuteck.ru/articles2/sys_ogr_dost/-rfid_technology

3. Пассивные ИК-извещатели движения [Электронный ресурс]. URL: http://os-info.ru/oxrannaya-signalizaciya/passivnye-ik-izveshhateli.html

4. Adib F. See Through Walls with Wi-Fi / Fadel Adib, Dina Katabi [Электронный ресурс]. URL: https://people.csail.mit.edu/fadel/papers/wivi-paper.pdf

5. Prof Kamal K Vyas. Pareek A., Dr S Tiwari. Gesture Recognition and Control Part 3 – WiFi Oriented Gesture Control & its application // International Journal on Recent and Innovation Trends in Computing and Communication, Sep. 2013, Volume: 1, Issue: 9, pp. 682–685.

Статья представлена заведующим кафедры, кандидатом технических наук, доцентом С. В. Хорошенко.

УДК 004.9

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ОБЛАЧНОГО СЕРВИСА БИТРИКС24 ДЛЯ СОВМЕСТНОЙ РАБОТЫ КОМАНДЫ ВЕБ-РАЗРАБОТЧИКОВ

В. В. Ловина, А. А. Шиян

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

Облачный сервис Битрикс24, разработанный компанией 1С-Битрикс, максимально актуален для компаний, сотрудники которой находятся удаленно друг от друга и не привязаны к определенному местоположению. Для совместной работы сотрудники компании получают доступ к рабочим инструментам сервиса, что позволяет значительно повысить эффективность их работы.

облачный сервис, Битрикс24, веб-разработчики.

Битрикс24 – это социальный интранет, социальная сеть сотрудников компании, разработанная компанией 1С-Битрикс. Используя данный про-

граммный продукт, сотрудники получают возможность хранить большие объемы рабочих данных в едином информационном пространстве, а также получать доступ к ним практически в любое удобное время.

Существует два варианта работы с продуктом Битрикс24 (рис. 1):

Рис. 1. Варианты использования программного продукта Битрикс24

– коробочная версия (программный продукт необходимо установить на сервер или хостинг компании для индивидуальной настройки бизнес-логики, интерфейса, интеграции с другими продуктами 1С-Битрикс);

– облачный сервис (пользователи не должны устанавливать и настраивать дополнительные компоненты, перейти к работе в сервисе можно сразу после регистрации на портале).

Используя облачный сервис, команда Web-разработчиков может значительно снизить затраты компании на программное обеспечение – двенадцать бизнес-пользователей могут бесплатно работать в Битрикс24 неограниченный период. Численные требования бесплатной версии продукта полностью удовлетворяют рабочим ресурсам компании (рис. 2).

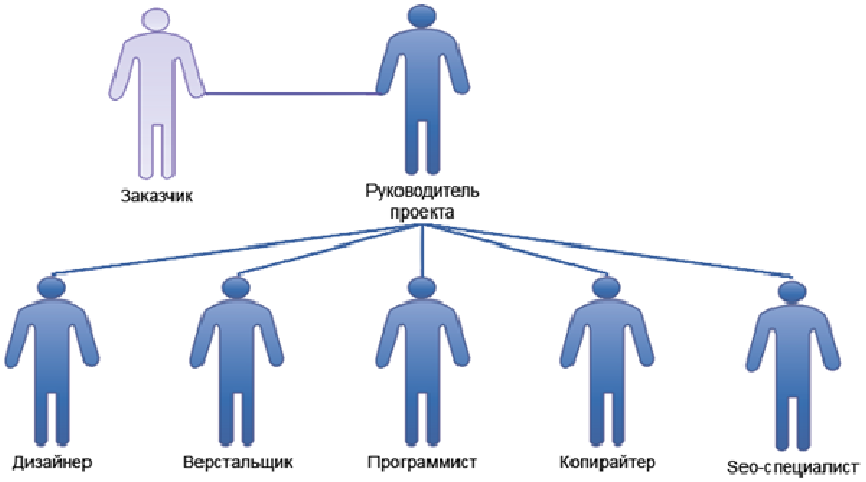


Рис. 2. Пользователи облачного сервиса

В представленной схеме все сотрудники и заказчик – бизнес-пользователи.

Облачный сервис Битрикс24 целесообразно использовать компаниям, которые не имеют своего офиса или другого офисного пространства, сотрудники не привязаны к физическому местоположению работы и могут находится удаленно друг от друга. Все имеющиеся информационные ресурсы компании размещены в облаке, а сотрудники могут работать с необходимыми данными, файлами и программами независимо от аппаратных характеристик используемых ими устройств и своего местонахождения.

Для организации работы компании и упрощения рабочих процессов Битрикс24 содержит в себе множество рабочих инструментов: рабочий календарь, задачи и проекты, облачное хранилище и электронный документооборот, отчеты о работе и т. д.

Наиболее полезный инструмент из выше перечисленных – это «Задачи и проекты». С помощью данного раздела руководитель компании или конкретного проекта имеет возможность отслеживать ход выполнения целей и задач, поставленных перед подчиненными, а также их временные затраты. Для простых, часто повторяющихся и единообразных задач есть возможность создать шаблон. Сложные задачи следует разделить на этапы и к каждому этапу добавить чек-лист. Если некоторые сотрудники задействованы в нескольких проектах одновременно, можно разделить их на рабочие группы, где будет собрана вся информация о проекте.

Кроме того, можно создать рабочие группы для сотрудников, которые работают над одним проектом, а также распределить права доступа между ее участниками. Это особенно эффективно в том случае, если сотрудник задействован сразу в нескольких проектах одновременно. В такой рабочей группе будет собрана вся информация о проекте.

В рабочем календаре можно отображать не только запланированные события – он синхронизирован с поставленными целями в инструменте «Задачи и проекты». Таким образом, личные календари сотрудников можно объединить с календарями рабочих групп проектов, в которых сотрудники задействованы. В свою очередь руководитель может просматривать календари своих подчиненных и график их занятости, выбирать оптимальные дату и время встреч или собраний для всей рабочей группы и добавлять событие в их календари. Сотрудники компании, получив уведомление о встрече, имеют возможность самостоятельно добавить в облачное хранилище отчеты, документы и прочие материалы, которые могут использоваться на встрече.

Облачное хранилище Битрикс24.Диск может использовать любой сотрудник компании через мобильное приложение или с любого доступного ему компьютера с доступом в Интернет. Это защищенное пространство, в котором сотрудники могут хранить не только свои рабочие файлы,

но и подключать к работе над ними своих коллег или клиентов, указав права доступа к документам. Все загруженные файлы синхронизируются с рабочим компьютером, пока он подключен к Интернету, поэтому даже в случае, когда нет доступа к облачному хранилищу, сотрудник может продолжить работу над файлами. Когда выход в Интернет будет восстановлен – все правки будут подгружены к Битрикс24.Диск.

Кроме того, непосредственно в Битрикс24.Диск можно создавать документы, таблицы и презентации, с которыми в дальнейшем будут работать сотрудники, это возможно благодаря интеграции с Microsoft Office Online и Google Docs. Сотрудники могут совместно редактировать файлы, блокировать их во время правок, чтобы избежать внесения одновременных исправлений, при этом вся история изменений будет сохраняться. Таким образом, компания может существенно сэкономить на покупке офисного программного обеспечения. После загрузки файлов в облачное хранилище, Битрикс24 индексирует их, что позволяет осуществлять в дальнейшем быстрый и максимально точный поиск документов.

Доступность ко всем рабочим инструментам Битрикс24 осуществляется не только непосредственно с рабочего места сотрудников компании, но и с их мобильных устройств. Это является существенным плюсом для компании, сотрудники которой находятся удаленно друг от друга.

Отдавая предпочтение облачному сервису Битрикс24, компании не нужно оплачивать дорогостоящую аренду помещений, а также приобретать, настраивать и обслуживать дорогостоящее программное и аппаратное обеспечение. Таким образом, компания существенно уменьшит свои внутренние расходы, что позволит не завышать стоимость на предлагаемые товары и услуги, расширить аудиторию потенциальных клиентов, а также выполнять все предусмотренные конкретные задачи или проекты в заданные сроки без сверхнормативных затрат [1].

Список используемых источников

1. Светлов Н. М., Светлова Г. Н. Информационные технологии управления проектами. М. : ЦОП ФГОУ ВПО РГАУ-МСХА им. К. А. Тимирязева, 2012. 148 с.

УДК 65.011.56, 654.024, 336.764

АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА БИРЖЕВЫХ ДАННЫХ ДЛЯ ОЦЕНКИ ЛОЯЛЬНОСТИ КЛИЕНТОВ ОПЕРАТОРОВ СВЯЗИ И КРЕДИТНЫХ ОРГАНИЗАЦИЙ

К. Е. Макаренков, А. В. Шестаков

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

Возможности мониторинга операторами связи обеспечения соглашений об уровне обслуживания определенных категорий потребителей можно существенно расширить посредством методов машинной обработки данных торговых бирж. Предлагаемые решения повысят бизнес привлекательность в NGOSS интеллектуальных средств анализа данных электронных торгов, совместимых с существующими программными продуктами BOSS, CRM и ERP-систем.

лояльность потребителя, машинная обработка данных.

Действующими правовыми нормативными документами государственного регулирования деятельности в области связи определено, что тарифы на услуги связи устанавливаются оператором связи самостоятельно, если иное не предусмотрено федеральным законом о связи и национальным законодательством о естественных монополиях. Однако, несмотря на определенную «свободу» оператора связи в вопросах формирования тарифных планов для различных групп потребителей услуг связи в условиях рыночных отношений необходимо обеспечить дифференцированный гарантированный уровень качества их предоставления, который закреплен в Соглашениях об уровне обслуживания (*Service Level Agreement*, SLA).

Поддержание требований Соглашения о SLA и мониторинг условий при сопровождении определенных групп пользователей, например, участников высокочастотного трейдинга, с высокими тарифами достаточно сложная техническая задача [1].

Одновременно с этим, наличие конкурентной среды обусловило необходимость варьирования оператором связи набора функций, которые входят в пакет, их объема и стоимости (тарифных планов) с учетом лояльности клиентов [2].

Сложилось объективное противоречие между стремлением операторов связи повысить прибыль за счет высокооплачиваемых услуг и организационно-технической сложностью решений по получению, сбору, обработке, анализу достоверных данных о потенциальных и реальных потребностях и потребителях таких услуг. Следует обратить внимание

и на определенный системный интерес к результатам системотехнического решения данной проблемы, например, со стороны кредитных организаций, по источнику объективных данных при формировании программ лояльности клиентов.

В настоящее время у операторов связи существует благоприятная бизнес среда: реализация концепции NGOSS (*Next Generation Operations Systems and Software*) в части подсистем «Стратегия, инфраструктура и продукт», «Основные виды деятельности» и «Управление организацией», внедрение и развитие программно-аппаратных и программных средств компонент BOSS (*Operation Support System*/*Business Support System*), CRM (*Customer Relationship Management*), ERP-систем (*Enterprise Resource Planning*). Если добавить, то обстоятельство, что большинство операторов связи обзавелось хотя бы простейшими техническими (программными) средствами для осуществления различных акций стимулирования клиентов (например, скидок), то становится очевидным, что на современном этапе востребована система, которая позволит, во-первых, гибко и своевременно формировать, и изменять эти стимулы, а во-вторых, прогнозировать их эффективность. В центре такой системы находится «программа лояльности» – набор маркетинговых мероприятий (таких, как скидки разного вида, бонусы, подарки и т. п.), направленные на удержание и привлечение постоянных клиентов [3].

Значительная часть современных информационных систем, реализующих программы лояльности, не имеет средств интеллектуального анализа и выработки управленческих решений. В связи с чем востребованность в методах автоматизированной обработки данных, оценки лояльности клиентов и в их практической реализации является весьма актуальной задачей.

Результаты проведенного анализа характеристик прототипов возможных к применению технологий фокусируются на:

автоматизированной маркетинговой CRM-системе по модели SaaS американской компании Salesforce.com, интегрированной с системой управления компании ExactTarget Inc. (США);

автоматизированной аналитической системе «Розница» компании ООО Микротест (Россия, Санкт-Петербург) для предприятий розничной торговли на платформе Cognos 8 Business Intelligence (BI).

В прототипах системы основные усилия направлены на создание средств анализа, визуализации данных, с помощью которых можно получить любую информацию в любом разрезе и в любом виде. Зачастую предоставленные пользователю возможности по формированию различных отчетов избыточны с учетом реализованных оригинальных методов и алгоритмов аналитической обработки данных. В ряде случаев пользователю непонятно, какую информацию получать, необходимы существенные за-

траты на получение «требуемых» данных из системы и соответственно – значительная стоимость.

Для решения указанной задачи целесообразно помимо обработки и анализа информации продаж и клиентских данных, так же провести сбор, обработку и анализ биржевых (рыночных) данных предоставляемых услуг, как представлено на рис. 1.

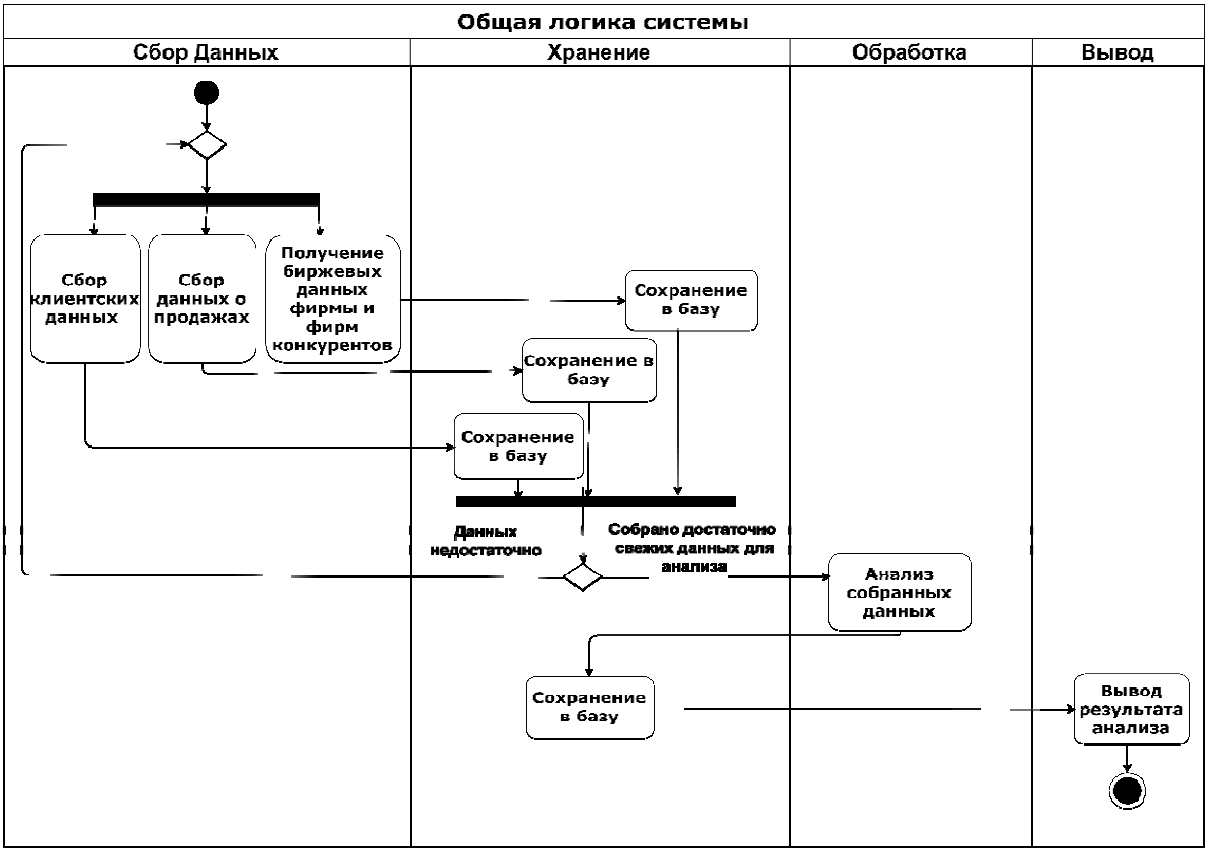


Рис. 1. Диаграмма деятельности (клиентов) в соответствии с прецедентом

Предлагаемый подход позволит повысить точность анализа, в связи увеличением числа анализируемых факторов. Помимо данных о продажах и персональных данных клиентов, необходимо получить рыночные показатели предоставляемых услуг, например, с помощью страниц API (*Application Programming Interface*), предоставляемых биржами.

Получение, сбор, обработка данных для систем поддержки принятия решений по программам лояльности клиентов состоит из четырех этапов:

первым этапом является сегментация клиентов. Необходимо получить ответ на вопрос: на какие группы клиентов будут сфокусированы применяемые программы лояльности, а также количественные показатели данных групп;

второй этап, на основе данных о продажах проводится оценка количества и скорости перехода клиентов из «пассивного» в активное состояние;

третьим этапом является оценка тренда предоставляемых услуг на основе данных продаж и данных предоставленных торговыми площадками. Коэффициент тренда активности пользователей рассчитывается на основе линии тренда, и является углом между осью абсцисс и линией тренда. Если величина значений угла находится в заданных диапазонах (как показано на рис. 2), то тенденция является положительной, в противном случае – отрицательной;

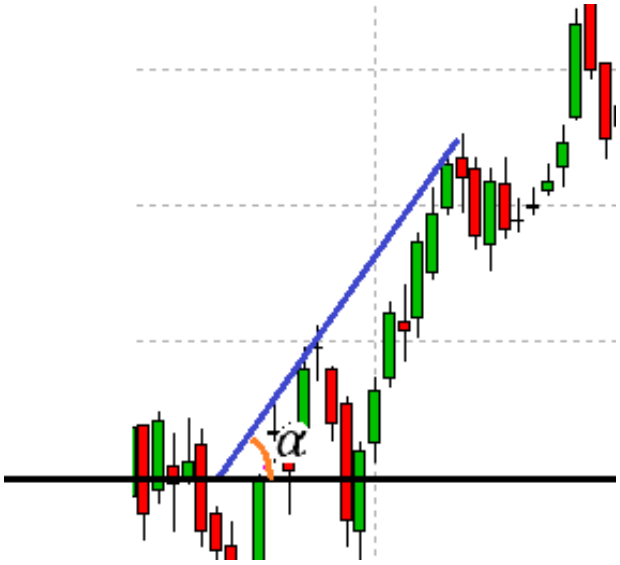


Рис. 2. Геометрическое представление коэффициента тренда активности пользователей

четвертым этапом является вычисление итогового коэффициента эффективности на основе коэффициентов перехода и коэффициентов тренда активности пользователей согласно последовательности процедур, представленных на рис. 3.

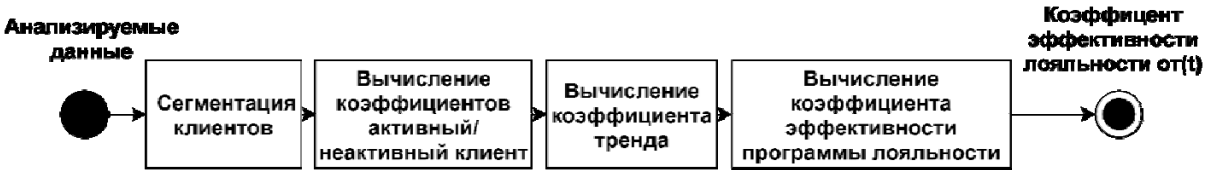


Рис. 3. Процедуры определения коэффициента эффективности программы лояльности

Так как большинство торговых площадок поддерживает протокол JSON-вызов удалённых процедур (*JavaScript Object Notation Remote Procedure Call*), то в «теле» ответа представляет необходимую информацию в формате JSON. В этих условиях наиболее корректным решением будет использование архитектуры REST (*Representational State Transfer*). Обращение к данным торговых площадок будет реализовано посредством предоставленного API, как представлено на рис. 4. Сервер предлагаемой системы, с учетом минимизации временных и ресурсных затрат, можно реализовать посредством технологий Java и Spring. Это обеспечит стабильность, так как разрабатывается для высоконагруженных условий использования.

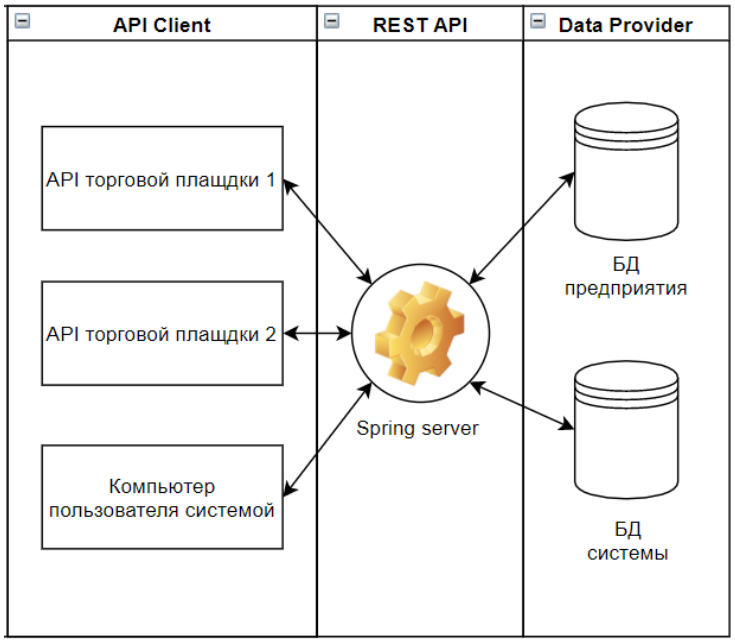


Рис. 4. Архитектура предлагаемой информационной системы (вариант)

Обращения к базам данных реализуется с применением библиотеки Hibernate для языка программирования Java, которая предназначена для решения задач объектно-реляционного отображения (ORM). В основу базы данных целесообразно принять PostgreSQL-решения.

Результаты анализа предварительных оценок предложенных решений, выполненных в соответствии с ГОСТ Р ИСО/МЭК 25010-2015 и ГОСТ Р ИСО/МЭК 25040-2014, показали на существенный прирост обобщенного показателя качества не только согласно модели качества программных изделий, но и модели качества при их использовании.

В текущей практической проработке находятся вопросы совместимости предложенных технических решений с изделиями PLM компании APPIUS, регистрации программы для ЭВМ и патентования результатов интеллектуальной деятельности.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. Абрамова Н. А. Как рассчитать экономическую эффективность скидки [Электронный ресурс] // Планово-экономический отдел: электрон. научн. журн. 2011. № 3. URL: http://www.profiz.ru/peo/3_2011/kak_rasshit_effek_skidki/ (дата обращения 22.01.2017).

3. Романова И. М., Троценко А. Е. Анализ программ лояльности операторов услуг сотовой связи на региональном рынке [Электронный ресурс] // Практический маркетинг: электрон. науч. журн. 2011. № 10. С. 16–22. URL: http://www.bci-marketing.ru/2011/pm11_10.pdf (дата обращения 22.01.2017).

УДК 519

ПОДВИЖНАЯ СЕТЬ ZIGBEE

Л. М. Макаров, Е. А. Пиликина, С. В. Протасеня

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

Рассмотрены вопросы организации робототехнической сети на основе технологии ZigBEE, обеспечивающей удаленное управление серийно выпускаемыми аппаратами по уборке помещений на обширной территории, с постоянной поддержкой режимов мониторинга качества производимых работ.

сеть ZigBEE, робототехнический комплекс устройств.

Беспроводные компьютерные сети – это технология, позволяющая создавать исполнительные вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей. Эти сети мобильны и легко трансформируются, например, в случае наличия подвижных объектов. Канал связи в такой сети реализуется на радиоволнового приемника и передатчика СВЧ диапазона [1]. Возможность организации беспроводной связи с терминальными, удаленными друг от друга, устройствами сети позволяет создавать сенсорные исполнительные сети, например, на основе типового робототехнического комплекса [2].

Беспроводные локальные сети (WLAN) обладают следующими преимуществами перед кабельными сетями (LAN):

– возможностью неограниченного передвижения в области покрытия WLAN, сохраняя доступ к корпоративным информационным ресурсам;

– высокой скоростью развертывания WLAN;

– малыми эксплуатационными затратами WLAN.

Типичным примером сети является архитектура ZigBee, в которой при относительно небольших скоростях передачи данных обеспечивается гарантированная доставка и защита пакетов передаваемой информации. Стандарт ZigBee предусматривает частотные каналы в диапазонах 868 МГц, 915 МГц и 2,4 ГГц. Наибольшие скорости передачи данных и наивысшая помехоустойчивость достигаются в диапазоне 2,4 ГГц. Поэтому большинство производителей микросхем выпускают приемопередатчики именно для этого диапазона, в котором предусмотрено 16 частотных каналов с шагом 5 МГц.

Скорость передачи данных вместе со служебной информацией в эфире составляет 250 кбит/с. При этом средняя пропускная способность узла для полезных данных в зависимости от загруженности сети и количества

ретрансляций может лежать в пределах от 5 до 40 кбит/с. Типичным примером является однокристальный трансивер SN 260, обладающий параметрами:

– Энергопотребление – 27 мА.
– Мощность передатчика до 5 дБм.
– Чувствительность приемного тракта – 98 дБм.
– Напряжение питания 2,1 – 3,6 В.
– Размер корпуса QLP40 7×7 мм.

Технологии ZigBee изначально создавалась для обслуживания распределенной сети датчиков и управляющих устройств с невысокими скоростями передачи данных. В этих технологиях реализована поддержка сетевой топологии «mesh», спящих и мобильных узлов, а также узлов, которые обеспечивают работу алгоритмов ретрансляции и самовосстановления.

Расстояние между узлами сети составляет десятки метров при работе внутри помещения и сотни метров на открытом пространстве. За счет ретрансляций зона покрытия сети может значительно увеличиваться. В основе сети ZigBee лежит ячеистая топология (*mesh*-топология). В такой сети, каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети. Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя. Возможны различные пути прохождения сообщений, что повышает доступность сети в случае выхода из строя того или иного звена.

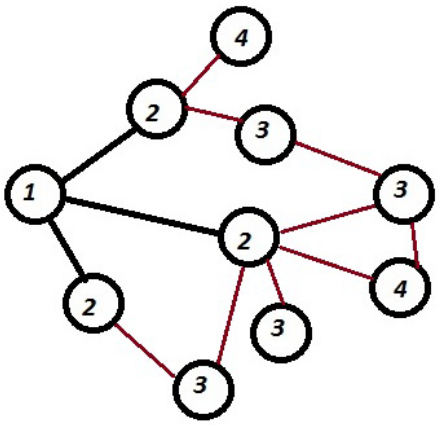


Рис. 1. Схема организации сети ZigBee:
1 – координатор; 2 – роутер;
3 – мобильный аппарат;
4 – спящий аппарат

В сети ZigBee существует 4 типа узлов: координатор, роутер, спящее устройство и мобильное устройство (рис. 1, см. выше).

Технология создания сети ZigBee описана в стандарте 802.15.4 IEEE . Сетевая технология ZigBee реализуется посредством программной надстройки для управления сетевыми устройствами (трансиверами).

Главное устройство в ZigBee-сети – это координатор. Координатор выполняет функции по формированию сети, а также является одновременно доверительным центром (*trust*-центром). Доверительный центр устанавливает политику безопасности и задает настройки во время подключения

устройства к сети. На практике роль координатора исполняет типичный офисный компьютер. Это позволяет оперативно управлять всеми процедурами исполнительных удаленных аппаратов – пылесосов.

На практике часто требуется наличие резервов сетевых ресурсов. Для этой цели можно рекомендовать организацию спящего режима для некоторых исполнительных устройств. Спящие мобильные устройства используют режимы пониженного энергопотребления. Как правило, это узлы с аккумуляторным энергопотреблением.

Роутеры осуществляют маршрутизацию пакетов по сети и должны быть готовы к передаче данных в любой момент времени. Поэтому эти узлы реализуются по схеме постоянного энергопотребления. Общая топология сети ZigBEE представлена на рис. 2.

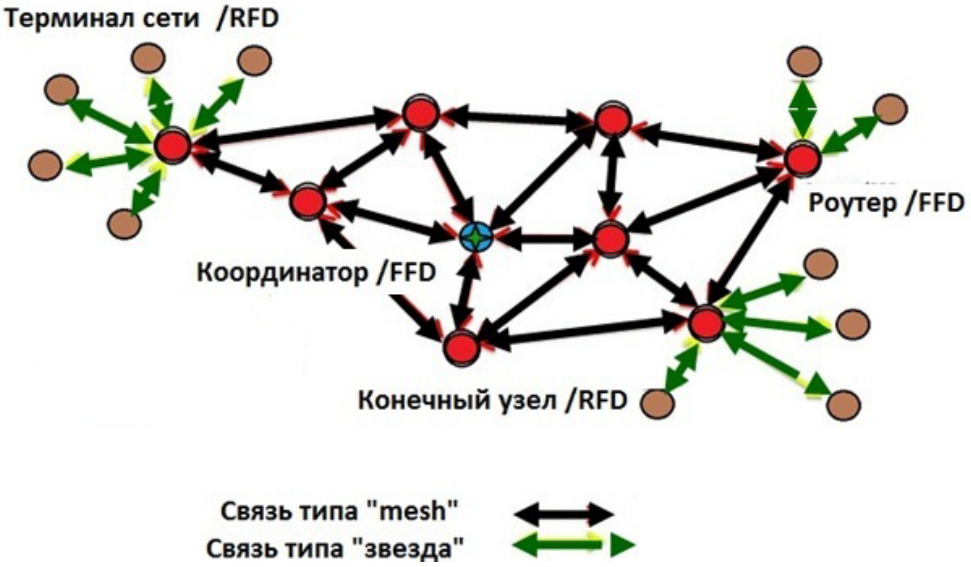


Рис. 2. Топология сети

Маршрутизатор ZigBee (*ZigBee Router*) – полнофункциональное устройство стандарта IEEE 802.15.4, которое не является координатором ZigBee, однако может быть координатором стандарта 802.15.4 и маршрутизатором сообщений между устройствами ZigBee и устройством, присоединяющим новые устройства к сети. Оконечное устройство – любое устройство стандарта IEEE 802.15.4 (RFD и FFD), не являющееся ни координатором ZigBee, ни маршрутизатором ZigBee. Пример присоединения сетевых устройств ZigBee к сети приведен на рис. 3.

Присоединение терминалов производится по принципу: верхний уровень приоритета доминирует над нижним уровнем. В результате образуется дуальная адресная иерархия из блоков. Эта иерархия является основой построения сети по технологии ZigBee при доставке данных по сети. Этот алгоритм в протоколах ZigBee реализован процедурами языка XML.

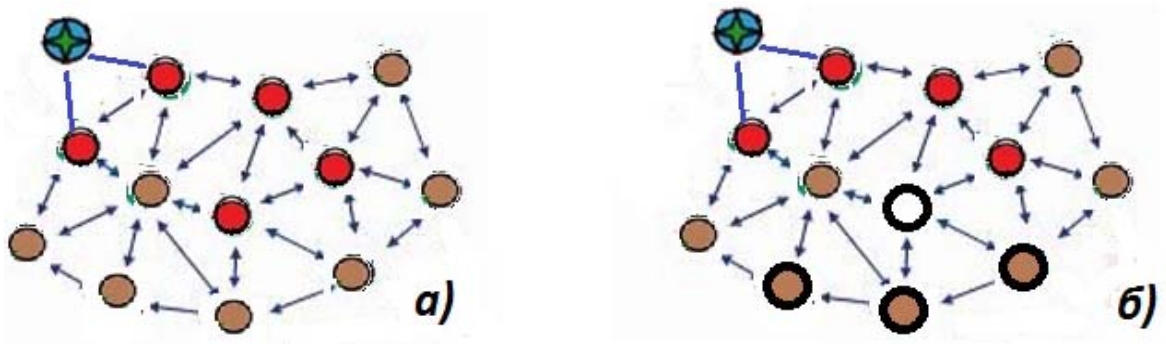


Рис. 3. Схема организации сети с разным количеством терминалов:
а) полная сеть; б) сеть с отключенным роутером и нескольких терминалов

Технология ZigBee позволяет создавать самоорганизующиеся и самовосстанавливающиеся беспроводные сети с автоматической ретрансляцией сообщений, с поддержкой батарейных и мобильных узлов. В качестве мобильного узла рассматривается модель пылесоса QQ-02, позиционируемого робототехническим комплексом (рис. 4).

Рис. 4. Робот-пылесос QQ-02

Конструкция робота предусматривает наличие микроконтроллера, обеспечивающего исполнение рабочих процедур по передвижению и контролю окружающего пространства. Предусмотрена возможность самостоятельного определения уровня энергоресурса и своевременной подзарядки аккумуляторов по специальной процедуре, без участия человека. Эта конструктивная особенность позволяет некоторые экземпляры оконечных терминалов перенастраивать и придавать статус роутеров. Это чрезвычайно важно на территориях современных зданий и сооружений, где прохождение управляющих сигнальных пакетов может быть затруднено.

Наличие в робототехническом комплексе детекторов «чистоты» позволяет формировать регулярные отчеты о качестве проводимых работ. Список исполнительных процедур робототехнического аппарата можно расширить посредством подключения к сети ZigBEE. В этом случае появляется возможность организации коллективной работы нескольких сетевых исполнительных аппаратов, работающих под контролем «координатора», дислокация которого может быть любой на территории обслуживаемого здания.

Список используемых источников

1. Макаров Л. М., Сёмина А. С. Телеметрическая система мониторинга зон повышения риска // International Scientific Review. 2017. № 4 (35). С. 25–27.

2. Макаров Л. М. Управление кибернетической системой // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II международная научно-техническая и научно-методическая конференция : сб. науч. ст. 2013. С. 624–628.

УДК 004.056.53

КОНЦЕПЦИЯ АНАЛИЗА ВЛИЯНИЯ МЕТОДОВ И СРЕДСТВ ИЗВЛЕЧЕНИЯ ЗНАНИЙ НА БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я. С. Маргаритова, Л. К. Птицына

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

Рассмотрены основные аспекты значимости соблюдения конфиденциальности персональных данных. Классифицированы методы и средства извлечения знаний. Описаны требования к защите информации. Формализовано представление о взаимосвязи методов и средств извлечения знаний с защищённостью персональных данных в среде информационных инфраструктур. Раскрыты ключевые положения концепции исследования влияния методов и средств извлечения знаний на безопасность персональных данных.

информационная безопасность, конфиденциальность, извлечение знаний, вторжения, нейронные сети, интеллектуальный анализ данных.

В современном технически оснащенном мире решение проблемы безопасности данных соотносится с одним из приоритетных направлений развития технологий информационной безопасности. В соответствии с федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) при обработке персональных данных оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. В связи с этим обеспечение безопасности персональных данных является предметом исследования учёных всего мира. В процессе исследований основное внимание уделяется уровням защищенности персональных данных при их обработке в информационных системах в зависимости от угроз, требованиям к защите персональных данных, требованиям к материальным носителям биометрических персо-

нальных данных и технологиям хранения таких данных вне информационных систем персональных данных.

В известных научных исследованиях информационные системы персональных данных позиционируются в классе разомкнутых сетей систем массового обслуживания, что не позволяет проследить влияние характера, методов и средств реализации масштабируемой обратной связи на качество их защищённости. Наряду с этим, существует множество методов и средств извлечения знаний, реализуемых интеллектуальными информационными системами. При подобной функциональной направленности интеллектуальные информационные системы, с одной стороны, могут представлять угрозу для безопасности персональных данных в случае их применения злоумышленниками, а, с другой стороны, их использование в обратной связи при обработке персональных данных может послужить средством для повышения уровня защищённости персональных данных.

Для повышения уровня эффективности выявления ситуаций, которые могут быть связаны с возможным вторжением, предлагается применять современные технологии интеллектуального анализа данных, которые позволяют решать слабоструктурированные и плохо формализуемые задачи. Основными задачами интеллектуального анализа данных являются поиск функциональных и логических закономерностей в накопленной информации, построение моделей, объясняющих найденные аномалии и/или прогнозирующих развитие возможных нежелательных ситуаций, а также обнаружение скрытых знаний, которые аналитик не в состоянии выявить самостоятельно. Технологии интеллектуального анализа данных, в отличие от традиционных методов обработки данных, позволяют эффективно выполнять оценку состояния наблюдаемых процессов, выявлять и ранжировать причины значимых изменений, прогнозировать развитие процессов и вырабатывать рекомендации по подготовке возможных вариантов решений с прогнозом их последствий.

В технологиях извлечения знаний могут использоваться различные методы и средства [1, 2]. Многообразие методов технологий извлечения знаний обеспечивается благодаря обширным возможностям математического аппарата теории вероятностей, теории графов, теории сложных систем, теории принятия решений, теории регрессионного анализа, теории последовательного анализа, теории временных рядов, теории инвариантов, теорий логик, теории нечётких множеств, теории нейронных сетей, теории эволюции, теории онтологий, теории семантических сетей. На базе выбираемых методов разрабатываются аппаратные, программные или аппаратно-программные средства технологий извлечения знаний. Представительный ряд методов ориентируется на интеллектуализацию технологий извлечения знаний. К этому ряду, прежде всего, относятся методы теорий

логик, теории нечётких множеств, теории нейронных сетей, теории эволюции, теории онтологий, теории семантических сетей.

Перечисленные методы могут интегрироваться в различных комбинациях для эффективного решения поставленных задач, в частности, решения задач, связанных с предотвращением несанкционированного доступа к персональным данным.

Методы интеллектуального анализа данных могут применяться в системах обнаружения вторжений (СОВ) для решения таких задач, как снижение вероятности ложных срабатываний системы; обнаружение аномалий; построение шаблонов атак. Для решения перечисленных задач могут использоваться механизмы, основанные на методах сетей Байеса, методе *k*-ближайших соседей, методе опорных векторов, методе структурирования задачи в виде древовидного графа решений, методах искусственных нейронных сетей [3, 4, 5, 6].

Благодаря введению средств интеллектуального анализа данных, выполняющих функции обратной связи в информационной системе, предоставляются новые приёмы управления защищённостью персональных данных.

Для определения эффекта от введения новых интеллектуальных средств в систему защиту персональных данных предлагается формализация, ориентированная на проведение сравнительного анализа динамических характеристик защищённости. В качестве динамических характеристик выбираются математические ожидания времени обнаружения угроз и времени их отражения [7].

Для проведения сравнительного анализа динамических характеристик защищённости предусматривается два этапа.

На первом этапе строятся две модели процессов обнаружения угроз системой защиты информации.

В первой модели первого этапа, описываемой в дискретном пространстве состояний матрицей переходов $\mathbf{P_O^B}$, отражается процесс функционирования системы защиты информации без организации обратной связи с помощью средств интеллектуального анализа данных.

Во второй модели первого этапа, представляемой в дискретном пространстве состояний матрицей переходов $\mathbf{P_A^B}$, отражается процесс функционирования системы защиты информации с обратной связью, реализуемой с помощью средств интеллектуального анализа данных.

Для каждой из указанных матриц $\mathbf{P_O^B}$, $\mathbf{P_A^B}$ находится соответствующая матрица переходов во множестве невозвратных состояний $\mathbf{C_O^B}$, $\mathbf{C_A^B}$.

На основе матриц $\mathbf{C_O^B}$, $\mathbf{C_A^B}$ находится соответственно E_O^B [k], E_A^B [k] математическое ожидание времени обнаружения угрозы при отсутствии и наличии средств интеллектуального анализа данных

$$\mathbf{T_O^B} = (\mathbf{E} - \mathbf{C_O^B})^{-1},$$
$$\mathbf{t_O^B} = \mathbf{T_O^B}\,\mathbf{e},$$
$$\mathrm{E_O^B}\,[\mathrm{k}] = t_{1\mathbf{O}}^{\mathbf{B}},$$

$$\mathbf{T_A^B} = (\mathbf{E} - \mathbf{C_A^B})^{-1},$$
$$\mathbf{t_A^B} = \mathbf{T_A^B}\,\mathbf{e},$$
$$\mathrm{E_A^B}\,[\mathrm{k}] = t_{1\mathbf{A}}^{\mathbf{B}},$$

где **E** – единичная матрица; $\mathbf{T_O^B}$ – матрица элементов $T_{ij\mathbf{O}}^{\mathbf{B}}$ $i, j = 1, 2, ..., M_{\mathbf{O}}^{\mathbf{B}}$; $T_{ij\mathbf{O}}^{\mathbf{B}}$ – математическое ожидание числа пребываний системы защиты информации при отсутствии интеллектуальных средств анализа данных в состоянии с номером j, при условии, что исходным состоянием являлось состояние с номером i; $\mathbf{T_A^B}$ – матрица элементов $T_{ij\mathbf{A}}^{\mathbf{B}}$ $i, j = 1, 2, ..., M_{\mathbf{A}}^{\mathbf{B}}$; $T_{ij\mathbf{A}}^{\mathbf{B}}$ – математическое ожидание числа пребываний системы защиты информации при наличии интеллектуальных средств анализа данных в состоянии с номером j, при условии, что исходным состоянием являлось состояние с номером i; $M_{\mathbf{O}}^{\mathbf{B}}$ – число невозвратных состояний системы защиты информации при отсутствии интеллектуальных средств анализа данных; $M_{\mathbf{A}}^{\mathbf{B}}$ – число невозвратных состояний системы защиты информации при подключении интеллектуальных средств анализа данных; **e** – единичный вектор столбец; $\mathbf{t_O^B}$ – вектор столбец элементов $t_{i\mathbf{O}}^{\mathbf{B}}$, $i = 1, 2, ..., M_{\mathbf{O}}^{\mathbf{B}}$; $\mathbf{t_{OA}^B}$ – вектор столбец элементов $t_{i\mathbf{A}}^{\mathbf{B}}$, $i = 1, 2, ..., M_{\mathbf{A}}^{\mathbf{B}}$.

На втором этапе строятся две модели процессов отражения угроз системой защиты информации.

В первой модели второго этапа, описываемой в дискретном пространстве состояний матрицей переходов $\mathbf{P_O^S}$, отражается процесс отражения угрозы системой защиты информации без организации обратной связи с помощью средств интеллектуального анализа данных.

Во второй модели второго этапа, представляемой в дискретном пространстве состояний матрицей переходов $\mathbf{P_A^S}$, отражается процесс отражения угрозы системой защиты информации с обратной связью, реализуемой с помощью средств интеллектуального анализа данных.

Для каждой из указанных матриц POS, $\mathbf{P_A^S}$ находится соответствующая матрица переходов во множестве невозвратных состояний $\mathbf{C_O^S}$, $\mathbf{C_A^S}$.

На основе матриц $\mathbf{C_O^S}$, $\mathbf{C_A^S}$ находится соответственно $\mathrm{E_O^S}$ [k], $\mathrm{E_A^S}$ [k] математическое ожидание времени отражения угрозы при отсутствии и наличии средств интеллектуального анализа данных. При этом используются выше приведённые операции линейной алгебры.

По результатам сравнения математических ожиданий времени обнаружения и времени отражения угроз $\mathrm{E_O^B}$ [k], $\mathrm{E_A^B}$ [k], $\mathrm{E_O^S}$ [k], $\mathrm{E_A^S}$ [k] выявляется эффект от введения интеллектуальных средств анализа данных в систему защиты информации.

Предлагаемая концепция анализа влияния методов и средств извлечения знаний на безопасность персональных данных расширяет математическое обеспечение систем защиты информации, предназначенное для повышения их эффективности.

Список используемых источников

1. Гаврилова Т. А., Хорошевский В. Ф. Базы знаний интеллектуальных систем. СПб. : Питер, 2000. 384 с.

2. Птицына Л. К., Шестаков С. М. Информационные сети. Интеллектуальные информационные агенты : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2008. 210с. ISBN 5-7422-1728-5.

3. Bhattacharyya D. K., Kalita J. K. Network Anomaly Detection A Machine Learning Perspective. 2010. URL: http://sanghv.com/download/jp/Books/Network Anomaly Detection-Machine Learning perspective.pdf (дата обращения 16.02.2018).

4. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети : учеб. пособие. М. : ФИЗМАТЛИТ, 2001. 224 с.

5. Ross Quinlan J. C4.5: Programs for Machine learning. Morgan Kaufmann Publishers 1993.

6. Buczak A., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. 2016. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp arnumber=7307098 (дата обращения 16.02.2018).

7. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Новые формализации аналитического исследования комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с. ISBN 978-3-659-23299-2.

УДК 007:519.2

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ БИНАРНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. ОКОНЧАНИЕ

В. А. Медведев

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

Рассматривается бинарная последовательность как модель различных её реализаций, в которой дискрета может принимать одно из двух возможных значений. Продемонстрирован способ определения вероятностей пачек нулей и единиц на основе вероятностей независимых отсчетов одной или нескольких позиций бинарной последовательности. Приведены формульные соотношения.

бинарная последовательность, модель, P-вероятности, G-вероятности.

Начало «Актуальные проблемы инфотелекоммуникаций в науке и образовании». Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2016, 2017.

Бинарная последовательность (БП) – это модель (общее) различных её реализаций. При описании модели используются вероятности двух типов: вероятности получения комбинаций нулей и единиц на определенном числе позиций БП [1] (назовем их Р-вероятности) и вероятности группирования значений БП (нулей и единиц) в конечные последовательности (пачки) [2] (назовем их *G*-вероятности). В [1, 2, 3] излагались способы вычисления *P*-вероятностей на основе *G*-вероятностей. В данной статье рассматривается обратный путь – получение *G*-вероятностей при исходных *P*-вероятностях для независимых отсчетов.

При отсчете одной позиции БП, как известно[1]:

$$P(1) = \frac{M_1}{M_1+M_0}\ ;\ \ P(0) = \frac{M_0}{M_1+M_0},$$

где

$$M_0 = \sum_{k=1} k\, G_0(k) \ \ \text{и} \ \ M_1 = \sum_{k=1} k\, G_1(k)$$

математические ожидания числа нулей и единиц в пачке.

Независимые отсчеты позиций БП характеризуются неизменностью вероятностей результатов текущего отсчета от результатов других отсчетов. В частности, например: $P(0/1) = P(1)$ – вероятность нахождения «1» после «0» равна абсолютной вероятности получения «1». Подставив выражения для вероятностей (см. [1]) в данное равенство, получаем:

$$\frac{1}{M_0} = \frac{M_1}{M_1+M_0}\,, \tag{1}$$

откуда вытекает основное соотношение для независимых отсчетов:

$$M_0 + M_1 = M_0 M_1. \tag{2}$$

Или, раскроем равенство $P(01) = P(0)\,P(1)$.

$$\frac{1}{M_0 + M_1} = \frac{M_0}{M_1 + M_0}\,\frac{M_1}{M_1 + M_0},$$

из которого получается тот же результат (2).

Отметим ещё раз, что для независимых отсчетов вероятности отсчета одной позиции БП составляют:

$$P(0) = \frac{1}{M_1};\ \ P(1) = \frac{1}{M_0}. \tag{3}$$

Приступим к нахождению *G*-вероятностей. Известно [2], что для общего случая:

$$P(110) = \frac{1}{\mathrm{M_0} + \mathrm{M_1}} \sum_{k=2} \mathrm{G_1(k)}.$$

Но для независимых отсчетов

$$P(110) = P(1)P(1)P(0),$$

а с учетом (2) и (3) получаем:

$$\frac{1}{\mathrm{M_0} + \mathrm{M_1}} \sum_{k=2} \mathrm{G_1(k)} = \frac{1}{{M_0}^2} \frac{1}{M_1},$$

что приводит к равенству:

$$\sum_{k=2} G_1(k) = P(1). \quad (4)$$

Аналогично для пачек нулей:

$$\sum_{k=2} G_0(k) = P(0). \quad (5)$$

Исходя из (4), (5) обнаруживаем, что вероятности пачек нулей и единиц с одной составляющей выражаются простыми равенствами:

$$G_0(1) = P(1), \qquad G_1(1) = P(0). \quad (6)$$

Далее, связывая соотношения

$$P(1110) = \frac{1}{M_0 + M_1} \sum_{k=3} G_1(k) \quad \text{и} \quad P(1110) = P(1)P(1)P(1)P(0)$$

приходим к заключению, что

$$\sum_{k=3} G_1(k) = P(1)^2. \quad (7)$$

Аналогично и для пачек нулей:

$$\sum_{k=3} G_0(k) = P(0)^2. \quad (8)$$

Тогда:

$$G_0(2) = \sum_{k=2} G_0(k) - \sum_{k=3} G_0(k) = P(0)P(1); \quad (9)$$

$$G_1(2) = \sum_{k=2} G_1(k) - \sum_{k=3} G_1(k) = P(0)P(1); \quad (10)$$

Продолжая цепочку аналогичных действий, получаем остальные вероятности для пачек нулей и единиц:

$$G_0(3) = P(1)P(0)^2; \qquad G_1(3) = P(0)P(1)^2;$$
$$G_0(4) = P(1)P(0)^3; \qquad G_1(4) = P(0)P(1)^3 \qquad \text{и т. д.}$$

Не трудно заметить, что G-вероятности в отдельности для нулей и единиц являются членами геометрической прогрессии, сумма которой, например, для пачек нулей составляет:

$$P(1)+P(1)P(0)+P(1)P(0)^2+ P(1)P(0)^3+ \ldots = \frac{P(1)}{1-P(0)} = 1.$$

И последнее. Определим математическое ожидание, например, для пачек нулей.

$$\mathrm{G}_0(1)+2\mathrm{G}_0(2)+3\mathrm{G}_0(3)+ 4\mathrm{G}_0(4) \ldots =$$
$$=P(1)+2P(1)P(0)+3P(1)P(0)^2+ 4P(1)P(0)^3 \ldots =$$
$$= P(1)+ P(1)P(0) + P(1)P(0)^2 + P(1)P(0)^3+ \ldots$$
$$+ P(1)P(0) + P(1)P(0)^2 + P(1)P(0)^3 + \ldots$$
$$+ P(1)P(0)^2 + P(1)P(0)^3 + \ldots .$$

Математическое ожидание представляет собой сумму геометрических прогрессий, каждая из которых имеет собственную сумму:

$$S_1 = \frac{P(1)}{1-P(0)} = 1; \qquad S_2 = \frac{P(1)P(0)}{1-P(0)} = P(0);$$
$$S_3 = \frac{P(1)P(0)^2}{1-P(0)} = P(0)^2; \qquad S_4 = \frac{P(1)P(0)^3}{1-P(0)} = P(0)^3 \text{ и т. д.}$$

В результате получаем:

$$1 + P(0) + P(0)^2 + P(0)^3 + P(0)^4+ \ldots = \frac{1}{1-P(0)} = M_0.$$

Список используемых источников

1. Медведев В. А. Модели бинарной последовательности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция сб. науч. ст. в 2-х т. 2015. Т. 1. С. 538–542.

2. Медведев В.А. Вероятностные характеристики бинарной последовательности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция сб. науч. ст. в 3-х т. 2016. Т. 2. С. 137–140.

3. Медведев В. А. Вероятностные характеристики бинарной последовательности. Продолжение // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция сб. науч. ст. в 4-х т. 2017. Т. 3. С. 329–333.

УДК 004.41

ТЕХНОЛОГИИ ТРЕКИНГА ОБЪЕКТОВ В ВИДЕОПОТОКЕ НА ОСНОВЕ ФИЛЬТРА ЧАСТИЦ

Н. А. Москаленко, Д. А. Осинкин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Задача трекинга объектов в видеопотоке является неотъемлемой частью многих прикладных областей, таких как построение систем видеонаблюдения, создание интерфейсов человек-компьютер, программ для передачи или сжатия видео и другое. При решении задачи трекинга объекта в видеопотоке необходимо обрабатывать огромное количество данных, кадров, что повышает затраты вычислительной мощности, а также повышает продолжительность обработки. Особенно это справедливо, если нахождение положения объекта в потоке не нормально, мультимодально или вообще произвольной природы.

трекинг объектов, обработка видео, фильтр частиц, распознавание объектов.

Одним из наиболее подходящих для задачи моделирования изменяющихся во времени произвольных распределений (трекинга объектов) являются последовательные методы Монте-Карло, или фильтры частиц, которые оценивают плотности при помощи конечных наборов частиц (семплов) реализующих распределение.

В основе фильтров частиц лежит модель, описывающая изменение скрытых переменных, характеризующих положение объекта в кадре, и получение наблюдаемых переменных итоговых изображений из видеопотока, а также метод аппроксимации плотности с помощью реализующей ее выборки, соответствующей задаче фильтрации задаче определения реального значения скрытых переменных в текущий момент времени на основе полной истории значений наблюдаемых переменных [1].

Фильтр частиц работает по следующему алгоритму [2]:

1. Генерируем N начальных семплов $\tilde{x}_1^i \sim \mu(x_1)$, веса устанавливаем равными:

$$\tilde{\omega}_0^i = 1/N, k = 0.$$

2. Для всех к от 1 до *t*.

a. Вычисляем веса:

$$\tilde{\omega}_0^i = p(y_k \mid \tilde{x}_k^i)\tilde{\omega}_{k-1}^i.$$

b. Нормализуем веса:

$$\omega_k^i = \frac{\tilde{\omega}_k^i}{\sum_{j=1}^{N} \tilde{\omega}_k^i}.$$

c. Для $i = 1, \ldots, N$ генерируем новый семпл X такой, что

$$\mathrm{P}(x_t^i = \tilde{x}_k^j) = \omega^j.$$

d. Генерируем новую выборку из N элементов из предложенного распределения:

$$\tilde{x}_{k+1}^i \sim f(x_{k+1} \mid x_k^i).$$

На каждом кадре определяется набор возможных состояний отслеживаемого объекта:

$$S_t = \{s_t^j\}, j \in \{1 \ldots N\}.$$

Данный набор обновляется при переходе от одного кадра к другому по рекурсивному алгоритму:

– Новый набор получается из предыдущего, где семпл из старого набора выбирается с вероятностью, пропорциональной его весу.

– Для каждого семпла новое состояния получается сэмплированием из модели движения:

$$p(X_t \mid X_{t-1} = x_{t-1}^i).$$

Изменения в новом кадре используются при обновлении весов с помощью подсчета правдоподобия наблюдения, т. е.

$$\pi_t^j = p(Z_t \mid X_t = x_t^j, Z_0, Z_1, \ldots, Z_{t-1}).$$

Начальная позиция объекта определяется рамкой выделения на изображении, т. е. каждая позиция-кандидат определяется некоторым вектором X, по которому как минимум можно получить значения центра, ширины и высоты рамки в абсолютных значениях.

Для предсказания новых положений частиц используется авторегрессионная модель первого порядка. По этой модели новое состояние, основанное на предыдущем состоянии, получается за счет добавления нормального шума ко всем показателям в случае, когда мы не моделируем скорость отслеживаемого объекта:

$$x_t = x_{t-1} + N(0, \sigma_x^2),$$
$$y_t = y_{t-1} + N(0, \sigma_y^2),$$
$$w_t = w_{t-1} + N(0, \sigma_w^2),$$
$$h_t = h_{t-1} + N(0, \sigma_h^2).$$

Таким образом решается проблема, когда маловероятные частицы получает все меньший вес и ситуации сильного изменении положения объекта характеризуются моделью как невозможные.

Данный алгоритм имеет следующие плюсы:

– Устойчивость к частичным перекрытиям объекта на видео.
– Уменьшено временные затраты на вычисление.
– Уменьшено затраты вычислительной мощности.
– Более качественное определение и сопровождение объекта.
– Возможность предсказания направления объекта.

Однако имеются и недостатки, такие как:

– При полном перекрытии перекрытия, невозможно сравнивать предсказанные положения объекта с самим объектом.
– Зависимость от зашумления кадра.
– В зависимости от доступных вычислительных мощностей видеопоток должен быть в определенном качестве (кадр размером от 0,3 до 1,0 Мп).

Для решения данных недостатков можно добавить специальный алгоритм «При потере объекта», который будет вводится, если минимальное из расстояний между признаками регионов и шаблона больше некоторого порога. Это позволит частицам продолжать находиться там же и двигаться с той же скоростью, что и объект до потери цели. Для решения задач с вычислительной мощностью и зависимостей зашумления стоит использовать улучшенные методы обработки изображений и видеопотока.

Список используемых источников

1. Пару слов о распознавании образов. URL: https://habrahabr.ru/post/208090/ (дата обращения 10.01.2018).

2. Дэвид А. Форсайт, Жан Понс. Компьютерное зрение. Современный подход. М. : Вильямс, 2004. 650 с.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 621.391

ТРАНСПОРТНЫЕ ВОЛОКОННО-ОПТИЧЕСКИЕ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ И ПРЕМЕНЯЕМОЕ ДЛЯ ИХ ПОСТРОЕНИЯ МНОГОАГЕНТНОЕ МОДЕЛИРОВАНИЕ

А. Д. Нестеров

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Статья посвящена применению терминологии для моделирования многоагентных систем, позволяющей представить ВОЛС как совокупность взаимоувязанных элементов (агентов) в зависимости от выполняемых ими функции, таких как: агент спектральной передачи; агент среды передачи;

ВОЛС, взаимосвязанные агенты, моделирование мультиагентных систем.

Характерной чертой информационной эры является бурное развитие коммуникаций (телекоммуникаций) – одной из составляющих инфраструктуры информационных технологий. В условиях возросшей потребности в обеспечении надежного канала связи, как в сфере построения глобальных информационных сетей, так и в области промышленной автоматизации возникла необходимость поиска альтернативных технологий (систем) передачи информации (данных). Данные технологии основаны на передачи информации по волоконно-оптической линии связи (ВОЛС), которая позволяет передавать информацию с существенно более высокими скоростями и надежностью, а также невосприимчива к электромагнитному излучению и имеет вполне приемлемые для большинства реализаций стоимостные показатели в пересчете на канал. Основой построения таких систем является волоконно-оптическая линия связи, которая состоит из разнообразных агентов, выполняющих различные функциональные задачи [1].

Агент спектральной передачи – спектральный диапазон, разбитый по длинам волн на несколько рабочих зон (окон прозрачности).

Окно прозрачности – диапазон длин волн оптического излучения, в котором имеет место меньшее, по сравнению с другими диапазонами, затухание излучения в оптическом волокне (ОВ) [2].

Спектр первого окна прозрачности 800–900 нм. В данном спектре элементами ВОЛС являются лазерные диоды и светодиоды (LED) на *GaAs*/*AlGaAs* основе применяемые качестве передатчиков, а кремние-

вые фотодиоды – для приемников. Однако потери ОВ в этом диапазоне относительно высокие, и оптические усилители (ОУ) не очень хорошо разработаны для этой области спектра. Спектр первого окна прозрачности подходит только для передачи информации на короткие расстояния, в основном в локальных вычислительных сетях (ЛВС).

Второе окно прозрачности использует длину волны около 1,3 мкм, где потери в ОВ гораздо ниже, и хроматическая дисперсия волокон является очень малой, так что дисперсионные расширение импульсов сводится к минимуму. Это окно изначально использовалось для передачи данных на большие расстояния. Однако, ОУ на 1,3 мкм (на основе, например, стекла, легированного празеодимом) не так хороши, как их аналоги на основе эрбия (1,5 мкм). Кроме того, низкая дисперсия не обязательно идеально подходит для протяженных линий, так как это может увеличить эффект оптической нелинейности. В настоящее время второе окно прозрачности используется преимущественно на городских и зоновых линиях связи.

Третье окно, использует длину волны около 1,5 мкм. Потери ОВ являются самыми низкими в этом диапазоне, и доступны легированные эрбием ОУ, которые обеспечивают очень высокую производительность. Дисперсия волокна, как правило, аномальная, но может быть адаптирована с большей гибкостью (со смещенной дисперсией волокна). Третье окно наиболее широко используется в магистральных линиях.

Спектр четвертого окна прозрачности использует длину волны 1,58–1,62 мкм применяются для увеличения рабочего диапазона систем спектрального мультиплексирования (WDM).

Пятое окно имеет длину волны 1,4 мкм и появилось в результате тщательной очистки ОВ от посторонних примесей. Таким образом, было получено ОВ AllWave, имеющее малые потери во всем диапазоне от 1280 до 1650 нм.

Из выше рассмотренных окон прозрачности основными считаются 1, 2, 3 с центральными длинами волн 850 нм для работы многомодовых ОВ (МОВ), 1310 нм (основной) и 1543 нм (стандартный) для работы одномодовых ОВ (ООВ).

Международным союзом электросвязи (МСЭ-Т) были утверждены спектральные диапазоны в интервале 1260…1675 нм, представленные в таблице 1.

От выбора окна прозрачности будет зависеть выбор передающей среды (агент среды передачи).

Агент среды передачи – ОВ с некоторыми его стандартами и модификациями представлен в таблице 2 [3].

ТАБЛИЦА 1. Спектральные диапазоны

Обозначение	Диапазон, нм	Русское название	Английское название
O	1260…1360	Основной	Original
E	1360…1460	Расширенный	Extended
S	1460…1530	Коротковолновый	Short wavelength
C	1530…1565	Стандартный	Conventional
L	1565…1625	Длинноволновый	Long wavelength
U	1625…1675	Сверх длинноволновый	Ultra-long wavelengh

ТАБЛИЦА 2. Рекомендации МСЭ-Т для ОВ

Стандарт	Описание	Модификации	Примечание
G.651.1	Характеристика многомодового оптического волокна и кабеля	–	Локальные сети малой протяженности
G.652	Характеристики одномодового оптического волокна и кабеля	A, B, C, D	Транспортные сети различного назначения и средней протяженности
G.653	Характеристики одномодового оптического волокна и кабеля со смещенной дисперсией	A, B	Магистральные сети большой протяженности
G.654	Характеристики одномодового оптического волокна и кабеля со смещенной длиной волны отсечки	A, B, C	Океанские и морские ВОЛС
G.655	Характеристики одномодового оптического волокна и кабеля с ненулевой смещенной дисперсией	A, B, C, D, E	Магистральные сети большой протяженности

Список используемых источников

1. Мельников М. В., Стахеев И. Г., Титова О. В. Основные характеристики элементов волоконно-оптического линейного тракта специального назначения / Бюллетень результатов научных исследований. 2015. Вып. 2 (15). С. 49–61.

2. Дмитриев С. А., Слепов Н. Н. Волоконно-оптическая техника: современное состояние и перспективы. М. : ООО «Волоконно-оптическая техника», 2005. 576 с.

3. Дейвис Р., Гаррет И., Гудфеллоу Р. К. и др. Волоконно-оптическая связь. Приборы, схемы и системы / Под ред. М. Дж. Хауэса, Д. В. Моргана. М. : Радио и связь, 1982. 270 с.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.5

PHP ИЛИ ASP.NET

А. Р. Новрузов, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В данной статье рассмотрены проблемы выбора языка программирования для разработки web-сайта, есть богатый выбор относительного того, какой язык использовать: Perl, PHP, ASP, ASP.Net, JSP, Coldfusion. Самыми распространёнными сегодня являются PHP и ASP.NET. В статье был произведен сравнительный анализ между этими платформами.

PHP, ASP.NET, программирование, веб-сайт, база данных, фреймворк.

Среди программистов разворачиваются многочисленные дебаты по поводу того, какой язык программирования лучше: PHP или ASP. В основном все статьи и обзоры по этому вопросу сводятся к воспеванию одного или другого языка и являются выражением сугубо личного мнения конкретного коддера. К тому же, прогресс не стоит на месте, и разработчики ежедневно работают над усовершенствованием языков программирования [1].

PHP (*Hypertext Preprocessor* – «PHP: препроцессор гипертекста»; первоначально *Personal Home Page Tools* – «Инструменты для создания персональных веб-страниц») – скриптовый язык общего назначения, интенсивно применяемый для разработки веб-приложений. В настоящее время поддерживается подавляющим большинством хостинг-провайдеров и является одним из лидеров среди языков, применяющихся для создания динамических веб-сайтов [2].

Язык и его интерпретатор (*Zend Engine*) разрабатываются группой энтузиастов в рамках проекта с открытым кодом. Проект распространяется под собственной лицензией, несовместимой с GNU GPL.

Синтаксис PHP подобен синтаксису языка Си. Некоторые элементы, такие как ассоциативные массивы и цикл foreach, заимствованы из Perl.

Для работы программы не требуется описывать какие-либо переменные, используемые модули и т. п. Любая программа может начинаться непосредственно с оператора PHP.

ASP.NET (*Active Server Pages* для .NET) – технология создания веб-приложений и веб-сервисов от компании Майкрософт. Она является составной частью платформы Microsoft .NET и развитием более старой технологии Microsoft ASP [2].

ASP.NET внешне во многом сохраняет схожесть с более старой технологией ASP, что позволяет разработчикам относительно легко перейти на ASP.NET. В то же время внутреннее устройство ASP.NET существенно отличается от ASP, поскольку она основана на платформе .NET и, следовательно, использует все новые возможности, предоставляемые этой платформой.

Хотя ASP.NET берёт своё название от старой технологии Microsoft ASP, она значительно от неё отличается. Microsoft полностью перестроила ASP.NET, основываясь на Common Language Runtime (CLR), которая является основой всех приложений Microsoft .NET. Разработчики могут писать код для ASP.NET, используя практически любые языки программирования, входящие в комплект .NET Framework (C#, Visual Basic.NET и JScript.NET). ASP.NET имеет преимущество в скорости по сравнению со скриптовыми технологиями, так как при первом обращении код компилируется и помещается в специальный кэш, и впоследствии только исполняется, не требуя затрат времени на парсинг, оптимизацию, и т. д.

Масштабируемость и простота обслуживания абсолютно не зависят от того, какой язык вы выберите. Масштабируемость и простота обслуживания веб-приложений зависят в первую очередь от:

- опыта программиста;
- использования лучших практик программирования;
- использования надежной платформы программирования;
- следовать программному руководству и стандартам.

Что же касается времени для написания программы на языке, то работа с ASP занимает в два раза больше времени, чем в PHP.

Сегодня языки программирования в основном имеют очень современную платформу и выбор одного или другого языка никак не повлияет на скорость работы большинства сайтов в интернете. Однако если языку программирования предстоит выполнить огромные и сложные задачи, как для сайтов Google, Yandex и других поисковиков, то программисты используют много разных языков, где каждый выполняет свою отдельную миссию.

Одна из основных задач любого веб-приложения является обеспечение доступа и обработка запросов к базе данных и вывод результатов на веб-серевер, а затем в браузер. На данном этапе, скорость языка программирования никак не влияет на скорость работы сайта. На его скорость влияет только сервер базы данных, веб-сервер, веб-браузер клиента и его пропускная способность.

Сегодня большинство серверов баз данных, таких как MySQL (в настоящее время принадлежит *Oracle*), PostgreSQL, MSSQL (*Microsoft SQL Server*) и Oracle, сражаются за превосходство в скорости и производительности. Мы постоянно наблюдаем рост производительности и новых воз-

можностей серверов баз – данных в новых версиях. Поэтому если программист использует язык структурированных запросов SQL, то его сайт будет иметь большую производительность.

MySQL используется Google, Facebook, YouTube, Yahoo, которые получают огромную аудиторию по всему миру. Поэтому я бы не стал ставить под сомнение способность сервера баз данных MySQL.

Проведя несколько своих исследований на нескольких сайтах онлайн-статистики, по состоянию на момент написания статьи, связи и интерфейсов между PHP и MySQL работает быстрее, чем ASP.net и MSSQL, но это едва заметно.

Еще одной основной задачей веб-приложения является получение доступа к файловой системе, для того, чтобы найти изображение и отправить его на веб-сервер. И снова, язык программирования играет здесь ничтожную роль. В основном имеет значение только работа операционной системы и файловой системы, которые не связаны с работой языка программирования.

ASP.net, как правило, написаны на C #. Вообще говоря, на момент написания статьи, C # быстрее, чем язык программирования PHP, но это может измениться, так как каждый язык программирования будет обновляться и совершенствоваться, чтобы бороться за более высокую скорость. Так что, если необходимо запустить 2000000 циклов выполнения расчетов, ASP.net выигрывает у PHP. Тем не менее, это очень необычный сценарий, так как обычный цикл использует 100 расчетов, а не 2000000 [3].

PHP, MySQL, PostgreSQL, веб-сервер Apache и операционная система Linux являются бесплатными, как и все их обновления. Кроме того, отсутствуют дополнительные платы на лицензии на другой физический сервер в качестве резервного при необходимости работать с несколькими серверами для балансировки нагрузки и кластеризации серверов.

LAMP (*Linux*, *Apache*, *MySQL* и PHP) является более популярным набором среди хостинговых компаний, и его популярность приводит к снижению ежемесячных расходов на хостинг с LAMP по сравнению с Windows хостингом.

ASP.net и IIS вы получаете бесплатно, если вы покупаете ОС Windows. Однако стоимость лицензии на Microsoft Windows Server, Microsoft SQL Server и будущих обновлений значительно велика. Например, лицензия на Microsoft Server 2008 R2 Standard – 64-разрядная стоит около $1029 и Microsoft SQL Server 2008 Standard Edition для малого бизнеса – около $1038. К тому же существует вероятность новых затрат на ОС Windows, если ваш сайт станет популярным и возникнет необходимость запустить сайт уже на нескольких физических серверах, что потребует таких функций, как балансировка нагрузки, кластеризации серверов или горячий резерв.

Так как PHP является языком с открытым исходным кодом, это позволяет огромному количеству дружественных разработчиков и программистов вносить в него изменения для усовершенствования и устранения неполадок, а также позволяет обеспечить поддержку платформы.

ASP – язык, с закрытым кодом, поэтому его обновление зависит только от разработчиков компании Microsoft. Поддержка также ограничена количеством участников разработки [3].

PHP и MySQL не зависят от редакторов, так как к ним имеют доступ обширное число разработчиков. Рзработчики PHP в основном используют такие текстовые редакторы как VI, VIM, Notepad ++.

В то время как большинство ASP программистов используют Microsoft Visual Studio для внесения каких-либо изменений.

VI и VIM очень продвинутые и независимые редакторы (программы) и программисты активно изучают и используют их возможности в полной мере. Это позволяет им писать очень сложные программы быстро и эффективно. Когда речь идет о необходимости использования и интеграции других основных языковых платформ, таких как JavaScript, Ajax, JQuery и т. д., лучше использовать PHP программистов, потому что они знакомы с открытой средой источника и ручного кодирования при использовании VI и VIM редакторов.

PHP не зависит от платформы и может работать на любой ОС – Linux, Unix, Mac OS X и Windows [4].

ASP.net построен для работы только на платформе Windows.

Мы отдаем предпочтение языку PHP. Нам он кажется намного проще, шустрее и что самое главное он бесплатный. Вот три главные причины, почему мы выбираем его. Однако с нами не согласятся любители ASP. ASP много лет жил живет и будет жить, ведь это кому-то нужно, значит не так уж он и плох.

Список используемых источников

1. Рихтер Дж. CLR via C#. Программирование на платформе Microsoft.NET Framework 4.5 на языке C#. СПб. : Питер, 2017. 896 с.

2. ASP.NET. URL: https://ru.wikipedia.org/wiki/ASP.NET (дата обращения 16.01.2018).

3. PHP против ASP.NET – что лучше? URL: https://nevlabs.ru/about/articles/web/php-vs-aspnet/ (дата обращения 16.01.2018).

4. Котеров Д. М., Симдянов И. Ю. PHP 7. СПб. : БХВ-Петербург, 2017. 1088 с.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 654.9

МЕТОДИКА СИНТЕЗА СИСТЕМЫ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО МОНИТОРИНГА С МЕТАУПРАВЛЕНИЕМ ФУНКЦИОНАЛЬНОСТЬЮ

А. А. Олимпиев

АО «Институт инфотелекоммуникаций»

Одна из проблем, связанных с синтезом системы оперативно-технического мониторинга, заключается в необходимости предсказания процессов адаптации к условиям применения, которые будут происходить на этапе поддержки применения. В статье предлагается методика синтеза оперативно-технического мониторинга, в которой задачи адаптации решаются на этапе технического проектирования.

Мониторинг, метауправление функциональностью, информационная система.

Система оперативно-технического мониторинга (СОТМ) – это информационная система (ИС), реализующая информационные технологии сбора, хранения, обработки и предоставления пользователю информации об объекте (как правило, искусственной системе или технологическом процессе) и предназначенная для поддержки принятия решений по оперативному управлению этим объектом.

Современные наиболее перспективные подходы синтеза СОТМ, предназначенных для использования в АСУ различного назначения, характеризуется следующими общими принципами:

– применение многоуровневой архитектуры, основанной на декомпозиции решения прикладных задач (сбора, обработки, хранения и предоставления пользователю информации) и распределения вычислений, связанных с этими задачами, между программными компонентами;

– использование нескольких баз данных, предназначенных для хранения результатов вычислений и внутрипрограммного представления информационной модели предметной области (или ее фрагмента) на разных уровнях архитектуры;

– применение стандартных и специфичных для этой СОТМ протоколов взаимодействия для обмена данными между программными компонентами и взаимодействия с системами хранения данных;

– применение разнообразных языков конфигурирования программных компонентов (ПК) для ограниченной адаптации к условиям применения на этапе ввода в эксплуатацию и поддержки применения;

– применение автоматизированных средств разработки программного обеспечения для наращивания функциональности и адаптации к изменениям в условиях применения.

С точки зрения применения метауправления функциональностью ИС [1] наибольший интерес представляют два последних принципа, которые в большинстве современных СОТМ имеют не системный характер и, как правило, их реализация может быть усовершенствована и унифицирована.

Метауправление функциональностью (МУФ) – это информационная технология, предназначенная для автоматизации процессов адаптации ИС к меняющимся условиям применения и продления ее жизненного цикла.

Исследование приемов и способов реализации МУФ при разработке ряда ИС (в том числе СОТМ) различного назначения, позволило сформировать предлагаемую методику синтеза СОТМ с МУФ. Структура методики приведена на рисунке (см. ниже).

С точки зрения методологии МУФ процедура синтеза СОТМ S_{COTM} может рассматриваться как разработка ее архитектуры M_{COTM}, программы адаптации (ПА) к изменениям условий применения и языка описания функциональности (ЯОФ).

Архитектура СОТМ (M_{COTM}) представляет собой формальное описание декомпозиции прикладных задач, решение которых возложено на СОТМ, распределенное по N ПК ($A_{n=[1..N]}$). Для K из N ПК задана база данных ($B_{k=[1..K]}$), которые требуют длительного хранения, либо не могут быть полностью загружены в оперативную память. Для всех ПК определены оптимальный набор P правил информационного взаимодействия ($I_{p=[1..P]}$), таким образом, что $K < P < 2N - 1 + K$.

Программа адаптации – совокупность правил, применяющихся для адаптации СОТМ к заданному множеству ситуаций, которые могут возникнуть на этапе поддержки применения.

Язык описания функциональности – предметно-, либо событийно-ориентированный язык, предназначенный для автоматической обработки ПК и описывающий процедуру изменения функциональности СОТМ, соответствующую новым условиям применения и учитывающую ранее накопленные функциональные изменения.

Процедура синтеза СОТМ начинается с анализа целей ее создания ($G_{\text{ц}}$), требований ($G_{\text{Т}}$), предъявляемых заказчиком (постановщиком задачи), и допустимых затрат ($G_{\text{З}}$) на ее разработку, представленных в виде формулировок общего вида (эвристик). Уже на этом этапе можно сделать предположение о перспективах применения СОТМ. Такое предположение может существенно сэкономить время, деньги и силы в дальнейшем.

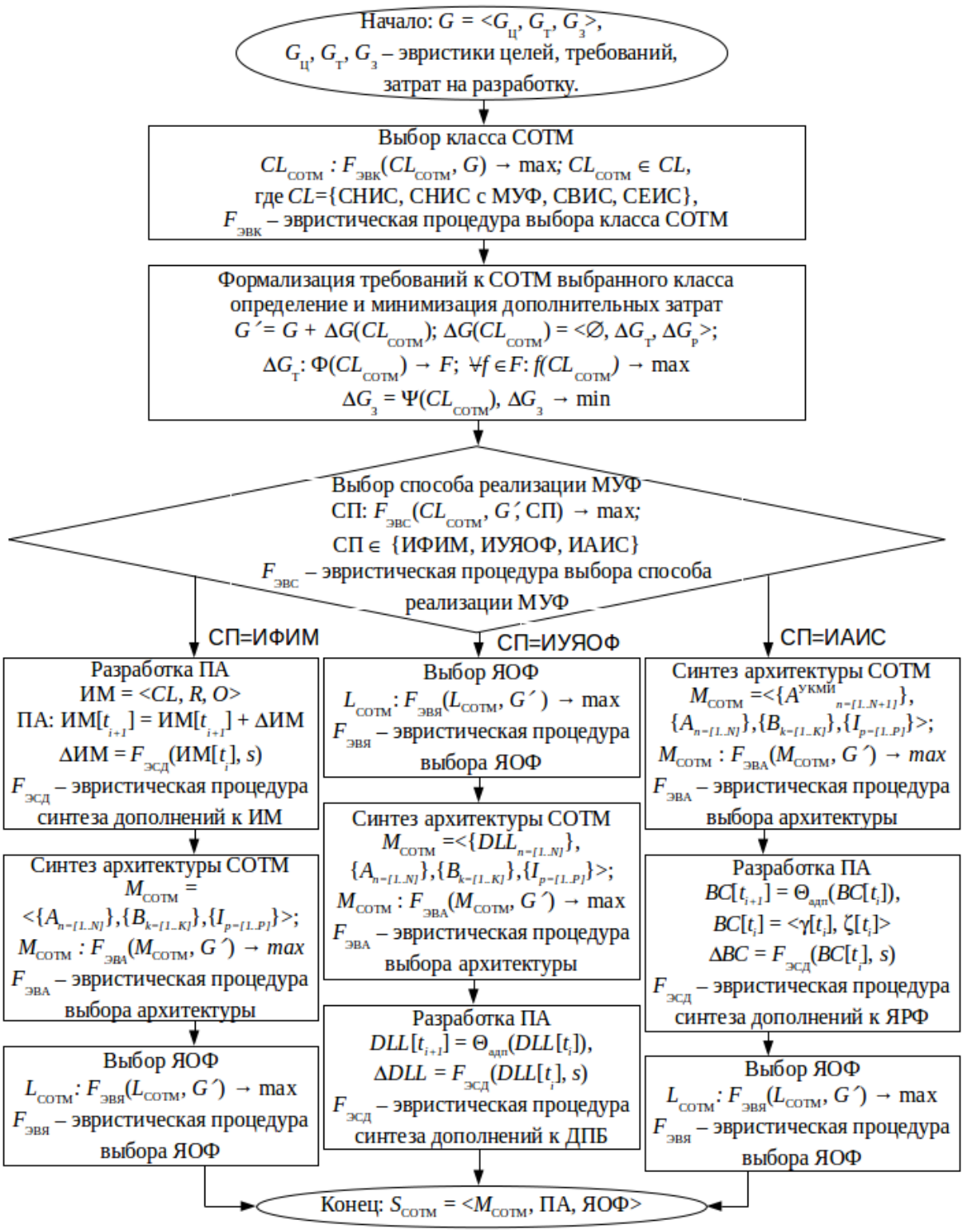


Рисунок. Структура методики синтеза СОТМ с МУФ

Большинство искусственных систем или технологических процессов характеризуются постоянным совершенствованием, которое обусловлено непрерывно происходящим техническим прогрессом. По этой причине рано или поздно наступает момент, когда требуется внести изменения в не-

которые ПК СОТМ, где будут учтены новые условия применения. Для снижения рисков, связанных с необходимостью внесения изменений в ПК и повторного развертывания СОТМ, применяются принципы реализации многоуровневой архитектуры с возможностью замены отдельных ПК и принципы реализации языков конфигурирования.

Однако эти принципы противоречивы, т. к. изменение конфигурации отдельного ПК может приводить к необходимости реконфигурирования всех ПК, с которыми он взаимодействует вплоть до верхнего уровня архитектуры. В результате сложность и стоимость адаптации СОТМ становится на столько высока, что убытки или вред, наносимые ее простоем из-за сложности конфигурирования, становятся сравнимы с ее повторным развертыванием или работкой и развертыванием новой СОТМ. Это особенно критично для экстренных ситуаций, когда время становится особенно дорогостоящим ресурсом.

Особенности конфигурирования разрабатываемой СОТМ могут варьироваться от простых (установил и работай) до сложных («обучить» ПК с нуля работе с новой предметной областью). При этом и ошибки в конфигурации могут иметь разную цену исправления (от простой замены значения конфигурационного параметра в случае внесения неверного значения до повторного «обучения» в случае образования ложной нейронной связи) и серьезные последствия (вред человеческой жизни).

Недооценка и переоценка рисков, связанных изменениями в условиях применения, а также рисков, связанных с применением описанных выше механизмов, могут также иметь серьезные последствия. По этой причине важным моментом является выбор класса ИС, к которому будет относиться СОТМ (CL_{COTM}), и обосновать сделанный выбор. Методология МУФ вводит следующую классификацию ИС:

– синтаксически неизменная ИС без МУФ – ИС, функциональная адаптация которой не осуществляется, либо осуществляется с помощью программирования и повторного развертывания этой ИС;

– синтаксически неизменная ИС с МУФ – ИС, в которой с временем должны меняться отдельные прикладные алгоритмы (например, меняется точность вычислений отдельных величин);

– синтаксически вариантная ИС – ИС, в которой со временем меняется множество прикладных типов данных и алгоритмов их обработки;

– семантически вариантная ИС – ИС, цеди применения которой меняется со временем.

Обычно разработка любого из перечисленных классов обычно требует дополнительных затрат, которые не были учтены на этапе постановки задачи ($\Delta G_З$). Эти затраты могут быть обоснованы и минимизированы за счет положительного эффекта, привносимого реализацией МУФ.

Реализация МУФ также требует разработки дополнительных требований (ΔG_T), которые не были учтены на этапе постановки задачи (например, требования эргономичности и безопасности ЯОФ, защищенности конфигурации, целостности данных и т. п.). Эти требования должны быть особенно тщательно составлены и проанализированы для достижения максимального эффекта и оценки рисков.

После того как все требования проанализированы, риски оценены и принято решение о создании СОТМ выбранного класса, необходимо осуществить выбор способа, с помощью которого будет реализовано МУФ. Исследование показало, что основными являются следующие три способа:

1. Реализация МУФ с использование формализма информационной модели предметной области (ИФИМ), которая применяется во многих современных средствах разработки. Архитектура такой СОТМ создается за счет генерации заготовок программного кода, который дорабатывается программистами. В качестве ЯОФ выбирается псевдокодовый или графический (например, UML) язык. ПА такой СОТМ представляет собой рекомендации по ее доработке и конфигурированию. Этот способ отличается высокой скоростью разработки и доработки, но не является достаточно эффективным на этапе применения, поскольку адаптация СОТМ ограничена информационной моделью предметной области, а все другие изменения требуют переработки ПК и денежных вложений;

2. Второй способ связан с использованием универсального ЯОФ, в качестве которого выбирается интерпретируемый язык общего назначения. Программа-интерпретатор выбранного ЯОФ используется в качестве основы всех ПК и дополняется динамически подгружаемыми модулями (*DLL*), которые используются для адаптации к условиям применения. Архитектура такой системы – это множество интерпретаторов ЯОФ ($A_{[1..N]}$) и правил взаимодействия между ними ($I_{[1..P]}$). Программа адаптации – формализованный способ изменения множества *DLL*. Достоинствами Способа является высокая гибкость СОТМ по отношению к условиям применения, переносимость, эргономичность и однообразие ЯОФ всех ПК. Недостатки: сложность конфигурирования СОТМ с многоуровневой архитектурой и поддержания целостности данных.

3. Третий способ ориентирован на использование унифицированной архитектуры СОТМ. Его основными особенностями является оценка эффективности архитектуры, направлений адаптации и необходимости реализации механизмов адаптации для всех ПК. Архитектура такой СОТМ представляется в виде множества ПК, для каждого из которых указано наличие или отсутствие блока адаптации ($A^{(\text{КМИ})}{}_{[1..N]}$). ПА такой СОТМ описывает ситуации, когда ожидается необходимость в МУФ. После того, как ПА разработана, для каждого ПК, где ожидается применение МУФ,

выбирается комплект ЯОФ, которые будут использоваться для адаптации. Достоинствами способа – простота конфигурирования СОТМ с архитектурой любой сложности, сильная поддержка целостности и эргономичность ЯОФ. Недостатки – уникальность и непереносимость СОТМ, невозможность изменить набор направлений адаптации, сложность и дороговизна разработки.

Комбинация и обоснованность применения перечисленных способов может позволить получить переносимую, надежную СОТМ, которая сможет быть оперативно адаптирована к любым изменениям в условиях применения.

Список используемых источников

1. Шерстюк Ю. М. Основы метауправления функциональностью в информационных системах. СПб. : СПИИРАН, 2000. 155 с.

Статья представлена научным руководителем, доктором технических наук, доцентом Ю. М. Шерстюком

УДК 004.382.4+004.457+004.453.4

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ МИКРОКОМПЬЮТЕРА RASPBERRY PI В ЭФФЕКТИВНОЙ ЦИФРОВИЗАЦИИ НА ПРИМЕРЕ КАЗАХСТАНА

А. Б. Оспанова, Б. И. Тулеуов

Евразийский национальный университет им. Л. Н. Гумилева

Рассмотрен популярный среди разработчиков одноплатный компьютер Raspberry Pi. Предложены и описаны исследовательские проекты на основе моделей Raspberry Pi 3 Model B и Raspberry Pi Zero, предоставляющие на взгляд авторов рациональные решения в сферах деятельности, требующих использования специализированного программно-аппаратного обеспечения либо значительных аппаратно-вычислительных ресурсов.

Raspberry Pi, (одноплатный) микрокомпьютер, мобильное (автоматизированное) рабочее место специалиста, аппаратно-вычислительные ресурсы, универсальный компьютерный класс.

Одноплатные компьютеры Raspberry Pi [1] сразу после появления стали очень популярны среди разработчиков в мире, что обусловлено их достоинствами: маленькие размеры (плата соразмерна с банковской картой); характеристики CPU; наличие портов для комплектации дополнительными устройствами (USB, GPIO, HDMI, MicroSD и др.); гибкие возможности оснащения дополнительными платами расширения; доступность различных операционных систем; загрузка с ISO-образа на карте памяти; поддержка разрешения FullHD; ценовая доступность (стоимость платы составляет порядка $35). Такие особенности делают Raspberry Pi в большой мере полезным в обучающих, исследовательских, экспериментальных целях.

Предлагаемые проекты на основе Raspberry Pi

Предлагаются разработки, выполненные на основе Raspberry Pi модели 3 B, которая пока остается самой мощной моделью по техническим характеристикам, а также на основе Raspberry Pi Zero, преимуществом которого является минимальное оснащение и еще меньшие размеры. В Raspberry Pi 3 присутствуют интерфейсы Ethernet, RCA, HDMI, 4 разъема USB, MicroUSB, IIC, SPI, CSI, GPIO, UART, JTAG; есть поддержка Wi-Fi и Bluetooth, а также Pi 3 имеет новый процессор. Raspberry Pi Zero оснащен слотом для карт microSD, портом mini-HDMI, Micro-USB (2), GPIO.

Представляемые проекты можно разбить на 3 группы (табл. 1).

ТАБЛИЦА 1. Предлагаемые проекты и их общие идеи

Общее название группы проектов	Общая идея группы проектов
А. Портативное автоматизированное рабочее место специалиста	Предоставляют рациональные решения в сферах деятельности, требующих использования специализированного программного обеспечения и постоянного неограниченного доступа к нему
Б. Многопрофильный бюджетный компьютерный класс и специализированная лаборатория	Предоставляют рациональные решения в организации практических занятий по дисциплинам, требующим использования специализированного программного обеспечения (2), либо значительных аппаратных (4.1, 4.5, 4.6) и вычислительных ресурсов (4.2–4.5), либо лабораторные практикумы сопряжены с рисками для аппаратного оборудования и программного оснащения (4.1, 4.2, 4.5)
В. Специализированные программно-аппаратные устройства, защищенные от несанкционированного доступа	Предоставляют решения в сферах деятельности, требующих разработки специализированного программного и аппаратного обеспечения с применением технических методов защиты информации

Далее даны описания проектов. Некоторые из предлагаемых проектов авторами реализованы полностью или частично и используются в частной и профессиональной деятельности.

Проект 1. Портативное автоматизированное рабочее место специалиста по сетевой безопасности с поддержкой принятия решений

Создание аппарата размером с банковскую карту с дисплеем, улучшенным беспроводным модулем на базе дистрибутива Kali Linux. Это программно-аппаратное устройство вкупе с разработанным руководством пользователя и учебными пособиями будет являться гибким инструментом специалиста по сетевой безопасности. Разработанное программное обеспечение и интеллектуальная система с поддержкой принятия решений позволят выполнять штатные задачи по обеспечению сетевой безопасности пользователям, не имеющим специализированных глубоких знаний или большого практического опыта в данной области.

Проект 2. Учебно-исследовательская лаборатория для проведения исследований и практических работ по криптографии и криптоанализу

Изучение практической криптографии и методов криптоанализа. Создание устройства с предустановленным специализированным программным обеспечением, необходимым для исследований и проведения практических работ по криптографии и криптоанализу позволит иметь «мобильную» оборудованную лабораторию без привязки к определенному помещению или компьютерному классу. Рабочее окружение состоит из следующих компонентов. Установленные и настроенные необходимые утилиты, компиляторы и интерпретаторы (для *Windows*, это могут быть, например, MinGW, Python, двоичный редактор, специальные библиотеки для языков программирования), разработанные управляющие скрипты, математические пакеты. Реализации классических и современных криптографических алгоритмов, математических операций, необходимых в криптографии (теория делимости, модульная арифметика, теория простых чисел, алгебраические структуры и др.) с использованием криптографических библиотек и без них, библиотек для работы с большими числами и без них, методов параллельного программирования и без них, с использованием математических пакетов. Реализации криптографических атак (в том числе, по материалам и публикациям современных криптоаналитиков). Специализированная электронная библиотека с рекомендованными источниками.

Проект 3. Мобильное автоматизированное рабочее место специалиста, нуждающегося в специализированном программном обеспечении конкретных версий и изданий по требованию

Создание аппарата размером с банковскую карту с отказоустойчивым предустановленным рабочим окружением для выполнения индивидуальных специализированных задач.

Проект 4. Многопрофильный универсальный компьютерный класс для проведения дисциплин, требующих значительных вычислительно-

аппаратных ресурсов, либо практические занятия по данным дисциплинам сопряжены с рисками для аппаратного и программного оснащения

4.1. Изучение схемотехники, электроники, аппаратного устройства электронно-вычислительных машин, робототехники и т. п.

4.2. Изучение в рамках дисциплины «Методы и средства защиты информации» вредоносного программного обеспечения (анализ, дизассемблирование и т. п.).

4.3. Изучение суперкомпьютеров и вычислительных кластеров.

4.4. Изучение распределенных систем и параллельное программирование с использованием MPI на различных операционных системах.

4.5. Изучение операционных систем.

4.6. Изучение компьютерных сетей.

Проект 5. Аппаратно-программное устройство с защищенной как на аппаратном уровне, так и с помощью программных средств системой проверки знаний

Организация эффективной системы для объективной проверки знаний по сей день остается актуальной задачей. В рамках данного проекта предлагается механизм проведения среза знаний (к примеру, проводимых в Казахстане ВОУД, ЕНТ) с использованием устройства со специально разработанным программным обеспечением на основе модифицированного Raspberry Pi Zero. Проект предполагает аппаратные и программные разработки, а также создание соответствующей документации.

Проект 6. Аппаратно-программное устройство с защищенной как на аппаратном уровне, так и с помощью программных средств системой передачи данных

Организация эффективной системы для передачи секретной информации также является актуальной задачей. В рамках данного проекта предлагается механизм обмена секретной информацией с использованием устройства со специально разработанным программным обеспечением на основе модифицированного Raspberry Pi Zero. Проект предполагает аппаратные и программные разработки, а также создание соответствующей документации.

О реализации проектов 1–6

Авторы создали опытный образец устройства на основе Raspberry Pi 3 с локальным подзаряжаемым источником питания, TFT дисплеем диагональю 3,5 дюйма с операционными системами Kali Linux и Windows – см. рис.

Рисунок. Работающее устройство Raspberry Pi 3

Далее в таблице 2 дано описание конфигурации устройства на рисунке. Подробное описание других конфигураций и рекомендации по сборке есть в [1].

ТАБЛИЦА 2. Конфигурация устройства по проектам групп А) и Б) (см. табл. 1)

1	Raspberry Pi 3 B
2	Плата расширения с локальным источником питания на 3,7 V, 2500 mAh
3	Карта MicroSD с предустановленной операционной системой (8 Гб и 32 Гб)
4	Сенсорный TFT дисплей с диагональю 3,5 дюймов
Дополнительно имеются миниклавиатура USB, USB мышь, дисплей с HDMI выходом и диагональю 12 дюймов, адаптер питания 5 V, 2,5 A	

По проекту 1 разработанное устройство практически готово к использованию. Необходимо создание программного рабочего окружения, загрузочного диска и руководства пользователя.

Проект 2 внедрен в учебный процесс (ведется преподавание дисциплины «Криптоанализ с помощью программных средств» в магистратуре по специальности «Системы информационной безопасности»). На данный момент имеется один экземпляр устройства с настроенным рабочим окружением, состоящим из необходимых утилит (в том числе разработанных авторами) и математических пакетов.

Проект 3 предполагает наличие заказов по требованиям конкретных специалистов, а также разработку готовых аппаратов и/или загрузочных дисков с рабочим окружением на основе предварительно проведенного анализа рынка потенциальных потребителей.

Реализация проектов группы Б) в основном заключается в аппаратных сборках (кроме 2)) и не представляет каких-либо трудностей при наличии необходимых комплектующих.

Заключение

В работе предложены исследовательские проекты на основе одноплатного компьютера Raspberry Pi. Даны описания проектов, выделены шаги реализации и их содержание по каждому из предлагаемых проектов, а также приведены результаты по некоторым частично или полностью реализованным проектам.

Список используемых источников

1. Официальный сайт Raspberry Pi. URL: https://www.raspberrypi.org/
2. Оспанова А. Б. Инструменты сетевой безопасности на основе микрокомпьютера Raspberry Pi // Труды IV международной научно-практической конференции «Интеллектуальные информационные и коммуникационные технологии – средство осуществления третьей индустриальной революции в свете стратегии «Казахстан–2050», Астана. 2017. С. 380–382.

УДК 004.5

ПРИМЕНЕНИЕ НЕЙРОКОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ ДЛЯ УПРАВЛЕНИЯ ПЕРЕДВЕЖНОЙ ПЛАТФОРМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ю. Н. Островский, С. А. Тиридатов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматриваются вопросы, связанные с применением нейрокомпьютерных интерфейсов для управления передвижной платформой специального назначения, основанных на распознавании действий, мысленно представляемых военнослужащим. Приведена общая структура с этапами сбора и обработки сигнала ЭЭГ, а также обоснование выбора аппаратной части.

нейрокомпьютерный интерфейс, мозг-компьютер, передвижная платформа, драйвер электродвигателей, аппаратура радиоуправления.

Нейрокомпьютерный интерфейс (НКИ) – (англ. *Brain-Computer Interface*, BCI) является системой коммуникации человека с электронным устройством (например, с компьютером, тренажерно-обучающим ком-

плексом, экзоскелетом, протезом, роботизированным комплексом, летательным аппаратом), основанной на непосредственном преобразовании намерений человека, отраженных в биопотенциалах мозга, в управляющие команды.

Интерфейс мозг-компьютер (ИМК), он же нейроинтерфейс – это технология, позволяющая обрабатывать электрические сигналы с коры головного мозга, усиливать и передавать их на компьютер, далее с помощью алгоритмов обработки происходит синхронизация с любым управляющим устройством или компьютерным приложением [1].

В качестве аппаратного обеспечения был выбран НКИ компании Нейроботикс. Для работы с нейрокомпьютерным обеспечением необходим биоусилитель, ЭЭГ-шапочка (рис. 1) и соответствующее программное обеспечение для съёма сигналов с биоусилителя CyborgInteraction (рис. 2). Наиболее удобным и мобильным (носимым) является Нейробелт, его технические характеристики:

1. 8 каналов регистрации ЭЭГ.
2. беспроводной передача по Bluetooth до 10 м.
3. частота опроса 122 Гц.
4. длительность непрерывной работы не менее 8 часов.
5. Вес 50 г.
6. Поддерживаемые операционные системы Windows 8.1/10.

Рис. 1. ЭЭГ-шапочка компании Нейроботикс

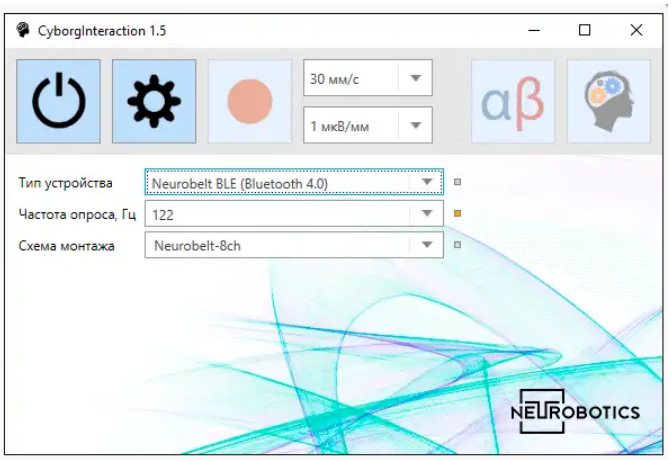


Рис. 2. ПО для съёма сигналов с биоусилителя CyborgInteraction

НКИ в системе специального назначения применяется для управление когнитивным состоянием военнослужащего с помощью биологической обратной связи, решение ситуационных задач, тактических, дистанционное управление объектами [2].

НКИ в системе специального назначения применяется для управление когнитивным состоянием военнослужащего с помощью биологической об-

ратной связи, решение ситуационных задач, тактических, дистанционное управление объектами [3].

В качестве дистанционно управляемого объекта предполагается разработка передвижной платформы специального назначения, обладающая рядом характеристик:

– грузоподьемность – 80–100 кг;
– дальность управления (пилотного макета) – 10–30 м;
– скорость движения – 5–15 км/ч;
– время автономной работы – 2–3 ч.

Разработка проекта разделена на два основных этапа. В рамках первого этапа требуется разработать программно-аппаратную составляющую передвижной платформы специального назначения используя стандартные методы управления и контроля моделями по средством управления при помощи пульта радиоуправления.

Второй этап разработки заключается в смене стандартных средств контроля моделями на управление при помощи нейрокомпьютерного интерфейса.

Для реализации первого этапа был проведен анализ необходимых комплектующих:

– выбор аппаратуры радиоуправления;
– выбор драйвера (контроллера) электродвигателей.

Главными компонентами аппаратуры управления являются передатчик (пульт управления) и приемник радиосигнала [4].

Передатчики бывают двух основных типов, пистолетный с рычагом ускорения и колесом управления (обычно используются для автомоделей и судомоделей), а также рычажного типа, с многопозиционными тумблерами (чаще используются для авиамоделей).

Второй частью аппаратуры радиоуправления является приемник радиосигнала, который устанавливается непосредственно на модели. К приемнику подключаются все исполнительные устройства и механизмы – регуляторы скорости, электромагниты, серво машинки, электромагниты и прочие.

Для каждого вида модели (авто, авиа, судо) устанавливается своя необходимая дальность действия. Так для авиамодели необходимая дальность находится в диапазоне от 1000 до 2000 метров. Для авто и судомоделей дальность действия аппаратуры значительно меньше от 50 до 200 метров с точки зрения видимости модели.

Производством аппаратуры для радиоуправления на данный момент занимается всего несколько фирм. Наиболее распространёнными являются трех, четырех и шести канальные системы.

Драйверы электродвигателей часто используются в RC- аппаратуре. Данные устройства позволяют преобразовывать сигналы слаботочных управляющих контроллеров в более мощный сигнал, которым будет управляться сам электродвигатель. При этом, напряжение питания электродвигателя не играет никакой роли. На данный момент ведущими компаниями по разработке драйверов электродвигателей являются: Fairchild, Sanyo, ST Microelectronics, Toshiba, Texas Instruments, Rohm. Драйверы электродвигателей постоянного тока, выпускаемые данными компаниями, подразделяются на три вида [5]:

– управления одним электродвигателем;

– управления двумя электродвигателями постоянного тока без стабилизации скорости;

– управления одним электродвигателем постоянного тока с функцией стабилизацией тока.

Для выбора драйвера нужно знать необходимое напряжение питания и мощность электродвигателя, что связано с напряжением питания выходного блока, максимальным выходным током и рассеиваемой мощностью. Помимо этих характеристик пользователь должен определить необходимость наличия таких дополнительных функций, как термозащита (отключение при перегреве), энергосбережение, выбор диапазона выходного напряжения и возможность одновременной работы с регулятором скорости.

На рис. 3 представлены три основные структурные схемы, соответствующие видам драйверов постоянного тока.

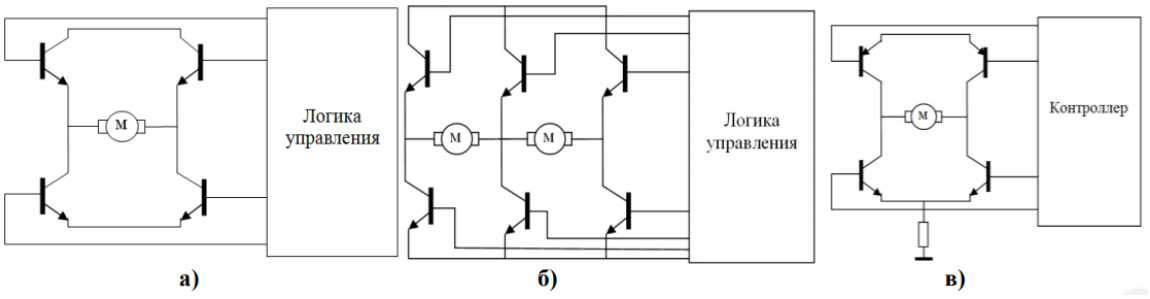


Рис. 3. Структурные схемы: а) драйверы одного электродвигателя постоянного тока; б) драйверы двух электродвигателей постоянного тока; в) драйверы электродвигателя постоянного тока с регулятором скорости.

Для перехода ко второму этапу разработки необходимо устранить ключевую проблему, без решения которой невозможно управление внешними устройствами в нейрокомпьютерном интерфейсе, является отсутствие быстрого, надежного по содержанию канала обратной связи. Для решения данной проблемы будет реализована структурная схема ИМК, приведенная на рис. 4.

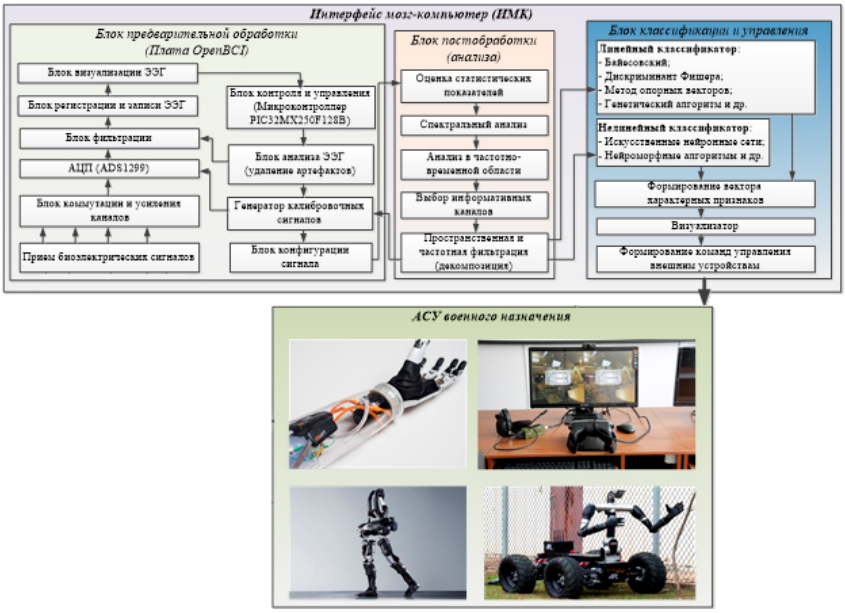


Рис. 4. структурная схема ИМК

Для разработки аппаратно-программного комплекса ИМК военного назначения, требуется проведение глубоких фундаментальных исследований, в том числе сопровождающих различные движения. Методологической базой таких исследований должны стать представления о системной деятельности мозга.

Список используемых источников

1. Pfurtscheller G., Christa N. EEG-Based Brain-Computer Interfaces // Niedermeyer's Electroencephalography: Basic Principles, Clinical Applications, and Related Fields / edited by D. L. Schomer, H. L. S. Fernando. 6th. Philadelphia, Pa.: Lippincott Williams & Wilkins, 2010. PP. 1227–1236. ISBN 978-0-7817-8942-4.

2. Зенков Л. Р. Клиническая электроэнцефалография (с элементами эпилептологии). Руководство для врачей. М. : МЕДпрессинформ, 2004. 368 с.

3. Ганин И. П. Интерфейс мозг-компьютер на волне p300: исследование эффектов повторения и движения стимулов: дис. ... канд. биол. наук: 03.03.01, 03.03.06 / Ганин Илья Петрович. М., 2013. 199 с.

4. Аналоговая система радиоуправления // Радиолюбительский портал «RadiobookA». URL: http://radiobooka.ru/peredatchik/951-analogovaja-sistema-radioupravlenija.html (дата обращения 07.02.2018).

5. Аппаратура радиоуправления моделями // «RC design». URL: http://www.rcdesign.ru/articles/radio/tx_intro (дата обращения 07.02.2018).

Статья представлена начальником НИЦ ВАС, кандидатом военных наук, доцентом В. Э. Гелем.

УДК 602

НЕЙРОКОМПЬЮТЕРНЫЙ ИНТЕРФЕЙС ДЛЯ ОБУЧАЮЩИХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

Ю. Н. Островский, М. Х. Шайсултанов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматривается метод построения программно-аппаратного модуля нейрокомпьютерного интерфейса с биологической обратной связью для повышения эффективности обучающих систем на основе внедрения современных информационных технологий. Приведена общая структура с этапами сбора и обработки сигнала энцефалограммы, а также обоснование выбора аппаратной части.

нейрокомпьютерный интерфейс, биологическая обратная связь, энцефлограмма.

Нейрокомпьютерный интерфейс (НКИ) (называемый также прямой нейронный интерфейс, мозговой интерфейс, интерфейс «мозг – компьютер») – устройство или принцип работы, предназначенный для обеспечения односторонней или двухсторонней связи между мозгом и электронным устройством[1]. В данной статье рассматривается нейрокомпьютерный интерфейс для обеспечения двухсторонней связи на основе биологической обратной связи (БОС).

Нейрокомпьютерный интерфейс с биологической обратной связью реализуется посредством внешней цепи обратной связи, организованной преимущественно с помощью микропроцессорной или компьютерной техники (рис. 1).

Одно из самых перспективных направлений развития нейрокомпьютерного интерфейса(НКИ) является медицина. НКИ позволит создавать протезы с высокой отзывчивостью, манипулировать подобного рода протезами можно будет наравне с здоровыми органами. Вопросами создания и имплантирования различных искусственных устройств для восстановления нарушений функций нервной системы и сенсорных органов занимается область неврологии – нейропротезирование. Самым распространенным нейропротезом является кохлеарный имплантат, который используется для компенсирования потери слуха некоторым пациентам с выраженной или тяжёлой степенью нейросенсорной (сенсоневральной) тугоухости. Однако медицинские НКИ могут найти применение не только в медицине. На основе данных технологий возможно создать эффективные обучающие системы. Применение таких методов имеет ряд преимуществ, например,

такие как повышение интереса обучаемого к процессу обучения и качества обучения в целом, снижение степени травматизма обучаемого за счёт исключения механической составляющей и взаимодействия с ней, повышение скорости получения первичных навыков и знаний и т. д.

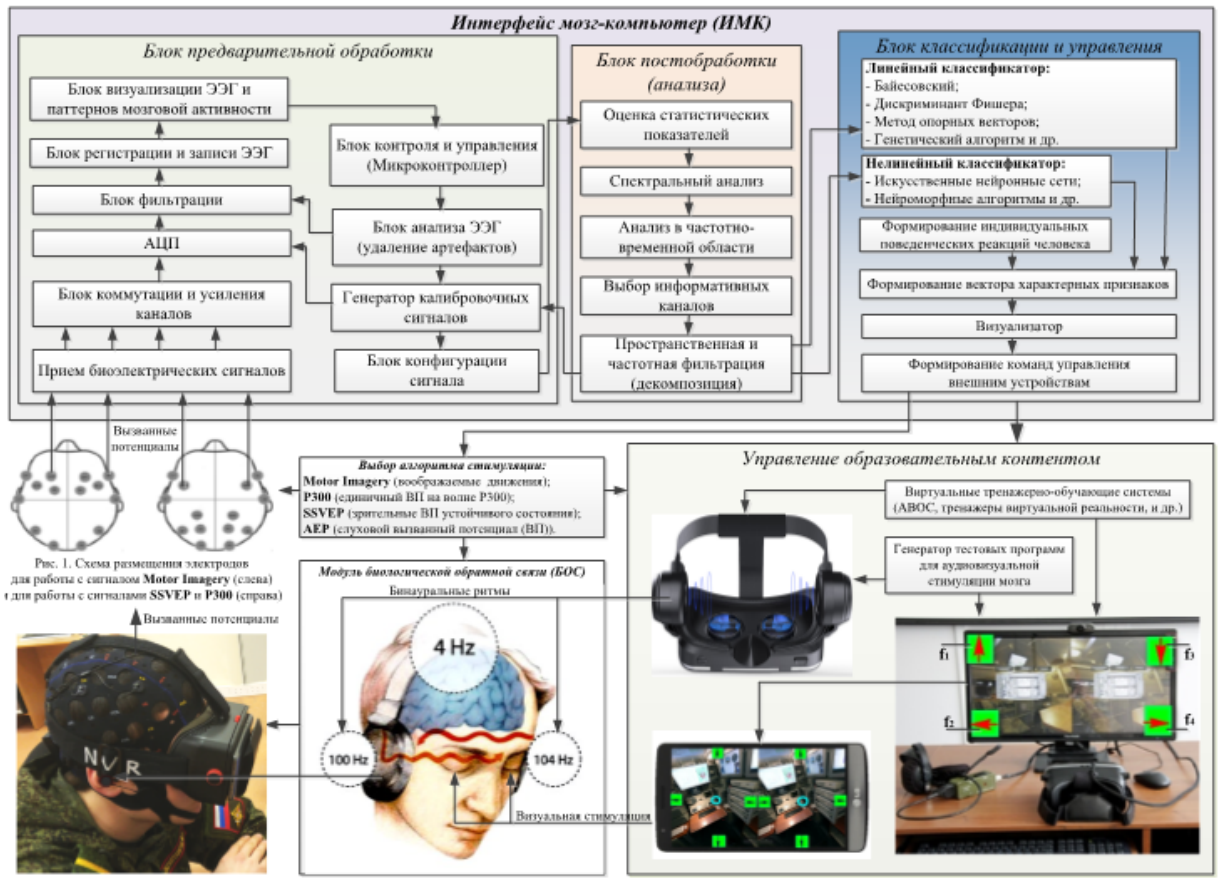


Рис. 1. Схема построения интерфейса мозг – компьютер с использованием БОС

На рис. 1 представлена схема работы нейрокомпьютерного интерфейса, которая состоит из трех блоков:

– предварительной обработки;
– постобработки;
– классификации и управления.

Для решения проблемы предварительной обработки и постобработки сигналов головного мозга используется шлем Нейробелт EEG-8BG (рис. 2).

Данный НКИ позволяет регистрировать сигналы с коры головного мозга при помощи 8 датчиков с частотой опроса 120 Гц. Пример визуализации сигналов с использованием программы Cyberinteraction представлен на рис. 3.

Рис. 2. Нейрокомпьютерный интерфейс «Нейробелт»

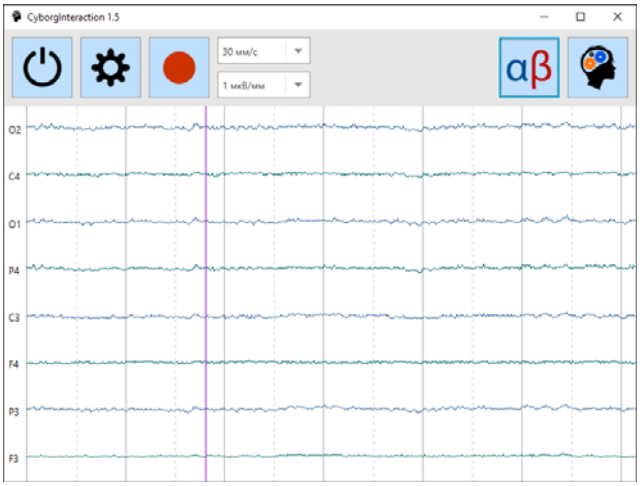


Рис. 3. Графики ЭЭГ

В качестве модуля биологической обратной связи используются очки в которых транслируется визуальный сигнал с алгоритмом стимуляции SSVEP.

SSVEP (*steady state visually evoked potentials* — соматосенсорные вызванные потенциалы) – это сигналы, которые головной мозг генерирует в ответ на визуальную стимуляцию. Когда сетчатка глаза возбуждается вспышками частотой от 3,5 до 75 Гц, мозг генерирует электрическую активность с такой же частотой, с которой мигают вспышки [2].

SSVEPs обычно варьируются от 5 до 60 Гц, интервал зависит от индивидуальных психофизиологических особенностей. Сигнал регистрируется при помощи электроэнцефалографии, запись ЭЭГ происходит со скальпа [2].

Восприятие зрительной системой мигающего света на определённой частоте стимулирует зрительный путь и заставляет всю систему включая мозг, работать на такой частоте. При стимуляции, мозг генерирует электрические сигналы на стимулирующих частотах, а также на частотах, кратных стимулирующим. Например, если человек смотрит на вспышку, которая мигает с частотой 5 Гц, его мозг будет генерировать частоты, равные 5 Гц, 10 Гц и 15 Гц и т. д. [2]. На рис. 4 представлен принцип работы SSVEP.

Для решения проблемы классификации и управления в качестве аппаратного комплекса выбран одноплатный компьютер Raspberry Pi 3b (рис. 5). Блок классификации и управления реализует основные математические алгоритмы (аппарат) распознавания мыслительной деятельности с последующим формированием команд управления внешним устройствам. Построение классификатора предполагает реализацию, как линейных

классических математических моделей, так и нелинейных адаптивных алгоритмов, и моделей.

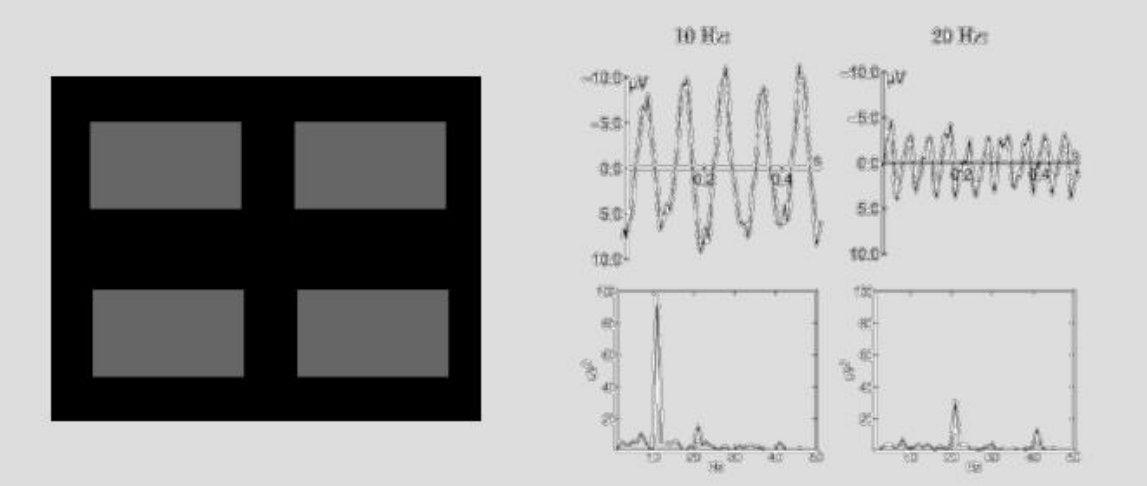


Рис. 4. Слева изображены четыре области, которые поочередно мигают с частотой 10 Гц и 20Гц. Сигналы с частотой 10 Гц и 20Гц (сверху), спектры сигналов с частотой 10 Гц и 20Гц (снизу).

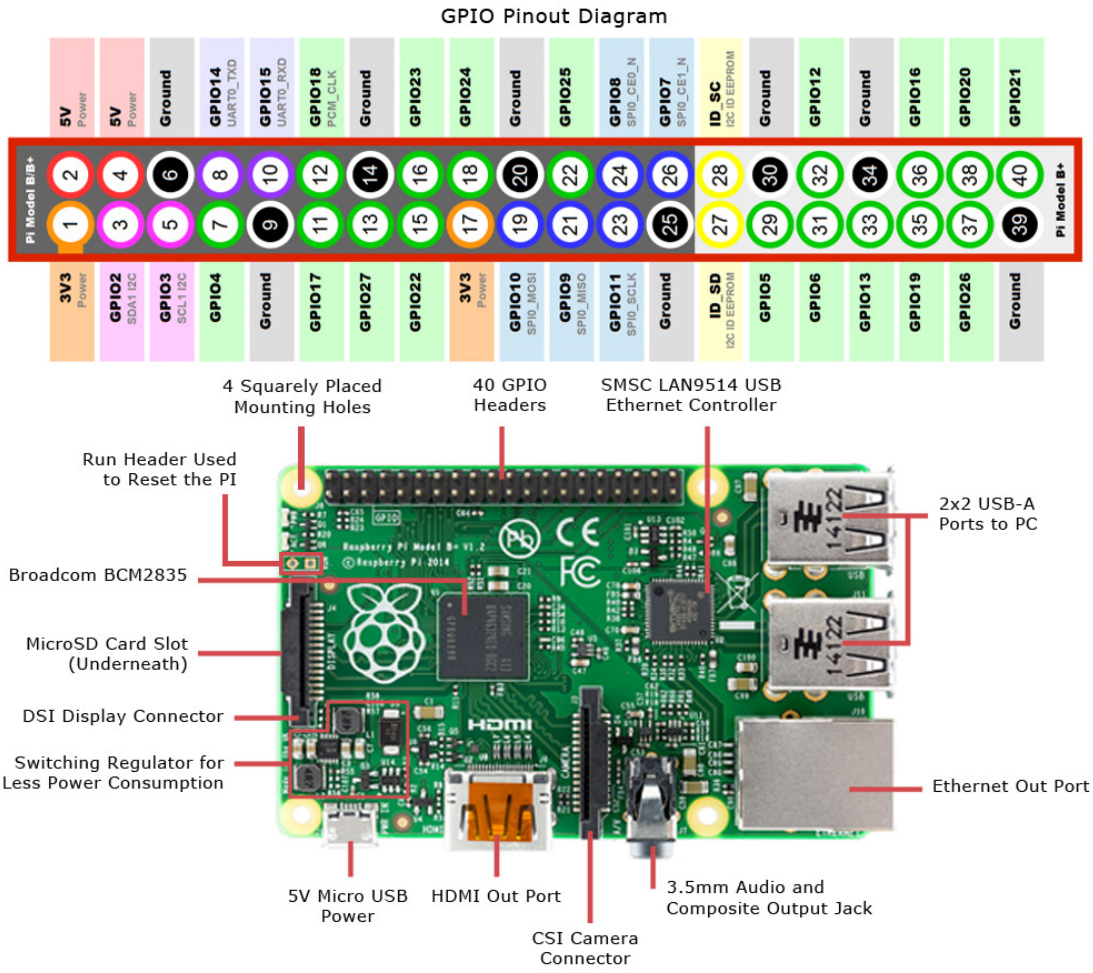


Рис. 5. Одноплатный компьютер Raspberry Pi

Для разработки программно-аппаратного модуля нейрокомпьютерного интерфейса с биологической обратной связью, требуется проведение глубоких фундаментальных исследований, направленных на понимание механизмов формирования пространственно-временных паттернов ЭЭГ, в том числе сопровождающих различные движения. В данной статье продемонстрированы этапы построения такого модуля с применением алгоритма стимуляции SSVEP.

Список используемых источников

1. https://geektimes.ru/post/241240/
2. https://ru.wikipedia.org/wiki/SSVEP
3. Pfurtscheller G., Christa N. EEG-Based Brain-Computer Interfaces // Niedermeyer's Electroencephalography: Basic Principles, Clinical Applications, and Related Fields / edited by D. L. Schomer, H. L. S. Fernando. 6th. Philadelphia, Pa.: Lippincott Williams & Wilkins, 2010. PP. 1227–1236. ISBN 978-0-7817-8942-4.
4. Pfurtscheller G., McFarland D. J. BCIs that use sensorimotor rhythms // Brain-Computer Interfaces: Principles and Practice / edited by J. R. Wolpaw, E. W. Wolpaw. Oxf.: Oxford University Press, 2012. PP. 227–240. ISBN 978-0-19-538885-5.

Статья представлена начальником НИЦ ВАС, кандидатом военных наук, доцентом В. Э. Гелем.

УДК 004.056.5

АНАЛИЗ СОСТОЯНИЯ ИССЛЕДОВАНИЙ ПО МОДЕЛИРОВАНИЮ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

О. И. Пантюхин[1], И. Б. Паращук[2, 3], И. Б. Саенко[2, 3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[3]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В статье предложены систематизированные результаты детального анализа состояния исследований в предметной области разграничения доступа к информации с учетом специфики, свойственной облачным системам хранения данных, являющихся компонентами критически важных информационных систем. Приведены результаты

анализа состояния исследований в области применения методов искусственного интеллекта для оптимизации, верификации и реконфигурации политик разграничения доступа. Использование результатов данного анализа позволит повысить обоснованность принимаемых решений в области разработки и применения перспективных моделей контроля доступа с целью выяснения возможностей и способов их реализации в облачных инфраструктурах.

критически важная система, информационная система, политика разграничения доступа, облачная инфраструктура, информационная безопасность.

В соответствии с действующим «Перечнем приоритетных направлений развития науки, технологий и техники Российской Федерации», облачные инфраструктуры критически важных информационных систем и их защищенность относятся к критическим технологиям. К числу ключевых основных тенденций развития облачных инфраструктур относят дальнейшее увеличение их возможностей по обеспечению надежности, безопасности, производительности, управляемости и масштабируемости. Таким образом, вопросы обеспечения безопасности (а разграничение доступа является составной частью безопасности) стоят на одном из первых мест.

Повышение роли и стремительное распространение облачных инфраструктур в критически важных информационных системах, повышение совокупной стоимости активов устройств, программного обеспечения и критически важных данных таких систем, а также увеличение числа атак на них определяют актуальность задач разграничения доступа к информации в облачных инфраструктурах таких систем, а также обнаружения и разрешения конфликтов в используемых ими политиках разграничения доступа.

Облачные инфраструктуры представляют собой сравнительно новый вид компьютерных инфраструктур, которые привлекают к себе повышенное внимание в области информационных технологий и обладают повышенным интересом для потребителей информационных услуг и ресурсов. В то же время многие исследователи отмечают, что более широкому распространенному этой технологии препятствуют проблемы безопасности [1, 2, 3]. Недостатком большинства существующих облачных инфраструктур является отсутствие возможности гибкого управления со стороны пользователей доступом к своим данным, что вызвано универсальностью решений по контролю доступа, принимаемых поставщиками облачных услуг [1]. Многие исследователи отмечают, что неоднородность и большое разнообразие ресурсной среды облачного хранилища требуют всестороннего и детально проработанного механизма управления доступом, чтобы обеспечить динамические, постоянно расширяемые и хорошо настраиваемые требования по защите информации пользователей [2]. Однако существующие механизмы безопасности, обеспечиваемые поставщиками облачной

инфраструктуры, не удовлетворяют этим требованиям [3]. Кроме того, проблем безопасности информации в облачных инфраструктурах обостряются, если используются открытые веб-сервисы. Все это настоятельно требует проработки вопросов совершенствования политик разграничения доступа и моделей, лежащих в их основе.

Моделирование, анализ и практическая реализация компонентов систем разграничения доступа в облачных инфраструктурах критически важных информационных систем очень важна в условиях интеграции, в таких инфраструктурах частных политик разграничения доступа, которые используют разнородные модели контроля доступа с учетом повышенных требований по защищенности таких систем, высокой доступности и производительности. К таким системам относятся критически важные информационные системы, основанные на реализации облачных инфраструктур для хранения данных, применяемые в таких областях, как электроэнергетика, управление мегаполисами и крупными городами, транспорт, включая гражданскую авиацию и Российские железные дороги, системы управления нефтедобывающей и газодобывающей промышленности, банковские и коммерческие системы, образовательные и научные учреждения, средства массовой информации, системы административного управления и другие.

Анализируя модели контроля доступа к информации, которые применяются в облачных инфраструктурах, можно сделать вывод, что наибольшей популярностью обладает модель контроля доступа на основе ролей Role-Based Access Control (RBAC), в дополнение к которой предлагается использовать некоторые более перспективные модели. В [3], кроме RBAC, анализируются и предлагаются к использованию модель контроля доступа на основе атрибутов Attribute-Based Access Control (ABAC) и модель «множественной аренды» (*multi-tenancy*), являющаяся разновидностью модели организационного контроля доступа Organization-Based Access Control (OrBAC). В [1] предлагается использовать основанную на RBAC модель Amazon Web Services (AWS), позволяющую расширить возможности политик RBAC и облегчить интеграцию службы разграничения доступа в корпоративные приложения. В [2] предлагается гибкая междоменная модель разграничения доступа, основанная на механизмах преобразования ролей. В [3] среди анализируемых моделей доступа присутствуют мандатный механизм доступа Mandatory Access Control (MAC) и дискреционный механизм доступа Discretionary Access Control (DAC), но отмечается их низкая эффективность в облачных инфраструктурах. В качестве наиболее приемлемых, предлагается использование моделей RBAC и ABAC. В [1, 3] предлагается реализовать новую парадигму услуг, связанную с разграничением доступа – «контроль доступа как сервис» (*Access Control as a Ser-*

vice) с использованием применяемых в облачных инфраструктурах моделей доступа.

Вопросы моделирования, оценки, формирования и оптимизации политик разграничения доступа в мире в наибольшей степени проработаны для модели RBAC, поскольку она допускает строгую формализацию с выделением переменных, целевой функции и ограничений. Это позволяет выделить задачу оптимизации политики разграничения доступа на основе RBAC в отдельный класс задач интеллектуального анализа данных (*Data Mining*), получившего название Role Mining Problem (RMP) [4]. Разработаны различные варианты постановки этой задачи и предложен ряд методов и алгоритмов их решения [5]. В [6] разработаны простые эвристические алгоритмы, основанные на комбинаторных решениях. Для снижения сложности комбинаторных алгоритмов в [7] предложено использовать вероятностные модели. Однако вероятностный подход не гарантирует высокой точности решения задачи. Подход, основанный на кластерном анализе, предлагается в [8]. Однако это подход требует учета дополнительных параметров, характеризующих бизнес-процессы и потребности пользователей, что не всегда возможно сделать. В [9] предлагается подход, основанный на методах декомпозиции на основе булевых матриц (*Boolean Matrix Decomposition*). Однако, нигде не рассматривается задача реконфигурирования схемы RBAC. Такой же недостаток справедлив для cost-driven подхода, представленного в [10]. При подходе стоимость определяется затратами администрирования. Однако это подход распространяется только на отдельные варианты RMP. В [11] предложены метрики для оценки различных алгоритмов решения задачи проектирования схем RBAC. В качестве более общего подхода для решения задач RMP [12, 13], предлагается использовать генетические алгоритмы. В этих работах показано, что генетические алгоритмы, как и другие алгоритмы биоинспирированной оптимизации, следует рассматривать как достаточно эффективные средства решения задач оптимизации политик разграничения доступа. В работе [14] частично рассматриваются отдельные вопросы, связанные с задачей реконфигурирования схемы RBAC, предложен подход, согласно которому для реконфигурации схемы RMP используются метод access history logs. В [15] предложен подход к верификации политик разграничения доступ, основанный на адаптации различных ситуаций с помощью моделирования уступок, которые пользователи делают, чтобы достигнуть разрешения возможных конфликтов. Этот подход был рассмотрен применительно к социальным системам, однако он представляется применимым для облачных инфраструктур. В [16] для верификации политик разграничения доступа предлагается использование эвристик, которые понижают сложность механизма разграничения доступа.

Таким образом, анализ имеющихся мировых научных и практических подходов к моделированию, оценке, формированию и оптимизации политик разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем, позволяет сделать следующие выводы: проблема разграничения доступа в облачных инфраструктурах вызвана спецификой свойственных им угроз безопасности и является достаточно актуальной; данная проблема обостряется в критически важных информационных системах; решения этой проблемы связывается с использованием наряду с традиционной моделью контроля доступа RBAC новых перспективных моделей ABAC, OrBAC и других, построенных на их основе; разработка новых моделей, методов и алгоритмов для решения задач оценки, оптимизации, верификации и реконфигурации политик безопасности, основанных на моделях контроля доступа, является активно развивающимся научным направлением, в котором использование интеллектуальных методов, в частности генетических алгоритмов, эвристических многоагентных систем и т. д., позволит получить достаточно эффективные решения.

Результаты анализа имеющихся мировых научных и практических подходов к моделированию, оценке, формированию и оптимизации политик разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем, позволят создать новые модели, методы и алгоритмы, нацеленные на повышение уровня информационной безопасности инфраструктур облачного хранения данных и, соответственно, безопасности информации в критически важных информационных системах, использующих облачные инфраструктуры для своего построения, за счет применения средств искусственного интеллекта для совершенствования моделей контроля доступа и разработки на их основе эффективных методов и алгоритмов управления политиками разграничения доступа.

Работа выполнена при финансовой поддержке проекта РФФИ № 18-07-01369, при частичной поддержке бюджетной темы № АААА-А16-116033110102-5, а также при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01).

Список используемых источников

1. Fotiou, N., Machas, A., Polyzos, G.C. Access control as a service for the Cloud // J. Internet Serv. Appl. (2015) 6:11. doi:10.1186/s13174-015-0026-4.

2. Wu, R., Zhang, X., Ahn, G.-J. ACaaS: Access Control as a Service for IaaS Cloud. URL: http://sefcom.asu.edu/publications/science2013.pdf (дата обращения 13.09.2016).

3. Majumder, A., Namasudra, S., Nath, S. Taxonomy and Classification of Access Control Models for Cloud Environments) // Continued Rise of the Cloud, Computer Communications and Networks, DOI 10.1007/978-1-4471-6452, 2014, pp. 23–32.

4. Frank, M., Buhmann, J.M., Basin, D. On the Definition of Role Mining // Proceedings of the 15th ACM symposium on access control models and technologies (Pittsburgh, PA, USA, June 2010). SACMAT'10. ACM, New York, NY, 2010, pp. 35–44.

5. Vaidya, J., Atluri, V., Guo, Q. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles // Proceedings of the 12th ACM symposium on Access control models and technologies (Sophia Antipolis, France, June 2007). SACMAT '10. ACM, New York, NY, 2007, pp. 175–184.

6. Blundo, C. and Cimato, S. A Simple Role Mining Algorithm // In Proceedings of the 2010 ACM Symposium on Applied Computing (Sierre, Switzerland, March 2010). SAC'10, ACM, New York, NY, 2010. pp. 1958–1962.

7. Frank, M., Buhmann, J. M., and Basin, D. Role Mining with Probabilistic Models // In ACM Trans. on Inf. and Syst. Security, 15, 4 (Apr. 2013), article No.: 15.

8. Lu, H., Hong, Y., Yang, Y., Duan, L., and Badar, N. Towards User-Oriented RBAC Model // In Proceedings of the 27th Annual IFIP WG 11.3 Conference (Newark, NJ, USA, July 2013). DBSec. 2013, Springer, LNCS, 7964, pp. 107–129.

9. Frank, M., Streich, A.P., and Basin, D. Multi-Assignment Clustering for Boolean Data // In The Journal of Machine Learning Research, 13, 2012. pp. 459–489.

10. Colantonio, A., Di Pietro, R., Ocello, A. A cost-driven approach to role engineering // In Proceedings of the 2008 ACM symposium on applied computing (Fortaleza, Ceara, Brazil, March 16–20, 2008). SAC'08, ACM, New York, NY, USA, 2008. pp. 2129–2136.

11. Molloy, I., Li, N., Li, T., and Lobo, J. Evaluating Role Mining Algorithms // In: Proceedings of the 14th ACM symposium on access control models and technologies (Stresa, Italy, June 2009). SACMAT'09, ACM, New York, NY, 2009. pp. 95–104.

12. Saenko, I. and Kotenko, I. Genetic Algorithms for Role Mining Problem // In Proceedings of the 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing (Ayia Napa, Cyprus, February 2011). PDP'2011, IEEE, pp. 646–650.

13. Saenko, I. and Kotenko, I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // In Proceedings of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (Garching, Germany, February 2012). PDP'2012, IEEE, 2012. pp. 269–274.

14. Blundo, C. and Cimato, S. Constrained Role Mining // In Security and Trust Management. Proceedings of the 8th International Workshop (Pisa, Italy, September 2012), Revised Selected Papers. STM 2012, Springer, LNCS, 7783, 2012. pp. 289–304.

15. Such, J.M., Criado, N. Resolving Multi-party Privacy Conflicts in Social Media // IEEE Transactions on Knowledge and Data Engineering (July 2016), pp. 1851–1863.

16. Such, J.M., Rovatsos, M. Privacy Policy Negotiation in Social Media // Journal ACM Transactions on Autonomous and Adaptive Systems (TAAS), Volume 11, Issue 1, April 2016. Article No. 4.

УДК 658.15

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДИАГНОСТИКИ И ПРОГНОЗИРОВАНИЯ ФИНАНСОВОГО СОСТОЯНИЯ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ, ДИСКРИМИНАНТНОГО АНАЛИЗА И НЕЙРОННЫХ СЕТЕЙ

Э. Б. Песиков

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

Рассматривается подход к повышению качества прогнозирования банкротства предприятия, позволяющего обеспечить необходимый уровень принимаемых стратегических управленческих решений. Предлагается аналитический инструментарий для проведения диагностики и прогнозирования финансовой состоятельности, основанного на применении метода анализа иерархий, дискриминантного анализа с последующим уточнением результатов прогнозирования с помощью нейронной сети. Обсуждаются результаты вычислительных экспериментов по решению исследуемых задач.

предприятие, прогнозирование, банкротство, метод анализа иерархий, дискриминантный анализ, нейронная сеть, многослойный персептрон.

Введение

В сложных современных условиях проблема разработки эффективных методик прогнозирования банкротства носит актуальный характер. Повышение качества прогнозирования банкротства предприятия позволяет руководству предприятия своевременно выявлять необходимость разработки мероприятий по финансовому оздоровлению для предотвращения запуска формальных процедур банкротства. В работе рассматривается один из возможных подходов к проведению диагностики финансового состояния предприятия.

Цель работы заключается в разработке автоматизированной системы прогнозирования банкротства предприятия, основанной на применении метода анализа иерархий и дискриминантного анализа, с последующим уточнением результатов прогнозирования с помощью нейросетевых технологий.

Для достижения поставленной цели были решены следующие задачи:

– проведение сравнительного анализа существующих подходов к прогнозированию банкротства предприятия;

– выявление наиболее значимых факторов (показателей), отражающих финансовое положение предприятия, с использованием метода анализа иерархий (метода Т. Саати);

– разработка системы прогнозирования банкротства предприятия, основанной на применении методов дискриминантного анализа и искусственных нейронных сетей;

– разработка деловой ситуации, связанной с решением задач выявления наиболее значимых факторов и прогнозирования банкротства предприятия;

– проведение сравнительного анализа результатов вычислительных экспериментов по решению задачи прогнозирования банкротства предприятия с использованием двух методов.

К известным методам диагностики финансового состояния предприятия, основанным на применении математических моделей и методов, относятся двухфакторная и пятифакторная модели Альтмана, модель Ж. Конана и М. Гольдера, методика Р. Таффлер и Г. Тишоу, модель Фулмера, модель Спрингейта, методика Лиса, шестифакторная модель Зайцевой, методика Ковалева и др. [1].

Анализ существующих подходов к диагностике финансового состояния предприятия, основанных на применении количественных методов, позволяет сделать вывод о том, что в этих подходах в основном используются методы дискриминантного анализа [2]. В работе предлагается также использовать такие современные и перспективные инструменты, как методы искусственного интеллекта (искусственные нейронные сети), позволяющие в ряде случаев сократить время решения исследуемых задач и повысить точность результатов расчетов [3].

К числу важнейших задач при прогнозировании банкротства предприятия относится задача выявление наиболее значимых факторов (показателей), отражающих финансовое положение предприятия, и количественной оценке степени их влияния на финансовую состоятельность.

В работе для ранжирования факторов используется метод анализа иерархий – математический инструмент системного подхода к решению проблем принятия решений [4].

Применение метода анализа иерархий начинается с иерархической декомпозиции рассматриваемой проблемы на все более простые составляющие части и в экспертной количественной оценке степени взаимодействия элементов иерархии. Строится многоуровневая иерархия, вершиной (фокусом) которой является суть проблемы, обозначается как цель и в данной задаче носит название «Банкротство». На нижнем уровне располагаются факторы банкротства (альтернативы), на промежуточном уровне (критерии) размещаются группы факторов банкротства. Количественные оценки влияния элементов нижних уровней на элементы верхних

уровней иерархии проводятся методом парных сравнений, для чего на основе экспертных оценок составляются матрицы парных сравнений. На следующем шаге выполняется свертка всех оценок иерархии для получения приоритетов альтернатив относительно цели, расположенной в фокусе иерархии.

Результаты вычислительных экспериментов по решению задачи выявления наиболее значимых факторов банкротства

Финансовыми аналитиками предприятия были выявлены семь показателей (факторов), влияющих на финансовую состоятельность. Заданное множество показателей банкротства было разбито на два подмножества (группы) – группу «Финансовая устойчивость», в состав которой входят коэффициент обеспеченности основными средствами, коэффициент оборачиваемости активов, коэффициент финансовой зависимости, коэффициент нормы чистой прибыли, коэффициент автономии, и группу «Ликвидность», включающую в себя коэффициент текущей ликвидности и коэффициент покрытия. Требуется выявить пять наиболее значимых факторов из семи заданных факторов банкротства. В соответствие с методом анализа иерархий была построена иерархическая структура, представленная на рис. 1.

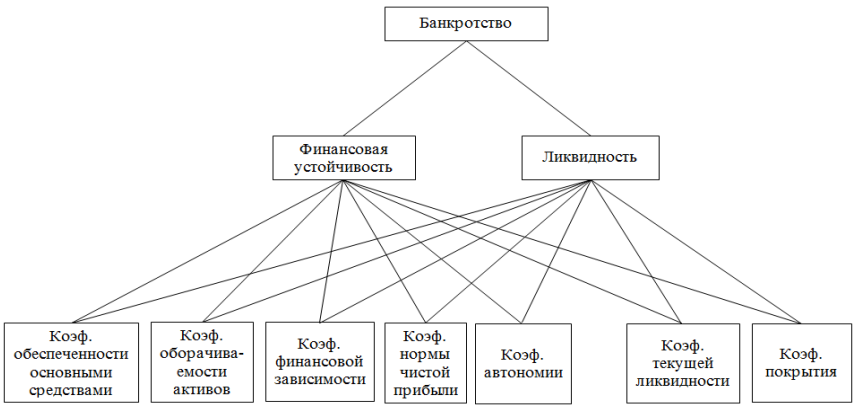


Рис. 1. Иерархическая структура проблемы банкротства

Экспертами была реализована процедура парного сравнения, в рамках которой критерии сравнивались попарно по отношению к цели, а альтернативы – попарно по отношению к каждому из критериев. Для вычисления количественных оценок степени влияния показателей на банкротство предприятия использовалась система поддержки принятия решений СППР «Выбор» [5].

Результаты вычислений «весов» факторов банкротства представлены на рис. 2.

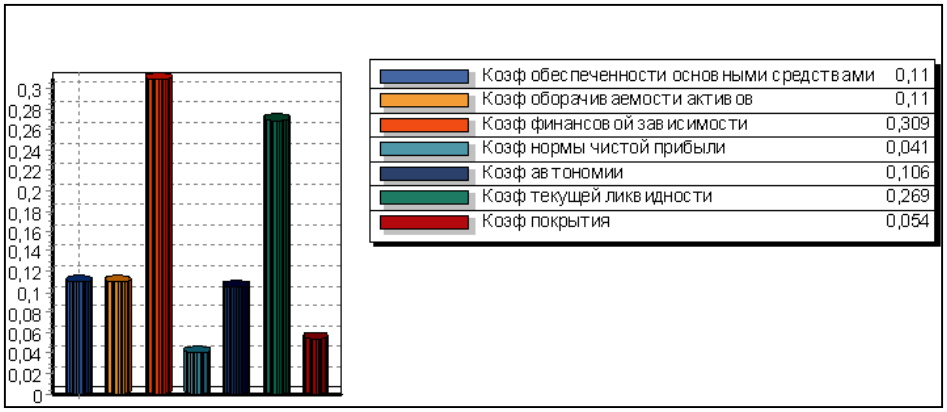


Рис. 2. Вид диалогового окна СППР «Выбор»
с результатами вычислений «весов» факторов банкротства

Анализ результатов расчетов «весов» факторов банкротства позволил выявить пять показателей с наибольшими значениями «весов»: коэффициент финансовой зависимости (фактор x_2); коэффициент текущей ликвидности (фактор x_1); коэффициент обеспеченности основными средствами (фактор x_3); коэффициент оборачиваемости активов (фактор x_4) и коэффициент автономии (фактор x_5).

Выявленные показатели использовались в дальнейшем при решении задачи прогнозирования банкротства предприятия.

Результаты вычислительных экспериментов по решению задачи прогнозирования банкротства

Аналитиками предприятия были рассмотрены 50 фирм, выпускающих аналогичную продукцию.

Значения пяти факторов банкротства были определены для каждого из 50-ти предприятий, половина которых находилась в состоянии, близком к банкротству, а другая половина работала успешно. Кроме того, для 51-го предприятия с неизвестным статусом («банкрот» или «не банкрот») известны значения факторов: $X_1 = 0{,}124$, $X_2 = 2{,}068$, $X_3 = 2{,}658$, $X_4 = 1{,}346$, $X_5 = 0{,}542$.

Необходимо определить статус 51-го предприятия с помощью дискриминантного анализа и искусственных нейронных сетей.

При применении дискриминантного анализа необходимо построить уравнения классификационных функций для каждой функций группы предприятий с определенным статусом.

Решение задачи прогнозирования банкротства проводилось с использованием программы “Statistica” [6].

На первом шаге определяются значения коэффициентов уравнений функции классификации для каждой группы предприятий. Результаты расчетов представлены на рис. 3.

Variable	Classification Functions; grouping: Status (Spreadsheet2 in Workbook1)	
	Bankrupt p=,50000	**Not a bankrupt p=,50000**
X1	19,8478	60,871
X2	-3,4146	5,581
X3	7,2679	23,724
X4	38,5313	131,522
X5	49,5301	127,199
Constant	-18,4200	-167,821

Рис. 3. Вид диалогового окна программы “Statistica” с значениями коэффициентов классификационных функций

Классификационные функции для каждой группы имеют вид:

– для первой группы предприятий со статусом «банкрот»:

$$z_1 = -18{,}42 + 19{,}8478X_1 - 3{,}414X_2 + 7{,}2679X_3 + 38{,}5313X_4 + 49{,}5301X_5;$$

– для второй группы предприятий со статусом «не банкрот»:

$$z_2 = -167{,}821 + 60{,}871X_1 - 5{,}581X_2 + 23{,}724X_3 + 131{,}522X_4 + 127{,}199X_5.$$

Чтобы определить, к какой группе относится предприятие, необходимо рассчитать для него значения переменных z_1 и z_2. Подставляя в уравнения классификационных функций заданные значения факторов банкротства для предприятия, получаем $z_1^* = 70{,}647$ и $z_2^* = 105{,}553$. Так как $z_1^* < z_2^*$, делается вывод о том, что предприятие имеет статус «не банкрот».

Для прогнозирования банкротства с помощью нейронных сетей используются те же исходные данные, что и в дискриминантном анализе. Для решения задачи прогнозирования банкротства с помощью нейронных сетей используется модуль «Neural Networks» программы «Statistica» [3].

Сравнительный анализ результатов экспериментов по обучению сетей на данных исходной выборки позволяет сделать вывод о том, что эффективность многослойных персептронов выше, чем эффективность сети, построенной на радиальных базисных функциях. При использовании выбранного типа нейронной сети (многослойного персептрона) был получен аналогичный результат прогнозирования. Таким образом, при расчетах двумя методами получена согласованная оценка вероятности банкротства.

Заключение

Проведенные вычислительные эксперименты подтверждают эффективность и корректность предлагаемого подхода к решению задачи прогнозирования банкротства предприятия. Совместное применение методов исследования операций, дискриминантного анализа и нейросетевых технологий при диагностике финансовой состоятельности позволяет повысить качество принимаемых решений о статусе предприятия. Предлагаемая сис-

тема прогнозирования банкротства представляет интерес для крупных предприятий, стремящихся получить конкурентное преимущество за счет применения аналитических систем прогнозирования финансового состояния предприятия.

Список используемых источников

1. Патласов О. Ю., Сергиенко О. В. Антикризисное управление. Финансовое моделирование и диагностика банкротства коммерческой организации. М. : Книжный мир, 2009. 512 с.

2. Ким Дж.-О., Мьюллер У., Клекка У. Р. Факторный, дискриминантный и кластерный анализ. М. : Финансы и статистика, 1989. 215 с.

3. Боровиков В. Нейронные сети. STATISTICA Neural Networks. Методология и технологии современного анализа данных. М. : Горячая линия – Телеком, 2008. 392 с.

4. Саати Т. Принятие решений. Метод анализа иерархий. М. : Радио и связь, 1993. 278 с.

5. Система поддержки принятия решений (СППР) «Выбор» [Электронный ресурс] // ciritas.ru: ЦИРИТАС – разработка программного обеспечения. URL: http://www.ciritas.ru/product.php?id=10 (дата обращения 05.01.2017).

6. Буреева Н. Н. Многомерный статистический анализ с использованием ППП «STATISTICA». Нижний Новгород, 2007. 114 с.

УДК 65.011.56

ПРЕДЛОЖЕНИЯ ОБ АВТОМАТИЗИРОВАННОМ ВЕДЕНИИ ПОДЛИННИКОВ КОНСТРУКТОРСКОЙ ДОКУМЕНТАЦИИ ПРЕДПРИЯТИЯ СВЯЗИ НА ОСНОВЕ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Н. В. Полпудникова, А. В. Шестаков

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

Рассматриваются вопросы ведения подлинников конструкторской документации предприятия-разработчика средств связи как бумажной, так и электронной конструкторской документации на различных этапах жизненного цикла продукции. С целью обеспечения интегрированных подходов в условиях изменения и развития технологий в делопроизводстве и документообороте электронными документами и повышения защищенности информации подлинников конструкторской документации предложены подходы к применению технологии распределенных реестров с учетом существующих и используемых на предприятиях программных и аппаратно-программных средств управления данными об изделии и жизненным циклом продукции.

подлинник конструкторской документации, PDM/PLM системы, технология распределенных регистров.

Одним из ключевых вопросов в жизненном цикле промышленной продукции (изделия), особенно систем, сетей и оборудования связи, является организация поддержания в актуальном состоянии подлинников документации, оформленных подлинными установленными подписями, пригодных для многократного снятия копий [1]. Перечень документации определен требованиями единой системы конструкторской документации (ЕСКД), единой системы технологической документации (ЕСТД), единой системы программной документации (ЕСПД) и других нормативно-технических документов (НТД).

Подлинник конструкторского (технологического, программного, ремонтного и т. д.) документа должен отражать состояние конструкции или технологии изготовления изделия в период утверждения их заказчиком, передачи подлинников организациям-изготовителям, прекращения производства данной конструкции и т. п. [2]. Естественно, что состояние конструкции или технологии изделия объективно подвержено изменению, например, с развитием технологий и сортамента комплектующих, возможностей их поставок, объемов и условий, из-за рисков недобросовестной конкуренции (даже на уровне межгосударственных отношений и всемирной торговой организации), а также финансовой устойчивости предприятий-разработчиков/изготовителей составных частей изделий (далее – СЧ).

Особую роль в жизненном цикле продукции выполняет организация-держатель подлинников документов, которая должна осуществлять не только хранение, учет подлинников документов и внесение в них изменений, а также поставлять (передавать) копии и/или дубликаты своим абонентам. На продолжительность и качество выполнения указанных процедур значительное влияние оказывают несколько факторов:

существующая регламентация процедур внесения изменений в документы и реестры (разработка предложения об изменении; выпуск предварительного извещения об изменении, дополнительного извещения об изменении, извещения об изменении), согласно ГОСТ 2.503–2013;

потребный объем изменений, вносимых в комплект документов и реестры. Так любое изменение в документе, которое вызывает какие-либо изменения в других документах, должно одновременно сопровождаться внесением соответствующих изменений во все взаимосвязанные документы [3]. Положение осложнится, если эти изменения затрагивают документы СЧ изделия и принятую иерархию организаций-держателей подлинников документации СЧ изделия;

необходимость разработки нового комплекта документов и изменение реестра (если хотя бы для одного изделия изменение документа окажется

неприемлемым, то на изменяемое изделие должен быть выпущен новый документ с новым обозначением);

ведение системы реестров смешанного учета бумажной и электронной документации в организации-держателе подлинников документации.

Как показывают результаты проведенного анализа ряда предприятий связи (организаций-держателей подлинников документации) существующая операционная деятельность по ведению ими подлинников конструкторской документации имеет определенные недостатки:

низкую оперативность внесения изменений при валидации по требованиям службы эксплуатации и заказчика в условиях стремительно развивающихся телекоммуникационных и информационных технологий;

сложность контроля со стороны заказчика и кооперационного взаимодействия предприятий-разработчиков и предприятий-изготовителей СЧ изделия при значительном количестве СЧ изделия;

риски изменений целостности данных в реестрах о проведенных изменениях в документах как СЧ изделия, так и на изделие в целом;

проблематичность обеспеченности ресурсами стадий и этапов жизненного цикла изделий при реализации принятых изменений.

Одним из действенных направлений разрешения сложившихся противоречий, по нашим оценкам, является применение распределенных реестров и блокчейн как системной технологии, которая позволит оптимизировать затраты и улучшить операционную эффективность взаимосвязанных бизнес-систем (рис. 1).

Рис. 1. Предмет исследования при разработке предложений по автоматизированном ведении подлинников документации

Развитие технологий распределенных реестров и блокчейна определены технологическими тенденциями в сфере криптовалют. Уровень некоторых решений представлен в таблице.

ТАБЛИЦА. Обобщенные данные об уровне технологии блокчейн

Продукт/ технология	Ethereum	Counterparty	Hyperledger Fabric
Компания-разработчик	Gavin Wood, Jeffrey Wilcke, Виталик Бутерин, и другие	Сообщество Counterparty	Блокчейн-консорциум Hyperledger
Назначение	Платформа для децентрализованных онлайн-сервисов	Криптовалютная платформа на основе сети Bitcoin	Платформа для распределенных приложений
Открытый исходный код	Да	Да	Да
Системотехническое решение	Единая децентрализованная виртуальная машина Ethereum (EVM)	Блокчейн Bitcoin одноранговой системы оплаты и финансовой платформы с портированной EVM, Multi-SIG	Открытые технологии распределенного реестра
Реализация	Сеть с 2015 года. v1.7.3	С 2014 года	v0.6, 2016; v1.0-alpha, 2017
Типажирование	Токены ETH. Несколько open-source лицензий	Токены XCP. Цифровые соглашения (смарт-контракты). Age of Rust; Augmentors; XCP DEX	Hyperledger Sawtooth; Hyperledger Iroha; Hyperledger Burrow

Несмотря на недостаточно устоявшуюся терминологию дадим следующее определение: «Блокчейн – это защищенный от несанкционированного доступа цифровой реестр общего пользования, который ведет учет транзакций в публичной или закрытой одноранговой сети». Распределенный между всеми узлами сети реестр непрерывно записывает историю операций с активами между одноранговыми узлами сети в виде блоков информации. Все утвержденные блоки транзакций соединяются в цепочку – с начального блока до последнего добавленного (англ. *block chain* – цепочка блоков). Блокчейн выступает единым источником достоверных данных, а участникам доступны только те транзакции, которые относятся к ним. На основе технологии блокчейна реализуются смарт-контракты. Смарт-контракт – это программа, которая при подтверждении всех сторон фиксирует, что операция достигнута и использует для этого определенный код.

Во многих странах мира технология блокчейна формирует новую цифровую экономику. Заявлено свыше 5000 практически значимых стартапов, из которых более сотни приносят значительный доход.

В нашей стране технологии распределенных реестров и блокчейн нашли применение и в других сферах. В феврале 2018 года Росреестром совместно с Гос. корпорацией «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)» и Акционерным обществом «Агентство ипотечного жилищного кредитования» внедрен блокчейн-проект для регистрации договоров участия в долевом строительстве в Ленинградской области [4]. О важности этого направления можно судить и по решению Федерального агентства по технического регулированию и метрологии создать технический комитет по стандартизации «Программно-аппаратные средства технологий распределенного реестра и блокчейн» (ТК-159) и его участия в работе международного технического комитета ИСО/ТК 307 «Блокчейн и технологии распределенного реестра» [5].

С учетом вышеизложенного предлагается организовать децентрализованную систему попарных смарт-контрактов (цифровых соглашений) на основе технологии распределенных реестров и блокчейна между предприятием-держателем подлинника документации на изделие в целом, предприятиями-держателями подлинников документации на СЧ изделия и предприятиями-изготовителями. Для обеспечения централизованной балансировки целостности данных смарт-контрактов (хранения контрольных сумм) дополнительно в систему включить орган управления заказчика (представителя заказчика). Для этого в службе технической документации (далее – СТД) предприятия-держателя подлинника документации на изделие в целом, предприятий-держателей подлинников документации на СЧ изделия, предприятий-изготовителей развернуть частные базы данных блокчейна (ЧБД) и организовать их попарное взаимодействие, резервирование и обмен данными об изменении подлинников документации. Развернуть и подключить ЧБД балансировки смарт-контрактов в органе управления заказчика (представителя заказчика) в соответствии с рис. 2.

Внедрение данного предложения на предприятии связи с реализованными прототипами PDM/PLM, CAD, CAM и ERP систем, например, на основе решений «ЛОЦМАН:PLM АРХИВ»; «1С:PDM Управление инженерными данными 3» для «1С:ERP», приведет к повышению достоверности данных об изменениях подлинников документации на изделие, существенному сокращению продолжительности работ по модернизации изделий в ходе их текущей эксплуатации, в том числе и на объектах заказчика.

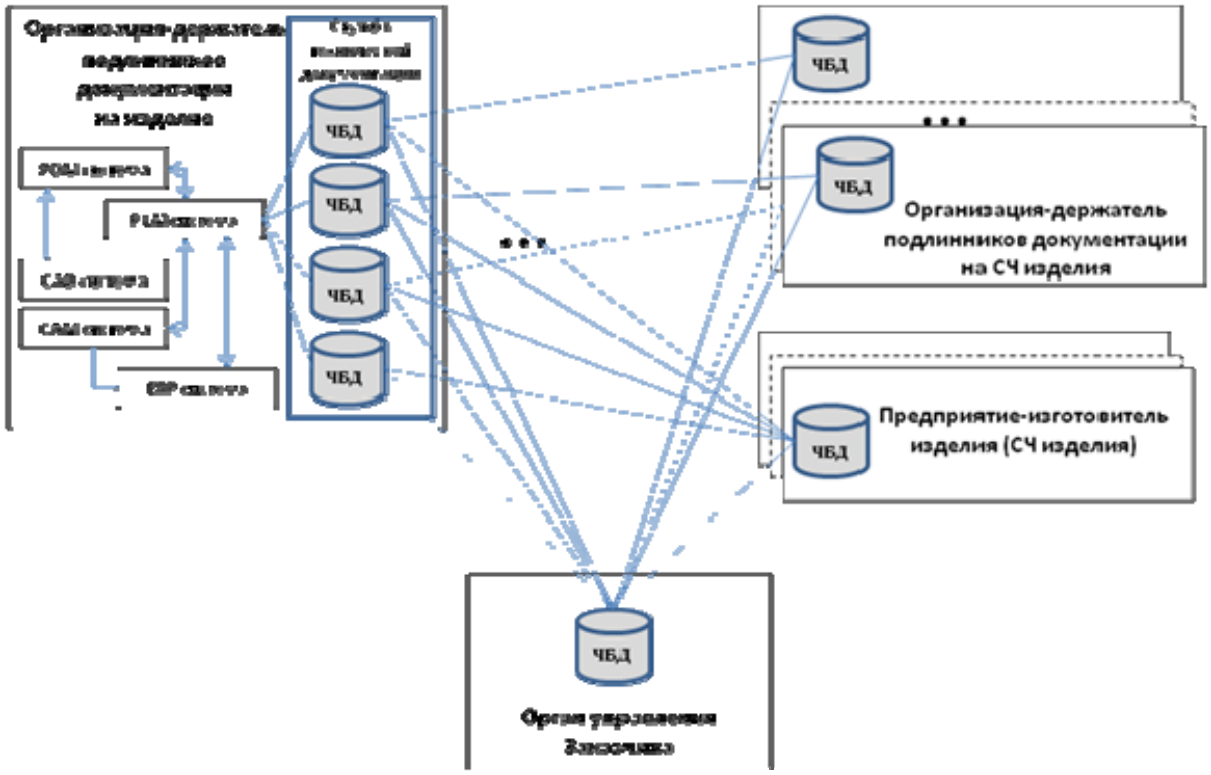


Рис. 2. Архитектура автоматизированного ведения подлинников конструкторской документации предприятия связи на основе технологии распределенных реестров

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. ГОСТ 2.501–2013. Единая система конструкторской документации. Правила учета и хранения. М. : Стандартинформ, 2014. III, 19 с. : ил.

3. ГОСТ 2.503–2013. Единая система конструкторской документации. Правила внесения изменений. М. : Стандартинформ, 2014. III, 27 с. : ил.

4. Росреестр зарегистрировал первый долевой договор с применением блокчейна. 2018. [Электронный ресурс] Режим доступа: https://rb.ru/news/rosreestr-blockchain (дата обращения 01.02.2018).

5. Приказ Федерального агентства по технического регулированию и метрологии от 15.12.2017 № 2831 «О создании технического комитета по стандартизации «Программно-аппаратные средства технологий распределенного реестра и блокчейн» [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/ 556016342 (дата обращения 01.02.2018).

УДК 004.7:004.422.8

АНАЛИЗ МЕТОДОВ КОМПЛЕКСИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л. К. Птицына, А. В. Тарабаров

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

Обоснована актуальность повышения качества функционирования комплексных систем защиты информации. Представлены основные направления совершенствования технологий обеспечения информационной безопасности. Описана система классификации методов комплексирования средств защиты. Выбраны расширенные профили качества комплексных систем защиты информации. Сформированы базовые классы ситуационных моделей комплексирования средств защиты. Раскрыт математический аппарат для анализа базовых классов ситуационных моделей комплексирования средств защиты.

информационная безопасность, защита информации, комплексирование средств, объектно-ориентированная модель, обратная связь.

В настоящее время одно из основных направлений развития производства во всех сферах социально-экономической деятельности ориентируется на создание экосистемы цифровой экономики.

Создание экосистемы цифровой экономики базируется на платформах и технологиях, где формируются компетенции для развития рынков и отраслей.

Для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики требуется среда, создающая условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики.

Среда образуется на основе развития нормативного регулирования, подготовки кадров, информационной инфраструктуры и повышения её информационной безопасности.

Эффективное взаимодействие субъектов рынков и отраслей экономики требует совершенствования системы информационной безопасности во всех секторах экономики.

Построение сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства и наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру

создают многообразные предпосылки для появления новых угроз информационной безопасности.

Ключевые направления развития технологий обеспечения информационной безопасности формируются на базе целевых обобщений формальных основ научных исследований в области безопасности. Обобщения проводятся на методологическом уровне. При каждом целевом обобщении соблюдается контекст определённой парадигмы обеспечения информационной безопасности, согласующийся с современными представлениями о состоянии дел в этой области.

При развитии технологий обеспечения информационной безопасности предусматривается совершенствование комплексных систем защиты информации.

Один из путей подобного совершенствования ориентируется на расширение приёмов комплексирования средств.

Опорными приёмами комплексирования считаются:

– комплексирование аппаратных средств;

– комплексирование аппаратно-программных средств;

– комплексирование аппаратно-программных средств.

Методологические основы анализа динамических характеристик комплексных систем защиты информации с традиционными приёмами комплексирования раскрываются в [1, 2, 3, 4, 5, 6].

При расширении рассматриваемых приёмов добавляется комплексирование виртуальных средств, требующее развития математического аппарата для анализа динамических характеристик комплексных систем защиты информации.

Помимо указанного приёма актуализируется появление инновационного подхода, при котором при комплексировании используются обратные связи. К инновационным приёмам комплексирования относятся:

– комплексирование аппаратных средств с обратной связью;

– комплексирование аппаратно-программных средств с обратной связью;

– комплексирование аппаратно-программных средств с обратной связью;

– комплексирование виртуальных средств с обратной связью.

Математический аппарат для анализа динамических характеристик комплексных систем защиты информации с предложенными инновационными приёмам комплексирования может базироваться на совмещении методов анализа логических моделей, методов анализа расширенных объектно-ориентированных моделей и методов анализа конечных цепей Маркова, одна из формализаций которого раскрыта в [7].

Наряду с описанными выше подходами к совершенствованию комплексных систем защиты информации, активно развиваются и направления, предусматривающие их интеллектуализацию с помощью агентных технологий. Методологический базис агентных технологий для обеспечения информационной защищённости раскрывается в [8, 9].

Дальнейшее совершенствование архитектуры комплексных систем защиты информации может проводиться посредством включения агентов-контролёров в обратные связи комплексирования. В таком случае появляются новые схемы технических решений:

– комплексирование аппаратных средств с агентом-контролёром в обратной связи;

– комплексирование аппаратно-программных средств с агентом-контролёром в обратной связи;

– комплексирование аппаратно-программных средств с агентом-контролёром в обратной связи;

– комплексирование виртуальных средств с агентом-контролёром в обратной связи.

Математический аппарат для анализа динамических характеристик интеллектуальных комплексных систем защиты информации с новыми схемами комплексирования может базироваться на совмещении методов анализа систем искусственного интеллекта, методов анализа логических моделей, методов анализа расширенных объектно-ориентированных моделей и методов анализа конечных цепей Маркова.

Список используемых источников

1. Птицына Л. К., Птицын А. В. Определение динамических характеристик распределенных систем защиты информации // Научно-технические ведомости СПбГПУ. Наука и образование. 2010. № 4. С. 284–288.

2. Птицына Л. К., Птицын А. В. Преодоление неопределенности относительно динамических профилей комплексных систем защиты информации // Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. Выпуск 5 (31) (по материалам XII Международного симпозиума по непараметрическим методам в кибернетике и системном анализе). Красноярск. 2010. С. 154–156.

3. Птицын А. В., Птицына Л. К. Аналитическое ядро динамического профиля параллельной идентификации угроз для образовательных программ по защите информации // Дистанционное и виртуальное обучение. 2011. № 4 (46). С. 76–86.

4. Птицын А. В., Птицына Л. К. Расширение возможностей объектно-ориентированного анализа для обеспечения управляемого качества комплексных систем защиты информации // Информационные технологии в проектировании и производстве. 2011. № 2. С. 55–60.

5. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Новые формализации аналитического исследования комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.

6. Птицына Л. К., Птицын А. В. Объектно-ориентированный анализ интеграции средств защиты информации // Вопросы защиты информации. 2013. № 1. С. 79–86.

7. Птицына Л. К., Лебедева А. А., Белов М. П. Метод анализа реактивных действий информационного агента при воздействии инфокоммуникационной среды // Международная конференция по мягким вычислениям и измерениям. 2017. № 1. С. 155–158.

8. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 1. С. 50–55.

9. 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.

УДК 004.7:004.422.8

ИНТЕЛЛЕКТУАЛЬНАЯ ИНТЕГРАЦИЯ КЛАСТЕРНЫХ СЕГМЕНТОВ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ

Л. К. Птицына, Н. Эль Сабаяр Шевченко

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

Актуализирована кластерная сегментация сервис-ориентированных систем крупных корпораций. Описаны ключевые особенности жёсткой и мягкой сегментации сервис-ориентированных систем. Предложен мультиагентный подход к мягкой интеграции кластерных сегментов сервис-ориентированных систем. Определены вариации в организации планирования действий мультиагентной системы интеграции. Выбрана форма представления алгоритмов планирования действий мультиагентной системы интеграции. Выделен механизм согласования планировщиков с обновлением технологического базиса мультиагентной системы. Разработана концепция сравнительного анализа вариаций в организации мультиагентной системы.

кластерная сегментация, мультиагентный подход к интеграции, планирование действий, мягкая интеграция, самоорганизация.

С увеличением объема данных, информации и знаний, усилением жёсткости конкуренции в условиях перехода к цифровой экономике актуализируется интеллектуальная кластеризация сервис-ориентированных распределенных систем крупных корпорации. При этом возникает объективная необходимость обеспечения быстрой и своевременной эволюции информационных систем при динамичном изменении окружающих сред в условиях априорной неопределённости их описаний [1]. Посредством объединения в кластеры обеспечивается непрерывный обмен знаниями,

опытом и технологиями, а также возможность совместного использования широкого круга вариаций в сочетании различных сервисов.

Согласно [2] кластер определяется как группа географически соседствующих взаимосвязанных компаний (поставщиков, производителей и иных участников производства) и связанных с ними организаций (образовательных заведений, органов государственного управления, инфраструктурных компаний), действующих в определенной сфере, взаимодополняющих друг друга и усиливающих конкурентные преимущества отдельных организаций и кластера в целом. Взаимодействие организаций, входящих в кластер, представляет собой совокупность кооперации и конкуренции (соконкуренции).

В экономике применение кластерных подходов интеграции выражается в образовании сетевых структур по принципу конкурентного сотрудничества (соконкуренции). Порождаемые конкуренцией связи между участниками сети, усиливают сотрудничество во взаимовыгодных направлениях.

Предлагаемая концепция определяется в рамках сервис-ориентированной архитектуры с гарантиями качества как гибкая интеллектуальная кластеризация интегрируемых сервис-ориентированных средств по схожему функционалу с общими взаимовыгодными целями в рамках актуальных требований, формирующая условия для кооперации и/или конкуренции при дальнейшей межкорпоративной интеграции. При этом наблюдаются высокая степень самоорганизации и непрерывная эволюция системы в целом. Соблюдение необходимых гарантий качества обеспечивается благодаря подключению модельно-аналитического интеллекта, формируемого на основе расширенного объектно-ориентированного моделирования сервис-ориентированных систем [3].

Неоспоримые преимущества подобной концепции заключаются в многообразии предоставляемых услуг для выполнения широкого спектра профессиональных задач при разных критериях качества. Главный упор в концепции делается на самоорганизацию комплексной сервис-ориентированной системы и адекватное реагирование комплексируемых сервисных компонентов на изменение широкого спектра жестких требований, обеспечивающей непрерывное обновление услуг с необходимым уровнем качества.

В предлагаемой концепции отдаются предпочтения мягкой сегментации сервис-ориентированных средств из-за наличия обширного многообразия недостатков жёсткой сегментации. При жесткой сегментации не учитывается факт переменных предпочтений в требованиях к системе, а, следовательно, наблюдается низкая конкурентоспособность; не реализуются технологии, побуждающие согласованность между организациями; не обеспечивается дальнейшая приоритетная эволюция системы при изме-

нении рыночных условий. Невыгодность жесткой сегментации сервис-ориентированных средств обусловливается и неспособностью соответствовать по реактивности динамичным изменениям окружающей среды.

В предлагаемой концепции мягкая кластерная сегментация масштабной комплексной сервис-ориентированной системы представляется как планируемая «актуальная интеграция», которая является мета-сборкой и характеризуется следующими ключевыми особенностями:

– планирование действий по интеграции в условиях априорной неопределенности относительно окружающей среды сервис-ориентированной системы (динамическая конфигурация сервис-ориентированных средств с учетом общих интересов кластера);

– выполнение сравнительного анализа моделей интеграций на основе оценивания качества планируемой интеграции и критериальный отбор вариантов, удовлетворяющих актуальным состояниям окружающей среды;

– соконкуренция сервис-ориентированных систем и оптимизация за счет самосовершенствования комплексируемых систем.

Планирование действий в системах искусственного интеллекта рассматривается как одна из ключевых особенностей вычислительного интеллекта артефактов [4]. Благодаря методологической канве априорного выбора оптимального алгоритма решения задачи планирования, раскрытой в [5], обеспечивается формирование компонентов первого слоя наукоёмкого ядра мягкой интеграции комплексируемых сервис-ориентированных систем. Второй слой наукоёмкого ядра образуется на основе сочетания методов аналитического расширенного объектно-ориентированного моделирования сервис-ориентированных систем, предложенных в [1, 6]. В условиях разноплановости профилей профессиональной деятельности и масштабности распределённости комплексируемых сервис-ориентированных систем проявляется целесообразность использования самоорганизующихся возможностей мультиагентных систем [7, 8, 9].

С учетом особенностей представленной концепции предлагается самоорганизующаяся мультиагентная система интеллектуальной интеграции кластерных сегментов сервис-ориентированных систем с планированием действий, где главный механизм взаимодействия базируется на кооперации и конкуренции (см. рис. ниже).

Каждый агент-организатор закрепляется за определённой сервис-ориентированной системой. Работа агента-организатора заключается в поиске сервисов и композиции подходящих кластерных сегментов для того, чтобы скоординироваться в действиях с остальным множеством агентов-организаторов и в решениях по межкорпоративной интеграции сервис-ориентированных систем.

Мультиагентная система описывается множеством **A**:

$$\mathbf{A} = (A_1, A_2 A_3, ..., A_N),$$

где $A_1, A_2 A_3, ..., A_N$ – агенты-организаторы мультиагентной системы интеграции кластера.

Каждый агент-организатор A_i представляется кортежем:

$$A_i = \left\langle P_i, ALGO_{i,k}, KB_i \right\rangle,$$

$$A_i \in A,$$

где P_i – планировщик *i*-го агента-организатора; $ALGO_{i,k}$ – *k*-й алгоритм планирования действий *i*-го агента-организатора; KB_i – база знаний *i*-го агента-организатора.

Каждая сервис-ориентированная система подчиняется своему агенту-организатору:

$$S_{A_i} = (S_{A_i,1}, S_{A_i,2}, S_{A_i,3}, ..., S_{A_i,N}),$$

где S_{Ai} – множество сервисов относящихся к *i*-му агенту A_i.

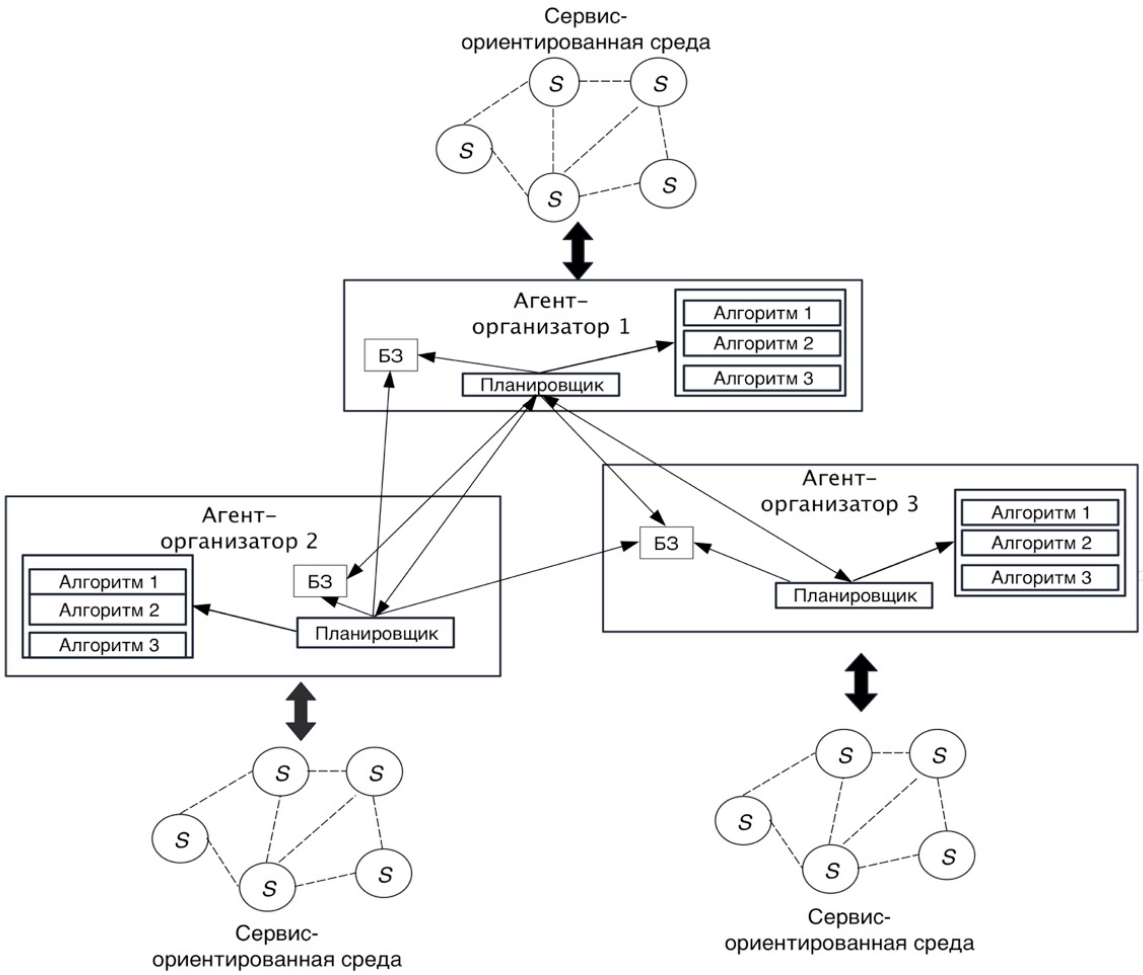


Рисунок. Интеллектуальный кластер с мягкой интеграцией распределенных сервис-ориентированных систем

Каждым агентом осуществляется отбор необходимых сервисов для композиции бизнес-процесса и обеспечения межкорпоративной интеграции по схожим целям.

Межагентное согласование является горизонтальным и мягковертикальным. В мультиагентной системе допускается наличие агента с полномочиями диспетчеризации/мониторинга для предотвращения хаотизации агентов-организаторов. Механизм согласования планировщиков осуществляется по принципу конкуренции, поскольку могут появляться задачи, которые агент не в состоянии решить самостоятельно. В таком случае за одним из агентов-организаторов закрепляется роль заказчика и выбирается агент-посредник.

На первом этапе взаимодействия поддерживается конкуренция между агентами для выработки рационального плана действий, а затем осуществляется кооперация для составления межкорпоративной интеграции. Весь интеграционный опыт вносится в базу знаний агентов, формирующий прецеденты.

Представленная концепция является опорной для создания и сопровождения сложных интеллектуальных распределенных сервис-ориентированных систем, гибко-интегрируемых в контексте самоорганизации и эволюционирующих в контексте самосовершенствования.

Список используемых источников

1. Птицына Л. К., Веселов В. О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоемкие технологии в космических исследованиях Земли. H&ES RESEARCH. 2015. N 2. С. 42–47.

2. Портер М. Конкуренция: пер. с англ. М. : Вильямс, 2005. 608 с.

3. Кондратьев Д. А., Птицына Л. К., Эль Сабаяр Шевченко Н. Моделирование интеллектуальных сервис-ориентированных систем [Электронный ресурс] // Информационные системы и технологии в моделировании и управлении: материалы I всерос. научно-практической. конф., Ялта, 23–24 мая 2016 г. СПб. : СПбГЭТУ «ЛЭТИ», 2016. С. 57–60. URL: http://istmu2016.csrae.ru/ru/1/publications (дата обращения 14.05.2016).

4. Рассел С., Норвиг П. Искусственныи интеллект. Современный подход, 2 изд. М. : Вильямс, 2007. 1408 с.

5. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знании. Планирование действий интеллектуальных агентов в информационных сетях : учеб. пособие. Федеральное агентство по образованию, СПбГПУ. СПб. : Изд-во Политехн. ун-та, 2006. 172 с.

6. 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. 71–80.

7. Теория систем и системный анализ в управлении организациями : Справочник : Учеб. пособие. Баринов В. А., Болотова Л. С., Волкова В. Н., Денисов А. А., Дуболазов В. А., Емельянов А. А., Катаев А. В., Кузин Б. И., Кузьменков В. А., Ланкин В. Е., Лыпарь Ю. И., Ногин В. Б., Птицына Л. К., Старовойтова М. И., Ступак В. Б., Тарасо-

ва А. В., Федоров А. В., Ходырев В. В., Чудесова Г. П., Широкова С. В., Юрьев В. Н. / Под ред. В. Н. Волковой и А. А. Емельянова. М. : Финансы и статистика, 2009. 848 с.

8. Городецкий В. И. Самоорганизация и многоагентные системы. Модели многоагентной организации // Известия РАН. Теория и системы управления. 2012. Вып. 2. С. 92–120.

9. Лихтенштейн В. Е., Конявский В. А., Росс Г. В., Лось В. Г. Мультиагентные системы: самоорганизация и развитие. М. : Финансы и статистика, 2017. 262 с.

УДК 519.688

ВРЕМЕННАЯ СЛОЖНОСТЬ АЛГОРИТМОВ И РЕГРЕССИОННЫЙ АНАЛИЗ В ЗАДАЧАХ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ

В. Ю. Сливков, А. И. Ходанович

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

Рассматриваются концептуальные аспекты теории сложности алгоритмов в задачах компьютерного моделирования. Показан пороговый эффект во временной сложности алгоритма, а также пример гипотетической эквивалентности классов алгоритмических задач. Приводится оценка временной сложности алгоритма в компьютерной модели нелинейной динамической системы с дискретной симметрией и результат регрессионного анализа численного решения.

алгоритм, временная сложность, компьютерная модель, регрессионный анализ.

Развитие теории алгоритмов начинается с доказательства К. Гёделем теорем о неполноте формальных систем, включающих арифметику, первая из которых была доказана в 1931 г. Возникшее в связи с этими теоремами предположение о невозможности алгоритмического разрешения некоторых математических проблем вызвало необходимость стандартизации понятия алгоритма. Первые стандартизованные варианты этого понятия были разработаны в 30-х годах XX века в работах А. Тьюринга, А. Чёрча и Э. Поста. Предложенные ими машина Тьюринга, машина Поста и лямбда-исчисление Чёрча оказались эквивалентными друг другу. Основываясь на работах Гёделя, С. Клини ввел понятие рекурсивной функции [1].

Одним из наиболее удачных стандартизованных вариантов алгоритма является введённое А. А. Марковым понятие нормального алгоритма. Оно было разработано десятью годами позже в работах Тьюринга, Поста, Чёрча и Клини в связи с доказательством алгоритмической неразрешимо-

сти ряда алгебраических проблем. Следует отметить также немалый вклад в теорию алгоритмов, сделанный Д. Кнутом, А. Ахо и Дж. Ульманом. Одной из лучших работ на эту тему является книга «Алгоритмы: построение и анализ» Томаса Х. Кормена, Чарльза И. Лейзерсона, Рональда Л. Ривеста, Клиффорда Штайна.

В рамках классической теории осуществляется классификация задач по классам сложности (*P*-сложные, *NP*-сложные, экспоненциально сложные и др.). Время, затраченное на реализацию алгоритма, как функция размерности задачи называется временной сложностью алгоритма и обозначается как $O[f_A(n)]$. Применительно к решению задачи на ПК – это время является в большинстве случаев свойством самого алгоритма и зависит от машины или от программы реализации. Отметим, что концептуальные вопросы алгоритмизации и программирования в информатике, практически, не обсуждаются в классических научных работах в области математического и компьютерного моделирования [2, 3].

Теория сложности (*complexity theory*) – это раздел теоретической информатики, связанный с оценками сложности работы алгоритмов. Сложность – понятие многогранное: здесь и время работы, и память, которая требуется алгоритму, и возможность его распараллеливания на несколько «процессоров», которые, как правило, моделируются машинами Тьюринга [1].

Экспоненциальные алгоритмы встречаются в задачах линейного программирования – оптимизации линейной функции при линейных же на нее ограничениях. В наиболее простой формулировке она сводится к тому, разрешима ли данная система линейных неравенств. Эта кажущаяся абстрактной задача имеет огромное количество применений и возникает в самых разных оптимизационных приложениях. В клиентах у крупнейшего производителя софта для решения задач линейного программирования (ЛП) – французской компании ILOG – ходят такие индустриальные гиганты, как Siemens, IBM, Visa International, France Telecom, United Airlines и многие другие.

Хотя о пользе решения систем линейных неравенств размышлял еще Фурье, впервые о применениях ЛП заговорили во второй четверти XX века. Начавшиеся исследования сразу же привели к успеху: по всей видимости, независимо друг от друга американец Джордж Данциг (*George Dantzig*) и советский математик Леонид Витальевич Канторович пришли (для разных, но эквивалентных формулировок исходной задачи) фактически к одному и тому же результату – симплекс методу.

Оценим вычислительную сложность задачи решения системы линейных алгебраических уравнений, часто встречающихся в различных приложениях с характерным пороговым эффектом (рис. 1, см. ниже). Для этого

воспользуемся стандартными функциями системы компьютерной математики Maple из пакета алгоритмов линейной алгебры [4, 5].

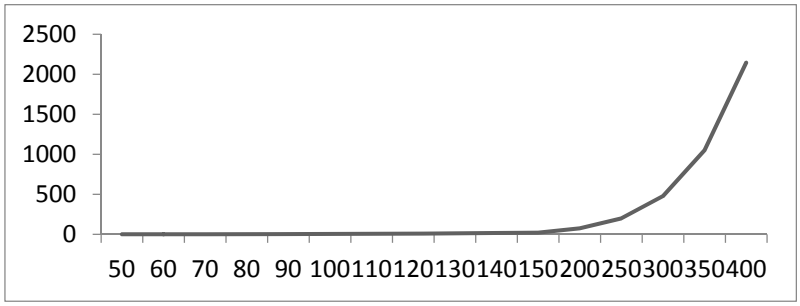


Рис. 1. Пороговый эффект во временной сложности алгоритма

Не менее интересен и пример вычисления n-го числа Фибоначчи. В процессе вычислительного эксперимента в среде Maple выяснено, что ее сложность является экспоненциальной $O(2^n)$. Подобные программы практически не применимы на практике. В этом очень легко убедиться, попробовав вычислить с ее помощью, например, 43-е число Фибоначчи. Тем не менее, можно написать программу с линейной сложностью и, возможно, с логарифмической используя рекуррентные формулы для чисел Фибоначчи [6]. Заметим, что данный пример иллюстрирует гипотетическую эквивалентность классов алгоритмических задач $P = NP$, причем, строгое математическое доказательство утверждения в настоящее время относится к фундаментальным задачам тысячелетия.

Когда тестируют учебные программы, то значения параметров, от которых они зависят, обычно невелики. Поэтому даже если при написании программы был применен неэффективный алгоритм, это может остаться незамеченным. Однако если подобную программу попытаться применить в реальных задачах математического моделирования, то ее практическая непригодность проявится незамедлительно.

Обычно решаемая задача имеет естественный «размер» (обычно количество обрабатываемых данных) которое мы называем n. В конечном итоге нам бы хотелось получить выражение для времени, необходимого программе для обработки данных размера n, как функцию от n. Обычно интересует средний случай – ожидаемое время работы программы на «типичных» входных данных, и худший случай – ожидаемое время работы программы на других входных данных.

Учитывая нетривиальный характер оценки сложности алгоритмических задач, в задачах компьютерного моделирования целесообразно изучение пороговых эффектов и нахождение критических параметров алгоритма в компьютерном эксперименте с регрессионным анализом полученных данных [6]. Демонстрационные примеры в теории сложности алгоритмов могут быть размещены в системе дистанционного образования Moodle,

дополняя учебные разделы математического моделирования реальных процессов и систем в информационной образовательной среде.

Впервые в практике математического моделирования показана возможность изучения классических парадоксов вычислительной физики и физики твердого тела в современном компьютерном эксперименте [7, 8]. Дана статистическая интерпретация закона равномерного распределения энергии по степеням свободы в результатах численного моделирования цепочки нелинейных связанных осцилляторов Ферми-Паста-Улама. Апробирована методика расчета энергии длинных наноразмерных акустических цепочек, дана полиномиальная оценка временной сложности алгоритма ФПУ. Дальнейшие исследования проводились в плане изучения физических свойств динамической системы Ферми-Паста-Улама с учетом флуктуаций плотности кристалла, с переходом на макроуровень в оценке молярной теплоемкости [8].

В рамках научно-исследовательской работы разработано программное обеспечение компьютерного эксперимента с нелинейными динамическими системами ФПУ, исследованы солитонные решения методами регрессионного анализа с использованием нелинейного программирования (рис. 2).

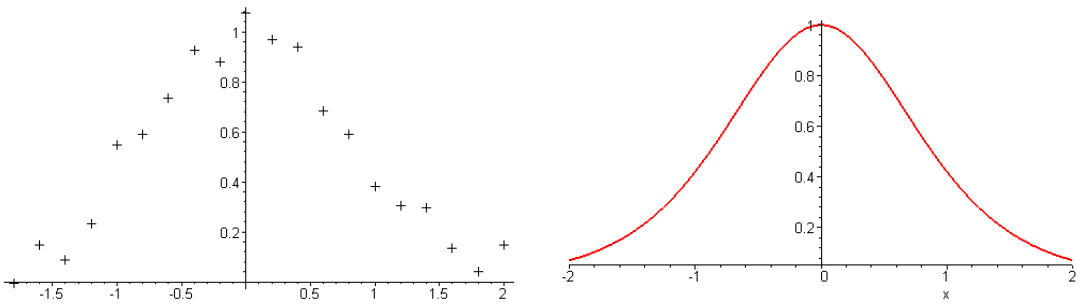


Рис. 2. Регрессионный анализ в компьютерной модели нелинейной динамической системы

В истории науки «много воды утекло» с момента наблюдения уединенной волны (*solitary wave*) на мелкой воде шотландским инженером и кораблестроителем Дж. С. Расселом (*J. Scott Russel*) (1834 г.). Вспомним комментарий исследователя: «Это самое прекрасное и необычное явление: в первый же день я понял, что это счастливейший момент в моей жизни… Никто никогда и вообразить не мог, что существует такое явление, как уединенная волна». К экзотическим нелинейным явлениям научная общественность не проявила интереса, фактически до теоретических работ голландских ученых Кортевега Д. и де Фриза Г. (*D. J. Korteweg, G. De Vries*) в области нелинейных волновых процессов (1895 г.). Американские специалисты Крускал М. и Забуски Н. рассматривают непрерывный аналог системы ФПУ и численные решения уединенных волн, вводят понятие «солитон» (1965 г.). Удивительное свойство солитона, являющегося вол-

ной, состоит в том, что он сохраняет свою форму после взаимодействия с себе подобным объектом: два солитона упруго отталкиваются, как две частицы. Это удивительное свойство дуальности (сочетанием свойств волны и частицы) наблюдается не только в натурных, но и численных экспериментах [9].

Аналогия вычислений и измерений позволяет применять экспериментальные методы в области компьютерного моделирования реальных процессов и систем. В частности, задачи регрессионного анализа для нестандартных функций, например, для солитонов можно интерпретировать как задачи нелинейного программирования со статистической обработкой данных. Для этого можно воспользоваться стандартными функциями популярных математических пакетов, в частности Maple.

Полученные результаты могут быть использованы в новых научных и методических разработках в области моделирования, алгоритмизации и программирования для научной специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ, а также для направления подготовки 44.03.01 – «Педагогическое образование», модуль «Информатика, информационные технологии и вычислительная физика» и 09.03.02 – «Информационные системы и технологии».

Список используемых источников

1. Лаптев В. В., Швецкий М. В. Методическая система фундаментальной подготовки в области информатики. СПб. : Изд-во СПбГУ, 2000. 506 с.

2. Дьяконов В. П. Maple 10/11/12/13/14 в математических расчетах. М. : ДМК Пресс, 2011. 800 с.

3. Попов Ю. П., Самарский А. А. Вычислительный эксперимент // Компьютеры, модели, вычислительный эксперимент. М. : Наука, 1988.

4. Самарский А. А., Михайлов А. П. Математическое моделирование: Идеи. Методы. Примеры. М. : Наука. Физматлит, 1997.

5. Соколов Д. А., Сорокина И. В., Ходанович А. И. Математическое и компьютерное моделирование в учебных исследованиях : монография. Германия / Deutschland : LAP LAMBERT Academic Publishing, Saarbrucken, 2012. 125 с. (эл. издание).

6. Ходанович А. И. Демонстрационные примеры в теории сложности алгоритмов. Новые образовательные стратегии в современном информационном пространстве. Сб. науч. тр. СПб. : Изд-во РГПУ им. А. И. Герцена, «Лема», 2011. С 188–191.

7. Ходанович А. И. Классические парадоксы вычислительной физики в современной науке и образовании // Современные наукоемкие технологии. 2016. № 2 (Ч. 3). С. 585–588.

8. Ходанович А. И., Сорокина И. В., Скоморохов Д. С. Вероятностно-статистические методы и модели в учебном компьютерном эксперименте // Мир науки, культуры, образования. 2017. № 1 (62). С. 210–214.

9. Ходанович А. И. Приоритеты компетентностного подхода в современном медиаобразовании // Инновационные технологии в медиаобразовании. II Международная научно-практическая конференция : материалы. 29–30 мая 2017 г. СПб. : СПбГИКиТ, 2018. С. 19–22.

УДК 621.391.037.3

СИНГУЛЯРНЫЕ ЧИСЛА МАТРИЦЫ КАНАЛА С ЗАМИРАНИЯМИ И ИХ ВЛИЯНИЕ НА УЯЗВИМОСТЬ КРИПТОСИСТЕМЫ ДИНА-ГОЛДСМИТ

В. С. Старостин

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

Исследуется бесключевая криптосистема, предложенная ранее Дином и Голдсмит. Данная криптосистема предлагалась в работе этих авторов как весьма перспективная. Однако в статье группы авторов, опубликованной недавно в «Трудах учебных заведений связи», было показано, что эта криптосистема теряет свои положительные свойства если количество антенн перехватчика даже не на много превосходит количество антенн легальных пользователей. Настоящая работа подтверждает теоретически данный «парадокс» и поясняет его связь со свойствами сингулярных чисел матрицы замирающего канала.

физический уровень секретности, замирающий канал, сингулярное матричное разложение.

Криптосистема, предложенная в 2013 г. Дином и Голдсмит в работе [1] могла бы претендовать, на первый взгляд, на звание «Революции в криптографии». Действительно, она не требует какого-либо предварительного распределения ключей и обеспечивает доказуемую секретность, поскольку ее криптоанализ сводится к решению вычислительно трудной задачи на решетке [2]. В работе [3] DG-криптосистема была впервые проанализирована с точки зрения секретности и практической реализуемости. В частности, там было показано, что при одинаковом количестве приемных антенн у легального пользователя ($n_г$) и перехватчика ($n'_г$), а также при одинаковых (в среднем) свойствах легального канала и канала перехвата, легальные пользователи могут обмениваться информацией достаточно надежно, тогда как перехватчик, используя под-оптимальные методы приема (из-за нереализуемой сложности оптимальных методов), получает недопустимо большую вероятность ошибочного приема информации. Сомнительность допустимости условия $n'_г=n_г$, была впервые отмечена в работе двух австралийских ученых [4]. В частности, они показали, что при прочих равных условиях, неограниченное возрастание отношения $n'_г/n_г$ приводит к убыванию вероятности ошибки перехватчика к нулю, а, следовательно, и к компрометации DG-криптосистемы. В этой работе были получены приближенные асимптотические результаты, которые

не подтверждались каким-либо моделированием. В работе [5] это пробел был восполнен. Парадоксальным образом оказалось, что незначительное увеличение числа n приемных антенн нелегального пользователя по сравнению с числом m передающих антенн существенно увеличивает его шансы на правильную дешифровку. Попытаемся объяснить этот «парадокс».

Напомним сначала условия, необходимые для функционирования DG-криптосистемы, описанные в оригинальной работе [1] и повторенные в [3]. Легальные пользователи A и B связаны каналом с замираниями, математическая модель которого имеет вид:

$$z = Ay + e\,, \tag{1}$$

где $y \in R^{n_t}$ – вектор, передаваемый от A и B, $A \in R^{n_t x n_г}$ – матрица, описывающая распространение сигнала по легальному каналу связи.

Канал перехвата от A к перехватчику E описывается уравнением:

$$z' = By + e'\,.$$

В работе [1] предлагаются следующий метод «модуляции» (шифрования) сигнала и его «демодуляции» (дешифрования):

Сначала производится преобразование:

$$y = Vx\,, \tag{2}$$

где $V \in R^{n_t x n_t}$,– ортогональная матрица, входящая в сингулярное (SVD) разложение матрицы A легального канала, т. е. $A = USV^T$.

Подставляя (2) в (1), получим:

$$z = Ay + e = USx + e\,.$$

Далее легальный пользователь B, пользуясь знанием матрицы A, выполняет преобразование:

$$z'' = U^T z = U^T USx + U^T e = Sx + \tilde{e}.$$

Так как матрица U^T ортогональна, то эффективный шум $\tilde{e}$ остается некоррелированным, гауссовым. Поэтому оптимальная оценка сообщения x будет иметь вид:

$$x' = \arg\min \left\| z'' - Sx \right\|, \tag{3}$$

где ||…|| означает Евклидову норму.

Поскольку прямоугольная матрица S, взятая из SVD разложения, имеет «диагональную» форму, то дешифрование сообщения x по правилу (3) можно заменить эквивалентным предписанием:

$$x_i' = \arg\min \left\| z_i'' - s_i x_i \right\|,$$

где $s=(s_1, \ldots, s_{n_t})$ – диагональ матрицы S.

Перехватчик *E* принимает вектор:

$$z' = By + e' = BVx + e' = U'S'(V')^T x + e' = Cx + e', \quad (4)$$

где $C = U'S'(V')^T V$, $U'S'(V')^T$ – SVD разложение матрицы B канала перехвата.

Матрица C несингулярная с вероятностью 100 %. Умножая обе части (4) на C^{-1}, получим:

$$\tilde{z} = C^{-1}z' = x + C^{-1}e'. \quad (5)$$

Поскольку матрица C^{-1} не обязательно будет ортогональной, то $C^{-1}e'$ гауссовский вектор, компоненты которого, вообще говоря, зависимы. В этом случае декодирование трудная задача [2]. Однако, можно попытаться использовать под-оптимальный метод дешифрования:

$$x_i'' = \arg\min_{x_i} \left|\tilde{z}_i - x_i\right|, \; i = 1, 2, ..., n_t. \quad (6)$$

В работе [5] было проведено моделирование DG-криптосистемы при увеличении количества n_r' антенн перехвата и было показано, что при увеличении количества приемных антенн перехватчика всего на 9 %, вероятность ошибки перехвата, использующего под-оптимальное правило (6) линейной сложности и вероятность ошибок легального пользователя при использовании оптимального приемника, совпадают.

Рассмотрим, не умаляя общности, при пояснении парадокса случай, когда элементы передаваемого сообщения $x_i \in \{0; 1\}$.

В канале перехвата, причем в том числе и для случая $n_r' > n_t$, под-оптимальное правило решения (6) будет эквивалентно следующему:

$$x_i'' = \begin{cases} 0, \text{ если } \tilde{z}_i \le 1/2, \\ 1, \text{ если } \tilde{z}_i > 1/2. \end{cases} \quad (7)$$

где $\tilde{z}_i$– координаты вектора $\tilde{z}$ из (5).

Для вероятности правильного приема i-го символа сообщения x_i в канале перехвата получаем из (7) следующее выражение:

$$P\{x_i' = x_i\} \ge \frac{1}{2}\left(P\left\{e_i'' \le \frac{1}{2}\right\} + P\left\{e_i'' \ge -\frac{1}{2}\right\}\right),$$

где e_i'' – координата вектора $e'' = C^{-1}e'$.

Поскольку $e_i' \in N(0, \tilde{\sigma}_e^2)$, то $P\{x_i = x_i''\} = 1/2 + \Phi\left(1/2\sqrt{Var\{e_i''\}}\right)$. Здесь $\Phi(a) = \frac{1}{\sqrt{2\pi}}\int_0^a \exp(-\frac{t^2}{2})dt$ функция Лапласа:

$$Var\{e_i''\} = \tilde{\sigma}_e^2 \sum_{k=1}^{n_t} \frac{v_{ik}^2}{S_k^2}. \quad (8)$$

Отсюда следует, что вероятности ошибок увеличиваются с ростом дисперсии эффективного шума и уменьшением сингулярных чисел.

Последнее связано с тем, что с физической точки зрения амплитуда декодируемого сигнала пропорционально соответствующему сингулярному числу. В канале перехватчика соответствующую роль играет величина $1/\tilde{\sigma}_e\sqrt{\sum_{k=1}^{n_t}\frac{v_{ik}}{S_k^2}}$, обратная эффективному шуму, и которую можно назвать эффективным коэффициентом передачи сигнала и которая в под-оптимальном алгоритме играет роль эффективного сингулярного числа.

Таким образом, ошибки приема обусловлены нижней частью спектра сингулярных чисел (минимальными числами).

Известно [6] асимптотическое поведение наибольшего и наименьшего сингулярных чисел s_{max}, s_{min} случайной матрицы $A \in R^{m\times n}$ независимых, одинаково распределенных гауссовых величин с нулевым средним и единичным стандартным отклонением. Если при $n, m \to \infty$ m/n стремится к $y \in [0;1]$, то $s_{min}/\sqrt{n}$ сходится по вероятности к $1-\sqrt{y}$, а $s_{max}/\sqrt{n}$ сходится по вероятности к $1+\sqrt{y}$.

Отсюда следует, что если число приемных антенн n лишь незначительно превышает число передающих m, то $s_{min} \approx \frac{n-m}{2\sqrt{n}} \ll 1$, а вероятность ошибки при декодировании символа x_i велика, если $s_i = s_{min}$. Отсюда также следует, что с ростом числа приемных антенн уже при $n - m \approx \sqrt{m}$ $s_{min} \approx 1$ и увеличивается дальше примерно как $s_{min} \approx \sqrt{n} - \sqrt{m}$.

Быстрое увеличение сингулярных чисел с увеличением асимметрии $(n-m)$ канальной матрицы A_{mn} легко объяснить с помощью теории возмущений.

Пусть $A^T Ax = s^2 x$, где x единичный собственный вектор матрицы $A^T A$, а s соответствующее сингулярное число матрицы A. Увеличим число столбцов матрицы A на единицу, приписав ей, например, справа столбец $a = \begin{pmatrix} a_1 \\ \cdots \\ a_m \end{pmatrix}$: $A' = (A|a)$. Тогда для нахождения сингулярных чисел матрицы A' надо найти собственные числа матрицы $A'^T A' = A^T A + a^T a$. Если $n, m \gg 1$, а элементы матрицы A' имеют такие же статистические свойства, что и элементы A, то нетрудно показать, возмущение $\Delta A^T A = a^T a$ в среднем невелико. Тогда по теории возмущений:

$$\Delta s^2 \approx x^T \Delta A^T A x = x^T a^T a x = (ax)^2 = \left(\sum_{i=1}^{m} a_i x_i\right)^2.$$

Так как $\{a_i\}$ независимые случайные величины с нулевым средним и единичной дисперсией, то мы находим, что математическое ожидание сдвига s^2 будет равно

$$E(\Delta s^2) = E(\sum_{i=1}^{m} a_i x_i)^2 = \sum_{i=1}^{m} E(a_i x_i)^2 = \sum_{i=1}^{m} E(a_i)^2 \, {x_i}^2 = \sum_{i=1}^{m} {x_i}^2 = 1.$$

Таким образом наибольший относительный прирост сингулярных чисел достигается в нижней части спектра.

Также можно показать, что при большом числе антенн даже у квадратной матрицы число малых сингулярных чисел в среднем не велико. Это приводит к тому, что легальный пользователь будет ошибочно декодировать лишь малое число символов, а вероятность успеха будет велика [3, 5].

По-иному дело обстоит в нелегальном канале, в котором вероятность успеха декодирования зависит от вариации (8). Так как $\{v_{ik}\}$ ортогональная матрица, то нетрудно показать [4], что

$$\frac{\tilde{\sigma}_e^2}{S_{\max}^2} \le Var\{e_i''\} = \tilde{\sigma}_e^2 \sum_{k=1}^{n_t} \frac{v_{ik}^2}{S_k^2} \le \frac{\tilde{\sigma}_e^2}{S_{\min}^2}. \qquad (9)$$

При значительном превышении числа приемных антенн над числом передающих ($\frac{m}{n} = y \ll 1$) $s_{min}, s_{max} \approx \sqrt{n}$. Следовательно (9), для любого символа дисперсия эффективного шума будет мала, а вероятность правильного приема велика [3, 5].

Вариация шума (8) это линейная комбинация эффективных шумов в каждом «канале» k. Есть основания предполагать, что в среднем коэффициенты v_{ik}^2 одного порядка. Тогда, если $m \approx n$, то в спектре сингулярных чисел имеются малые значения, которые в сумме обратных квадратов $1/S_k^2$ дают значительных вклад, приводя к большой дисперсии эффективного шума и тем самым к большой вероятности ошибки.

Таким образом, даже небольшое в процентном отношении увеличение количество антенн перехватчика приводит к компрометации DG-криптосистемы.

Автор выражает глубокую признательность профессору В. И. Коржику за постановку задачи, внимание и помощь в работе.

Список используемых источников

1. Dean T. and Goldsmith A. Physical-Layer Cryptography Through Massive MIMO // Proceedings of the IEEE Information Theory Workshop, Spain, Sept., 2013. pp. 1–15.

2. Micciancio D. and Regev O. Lattice-based Cryptography in Post-Quantum Cryptography: Springer, 2009. pp. 147–191.

3. Коржик В. И., Яковлев В. А., Тихонов С. В. Вторая революция в криптографии: миф или реальность // Проблемы информационной безопасности, Компьютерные системы. 2015. № 4. С. 79–89.

4. Steinfeld R. and Sakad A. On Massive MIMO Physical Layer Cryptosystem // arXiv:1507.08015v1[csIT], 2015.

5. Коржик В. И., Старостин В. С., Герасимович А. С. Исследования бесключевой криптосистемы Дина-Голдсмит // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 48–54.

6. Edelman A. Eigenvalues and Condition Numbers of Random Matrix, M.I.T. Doctoral Dissertation, Mathematics Department, 1989.

УДК 621.371

ИССЛЕДОВАНИЕ И АНАЛИЗ ТЕХНОЛОГИИ ДЛЯ ИЗГОТОВЛЕНИЯ ГЕНЕРАТОРОВ ШУМА В АКУСТИЧЕСКОМ ДИАПАЗОНЕ

А. П. Степанов, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Акустический канал утечки информации является одним из основных при передаче конфиденциальной информации. Для защиты от утечки информации по данному техническому каналу применяются пассивные средства, служащие для ослабления акустических сигналов, циркулирующих в выделенном помещении и активные средства, формирующие акустический сигнал, скрывающий речь человека.

акустический канал утечки информации, генератор шума.

Передача информации от человека к человеку может осуществляться разными методами. Но основной способ – живое общение, при котором может происходить обмен конфиденциальной информацией. И чем выше должности у обменивающихся информацией людей, тем яснее становится необходимость применения средств для сокрытия информации. Особенно это относится к военной сфере, лежащая в основе построения государства.

Для маскирования полезного сигнала, передаваемого по акустическому каналу, применяют источники шума, такие, как: тепловые шумы резисторов, дробовые шумы *p*-*n*-переходов. Однако для данных источников характерны малая мощность шума, низкая временная и температурная стабильность параметров, неравномерность спектральных характеристик по частоте. Помимо этого, при замене одного шумящего элемента на другой, необходимо производить настройку. Эти недостатки отсутствуют у цифровых источников шума [1].

Генератор шума на *p*-*n* переходе транзистора представлен на рис. 1.

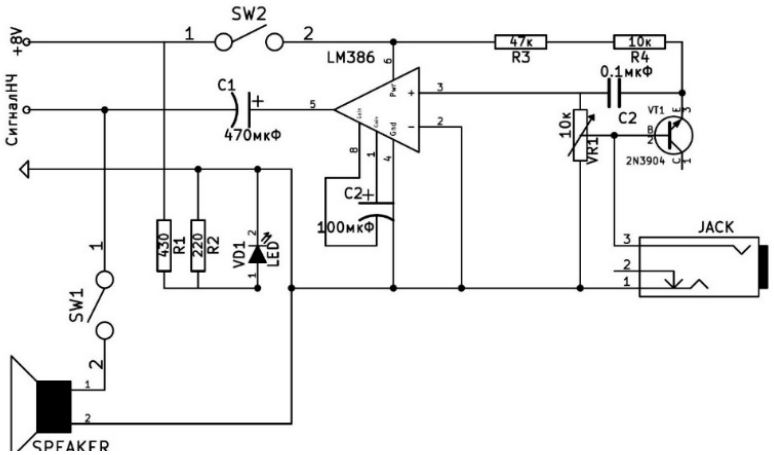


Рис. 1. Генератор шума на p-n переходе транзистора

Дробовой шум возникает на переходе база – эмиттер транзистора VT1. Переменный резистор VR1 позволяет регулировать ток через переход, т. е. уровень шума. Также данный резистор используется для управления внешним шумом. Итоговый сигнал усиливается микросхемой LM386 и попадает на динамик.

«Цифровой» шум представляет из себя временный случайный процесс, близкий по своим свойствам к процессам физических шумов. Цифровая последовательность двоичных символов в цифровых генераторах шума называется псевдослучайной последовательностью, представляющей из себя последовательность прямоугольных импульсов псевдослучайной длительности с псевдослучайными интервалами между ними. Период повторения всей последовательности значительно превышает наибольший интервал между импульсами. Наиболее часто применяются последовательности максимальной «длины» – *M*-последовательности, которые при заданном числе разрядов формирующего их регистра имеют максимальный период повторения.

Представленный генератор шума (рис. 2) содержит последовательный регистр сдвига, сумматор по модулю 2, тактовый генератор, цепь запуска и низкочастотные пассивные фильтры. Регистр с сумматором по модулю 2 образуют непосредственно формирователь *M*-последовательности. Цепь запуска предотвращает появление нулевой комбинации одновременно во всех разрядах регистра при включении питания. Фильтры служат для получения шумов с заданными спектральными свойствами [1].

Для защиты выделенных помещений применяют генераторы белого и розового шума, системы вибрационного зашумления, укомплектованные электромагнитными и пьезоэлектрическими вибропреобразователями. Качество данных систем оценивают повышением интенсивности маскирую-

щего воздействия над уровнем акустических сигналов. Величина превышения регламентируется руководящими документами ФСТЭК РФ [2].

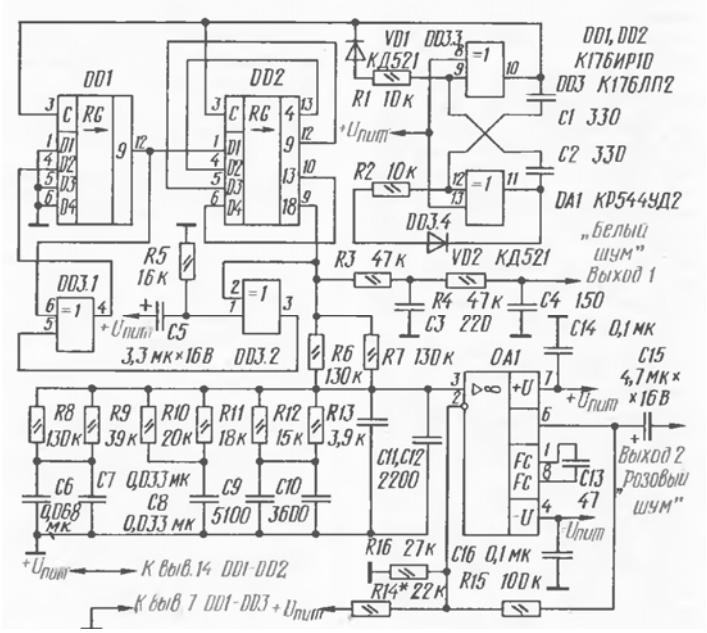


Рис. 2. Принципиальная схема цифрового генератора шума

Одним из известных генераторов является «Соната – АВ». Стабильность основных характеристик генератора обеспечивается применением цифровых формирователей шума. Стойкость создаваемой генератором заградительной помехи к различным методам её нейтрализации обеспечивается большим периодом используемых последовательностей и шумовой загрузкой регистров формирователя при включении питания.

Правильно установленная и отрегулированная система «Соната – АВ» позволяет нейтрализовать такие виды подслушивания, как:

1. Непосредственное подслушивание в условиях плохой звукоизоляции помещения.

2. Применение радио- и проводных микрофонов, установленных в полостях стен, в надпотолочном пространстве, вентиляционных коробах.

3. Применение стетоскопов, установленных на стенах (потолках, полах), трубах водо- (тепло-, газо-) снабжения.

4. Применение лазерных и микроволновых систем съёма аудиоинформации с окон и элементов интерьера.

Для построения системы защиты помещения требуется виброизлучатель и пьезоизлучатели [3].

Таким образом, применяемые в настоящее время генераторы шума позволяют уменьшить утечку информации по акустическому и виброакустическому каналам, они дают возможность собеседникам общаться, не думая о том, что их разговор станет известен третьим лицам. Однако

главный недостаток – дискомфорт, который испытывают те, кто находятся в сфере действия данного технического устройства. Это существенно сокращает время, в течении которого может длиться обмен информацией.

Список используемых источников

1. Мардер М., Федосеев В. Цифровые генераторы шума // Радио 1990. N 8. С. 68–71.

2. Бузов Г. А., Калинин С. В. Защита от утечки информации по техническим каналам. М .: Горячая линия – Телеком. 2005, 416 с.

3. Зайцев А. П., Шелупанов А. А. Технические средства и методы защиты информации. М. : Машиностроение. 2009. 512 с.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 075.80

ПРИМЕНЕНИЕ 3D-АНИМАЦИИ В ГИС ВОЕННОГО НАЗНАЧЕНИЕ

О. В. Стрелков

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В современное время решающим фактором является оперативное решение поставленных задач и правильное использование современных средств, для достижения положительного результата. Раньше использовались бумажные двухмерные карты, которые и сейчас не остаются во внимании, на них вручную наносятся объекты оперативной обстановки и по формулам вычисляют результаты каких-либо тактических решений. Задача состоит в том, чтобы показать наглядно движение объектов, указав их реальные характеристики, что позволит сократить время на принятие решений.

3D-анимация, геоинформационная система, программа, сценарий, моделирование, классификаторы трехмерных моделей.

Исследователями доказано, что большую часть информации человек воспринимает зрительным образом, то есть около 90 %, около 9 % информации воспринимается с помощью слуха и 1 % составляют другие органы чувств. Тем самым зрение играет очень важную роль для принятия решения от воспринимаемой человеком информации, что в свою очередь несет первостепенное значение на исход какой-либо операции в военное или

мирное время и может понести необратимые последствия как для народа, так и для государства в целом.

В военной деятельности: команда, задача или приказ должны излагаться до подчиненного кратко и четко, но в краткой форме или в письменной форме, возникают не мало важных вопросов, которые требуют уточнения для повышения вероятности на успех.

Что такое анимация?

Анимация – искусственное представление движения объекта в кино или в компьютерной графике путем последовательных отображений рисунков или кадров с частотой, при которой обеспечивается целостное зрительное восприятие образов или объектов [1].

Иными словами анимацией можно назвать оживление объекта.

3D-анимация – это трехмерное представление того же оживленного объекта.

Говоря о применении 3D-анимации в геоинформационной системе военного назначения, играет важную роль в XXI веке для визуализации военных действий или оперативной, тактической и других обстановок.

Применение анимации в геоинформационной системе, а точнее правильнее назвать использование сценариев, по которому будет действовать один или несколько объектов, увеличивает информативность и наглядность действий (движений) объектов в оперативной, тактической и других обстановках, что влияет на восприятие человеком с положительной стороны, а, то есть правдоподобней. Так как параметры можно настроить таким образом, что будут подходить к реальным условиям и показывать очень наглядно, нежели приводить какие-либо домысли или утверждения на тот или иной счет, чтобы убедить других участников в своей правоте того выбора действий, когда это все может показать ряд объектов, подстроенных под необходимый сценарий.

Конечно, к излагаемому можно предоставить какие-либо также факты, что увеличит вероятность на успех, но влияющим фактором есть и всегда будет оставаться зрительная часть, если не говорить, об иллюзиях, которые можно использовать при применении каких-либо аппаратах или средств, что может исказить визуальную картинку. Но в данной статье идет речь о применение в военной сфере, не то что можно применить против противника, а то, что позволит добиться успеха у начальников при проведении операции в военных условиях и добиться их поддержки. Так как в настоящее время решающим фактором на поле боя есть быстрое принятие решений.

В данной статье представлено описание создания 3D-анимации в ГИС «Оператор» для силовых структур, которое представлено ниже.

Как уже упоминал выше для создания 3D-анимации в ГИС «Оператор» используется сценарий, который применяется к одному или несколь-

ким объектам по определенной траектории, которая определяется совокупностью координат.

Для созданий сценария объекта, необходимо в первую очередь, чтобы 3D-модели были присвоены объектам на карте, то есть имелась уже трехмерная карта, которая запускается на основе двухмерной карты с трехмерными классификаторами объектов (описание этого вы можете найти в разделе 3 учебного пособия «Основы трехмерного моделирования элементов системы связи в геоинформационных системах военного назначения», второе издание [3]).

Сама настройка сценария осуществляется в окне отображения трехмерной модели, на которой расположены трехмерные объекты в соответствии с двухмерной картой. Как и в любом действии объекта, для создания его движения необходимо знать какие параметры он имеет для ряда характеристик, которые можно задать. Конечно, параметры уже изначально имеют значения по умолчанию, поэтому задавать все параметры нет необходимости, их можно уже редактировать по ходу работы, дабы более точно воспроизвести реальные условия или движения объекта.

Создание анимации, оно же сценария в ГИС «Оператор» имеет достаточно удобный и простой функционал для ее воспроизведения, по сравнению с программами, которые предназначены для создания трехмерных моделей и сцен объектов, а также создания анимации объекта. Такие программы как 3ds Max, Blender Foundation, и другие, не говоря о Unity3d, где необходимо программировать все параметры объекта.

Сравнивая эти программы, то для создания 3D-анимации в ГИС «Оператор» не требуется задавать количество кадров в секунду, выбирать расширение, указывать связи между объектами для взаимодействия и других параметров. Между тем, в ГИС «Оператор» есть основные особенности в оживление объекта, такие как: скорость движения, измеряющееся в километрах в час или задающееся по времени движения объекта, то есть начало или конец сценария, а также траектория движения и другие особенности, которые будут описаны ниже.

Для начала настроим параметры анимации и движения объекта, через меню «Параметры» – «Анимация» или «Движение» (не зависимо от выбора пункта, откроется окно со вкладками параметров).

В данном окне можно настроить ряд следующих параметров:

1. Размеры и масштаб.

2. Движение:

– при установке постоянной скорости при движении по 3D-модели отключается автоматическое изменение скорости перемещения при изменении масштаба модели. В ином случае скорость движения по модели подстраивается под изменение оператором масштаба модели для более удобного просмотра;

– при установке постоянной высоты при движении по 3D-модели сохраняется высота наблюдаемой точки (ориентира). В ином случае наблюдаемая точка (ориентир) движется с учетом высоты рельефа в текущем ее местоположении.

3. Текущие дата и время использующиеся для расчета высоты над горизонтом и азимута Солнца, а также:

4. Дополнительные параметры.

5. Сетка, что позволяет включить отображение координатной сетки определяющая в метрах.

Подробное описание каждого параметра можно найти на официальном сайте «КБ Панорама» [4].

Список используемых источников

1. Flash-технологии – 2 модуль. URL: http://24ikt.ru

2. Геоинформационная система «Карта 2011». Технология создания библиотеки трехмерных знаков тактической, оперативно-тактической обстановки. Панорама 1991–2013 Ногинск. 2013.

3. Иванов В. Г., Астахов А. И., Стрелков О. В. Основы трехмерного моделирования элементов системы связи в геоинформационных системах военного назначения: учеб. пособие**.** СПб. : ВАС, 2017. 144 с.

4. Сайт «КБ Панорама». URL: http://www.gisinfo.ru

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.65

СУБД POSTGRESQL И ЕЕ ПРИМЕНЕНИЕ ДЛЯ РАЗРАБОТКИ БАЗ ДАННЫХ В АСУ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А. А. Строков, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Анализ существующей проблематики применения сил специального назначения свидетельствует о том, что информационные аспекты выходят на первый план. Функциональная интеграция СУБД PostgreSQL в ОС Astra Linux внедряется в интересах повышения эффективности и защищенности применения систем специального назначения.

система управления базами данных, автоматизированная система управления, PostgreSQL, Astra Linux.

Автоматизированная система управления (АСУ) – комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия. АСУ применяются в различных отраслях промышленности, энергетике, транспорте, а также в области специального назначения.

АСУ специального назначения состоит из следующих составных частей:

- технического обеспечения (ТО);
- программного обеспечения (ПО);
- информационного обеспечения (ИО);
- организационного обеспечения (ОО);
- оперативного персонала (ОП).

Программное обеспечение АСУ – совокупность программ, необходимая для реализации функций АСУ, заданного функционирования комплекса технических средств АСУ и предполагаемого развития системы

Программное обеспечение АСУ подразделяется на общее ПО и специальное программное обеспечение.

Общее программное обеспечение АСУ поставляется в комплекте со средствами вычислительной техники. К общему программному обеспечению АСУ относятся необходимые в процессе функционирования и развития системы программы, программы для автоматизации разработки программ, компоновки программного обеспечения, организации функционирования вычислительного комплекса и другие служебные и стандартные программы (организующие программы, транслирующие программы, библиотеки стандартных программ и др.).

Специальное программное обеспечение АСУ разрабатывается или заимствуется из соответствующих фондов при создании конкретной системы и включает программы реализации основных (управляющих и информационных) и вспомогательных (обеспечение заданного функционирования системы, проверка правильности ввода информации, контроль над работой системы и т. п.) функций АСУ [1].

В данной статье мы рассмотрим специальное программное обеспечение для разработки АСУ специального назначения – СУБД PostgreSQL в ОС Astra Linux.

Актуальность использования СУБД PostgreSQL в ОС Astra Linux для АСУ специального назначения обусловлена, улучшенной системой зашиты данных, которая достигается путем применения встраиваемых

средств защиты информации, обеспечивающих, мандатное разграничение доступа и регистрацию событий безопасности (аудит).

PostgreSQL – это объектно-реляционная система управления базами данных (ОРСУБД, ORDBMS), основанная на POSTGRES, Version 4.2 – программе, разработанной на факультете компьютерных наук Калифорнийского университета в Беркли. В POSTGRES появилось множество новшеств, которые были реализованы в некоторых коммерческих СУБД гораздо позднее. PostgreSQL – СУБД с открытым исходным кодом, основой которого был код, написанный в Беркли. Она поддерживает большую часть стандарта SQL и предлагает множество современных функций:

- сложные запросы;
- внешние ключи;
- триггеры;
- изменяемые представления;
- транзакционная целостность;
- многоверсионность.

Кроме того, пользователи могут всячески расширять возможности PostgreSQL, например, создавая свои: типы данных, функции, операторы, агрегатные функции, методы индексирования, процедурные языки.

А благодаря свободной лицензии, PostgreSQL разрешается бесплатно использовать, изменять и распространять всем и для любых целей – личных, коммерческих или учебных [2].

Архитектура PostgreSQL разбита на 3 основные подсистемы:

1. Front End или клиентская часть системы, включающая в себя собственно клиентское приложение и библиотеку LIBPQ, реализующую интерфейс связи с сервером. Библиотека LIBPQ отвечает за установление соединения с сервером и передачу SQL-запросов.

2. Серверная часть, включающая в себя серверные процессы и контролирующий процесс-демон postmaster, отвечающий за взаимодействие с клиентами. Демон postmaster постоянно запущен в фоновом режиме на сервере. Он авторизует и принимает запросы от клиентов и осуществляет обмен данными между клиентом и сервером. При получении запроса соединения от клиента postmaster создаёт соответственный фоновый серверный процесс postgres, при этом используется связь один-к-одному. После того, как серверный процесс создан, клиент и сервер взаимодействуют напрямую.

3. Back End, включающий хранилище данных и средства управления хранилищем. Несколько серверных процессов могут одновременно иметь доступ к информации из хранилища.

После установления соединения, серверный процесс получает SQL-запросы в текстовом виде и трансформирует эти запросы в поток выходных данных.

Обработка запроса происходит в следующем порядке:

1. Парсер принимает запрос в виде текста в формате ASCII и проверяет его синтаксис, распознавая идентификаторы и ключевые слова. В результате работы парсера формируется дерево разбора, либо в случае неверного синтаксиса генерируется ошибка.

2. Далее за дело принимается служба контроля трафика. На этом этапе запрос идентифицируется как простой или сложный. Простые запросы перенаправляются непосредственно в модуль исполнения, сложные передаются через компоновщик планировщику/оптимизатору.

3. Компоновщик принимает дерево разбора запроса от парсера и преобразует его в альтернативную вспомогательную форму.

4. Сложный SQL-запрос может быть выполнен несколькими разными способами. Планировщик определяет наиболее оптимальный путь и передаёт управление модулю исполнения.

5. Модуль исполнения выполняет запрос оптимальным образом согласно дереву разбора, предоставленному планировщиком, и возвращает вывод в текстовом виде клиенту.

Взаимодействии с хранилищем данных которое осуществляется через службы доступа и загрузочный модуль предоставляет унифицированный доступ к серверным данным. С помощью сложной системы буферизации в хранилище возможен множественный доступ к одним и тем же таблицам параллельными запросами и процессами. Таким образом, хранилище является посредником между службами PostgreSQL и физическим диском, а также обеспечивает семафоры и блокировки файлов. На сервере PostgreSQL может существовать только одно хранилище.

Образец базы данных создаётся с помощью загрузочного модуля при первом запуске PostgreSQL. На этом этапе невозможно обращение к базе данных через обычные SQL-запросы.

Работа осуществляется через службу доступа к базе данных. Служба доступа отвечает за индексирование, сканирование, поиск, компиляцию и возвращение запрошенных данных.

Управление хранилищем включает в себя несколько независимых подсистем:

– Модуль сбора статистики – накапливает информацию о доступе к таблицам и индексам, вызовах серверных функций и командах, выполненных модулем исполнения. По запросу накопленная статистика передаётся другим процессам системы. В свою очередь, процессы системы периодически передают актуальные данные коллектору.

– Сборщик мусора Auto-Vacuum – набор процессов для автоматического освобождения неиспользуемой памяти в таблицах. Для принятия решения об очистке неиспользуемых данных сборщик мусора опирается на данные, полученные от модуля сбора статистики.

– Фоновый процесс записи логов – сохраняет логи произведённых операций и информацию для резервного восстановления системы в случае поломки. Все изменения, сделанные после последнего сохранения состояния системы, записываются в специальных лог-файлах [3].

Системные утилиты предоставляет некоторые общие функции для процессов серверной части. Системные утилиты доступны для всех подсистем сервера в фоновом режиме.

Необходимость применения данной СУБД в защищенных ОС и систем специального назначения обусловлена тем, что в дополнение к имеющимся средствам защиты в СУБД PostgreSQL встраиваются средства защиты информации, обеспечивающие, мандатное разграничение доступа, регистрацию событий безопасности (аудит).

Средства аудита доработанной СУБД PostgreSQL обеспечивают регистрацию следующих событий: использование идентификационного и аутентификационного механизма; запрос на доступ к защищаемому ресурсу; создание, уничтожение и изменение объектов СУБД; действия по изменению правил разграничения доступа.

Для каждого события регистрируется различная информация: дата и время; объект доступа, к которому применяется регистрируемое действие; субъект, осуществляющий регистрируемое действие; тип события; результат завершения события. [4]

На рисунке изображена диаграмма, демонстрирующая увеличение производительности СУБД PostgreSQL при работе в ОС Astra Linux.

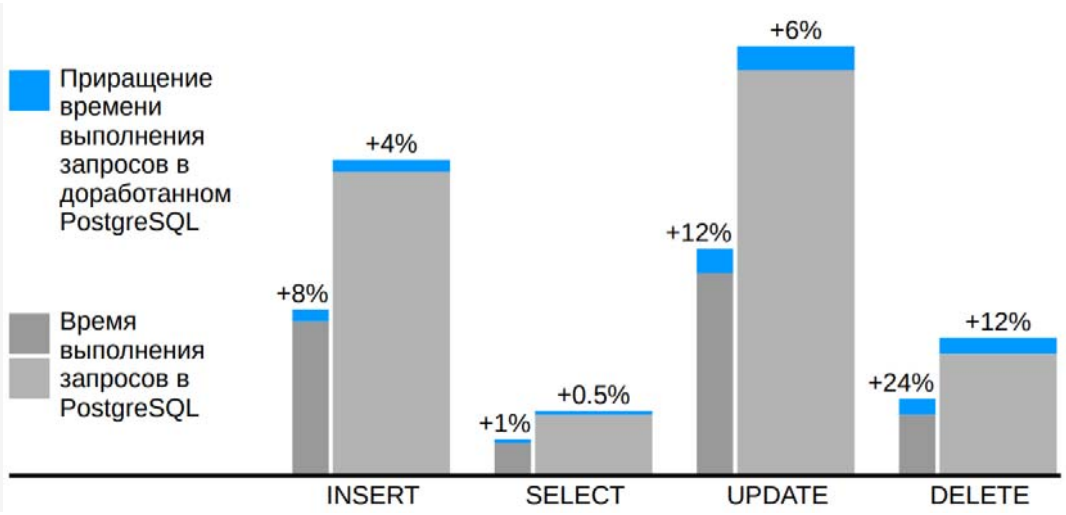


Рисунок. Диаграмма, демонстрирующая увеличение производительности СУБД PostgreSQL при работе в ОС Astra Linux

Если говорить о преимуществах PostgreSQL при разработке АСУ специального назначения, то, безусловно, это надежность транзакций и репликаций, возможность наследования и легкая расширяемость, а при работе в ОС Astra Linux это заметное увеличение производительности и дополнительные средства защиты информации (мандатное разграничение доступа, регистрацию событий безопасности). Очередным плюсом данной СУБД является отсутствие ограничений по максимальному размеру базы данных, по максимуму записей или индексов в таблице.

Таким образом, расширяется спектр проверенных временем и востребованных программных продуктов для создания защищенных решений для разработки автоматизированных систем специального назначения на базе ОС Astra Linux.

Список используемых источников

1. Описание структуры АСУ [Электронный ресурс] // Составные части АСУ URL: https://studfiles.net/preview/4520680/page:8/ (дата обращения 04.02.2018).

2. Концепция архитектуры PostgreSQL [Электронный ресурс] // Архитектура системы. URL: http://www.dataved.ru/2014/09/ postgresql.html (дата обращения 04.02.2018).

3. Что такое PostgreSQL? URL: https://postgrespro.ru/docs/ (дата обращения 04.02.2018).

4. СУБД PostgreSQL из дистрибутива операционной системы специального назначения "Astra Linux Special Edition" для обработки сведений, составляющих государственную тайну информации [Электронный ресурс] // Регистрация событий безопасности информации URL: https://pgconf.ru/media2015c/borisov.pdf (дата обращения 04.02.2018).

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Саенко.

УДК 004.49

ИССЛЕДОВАНИЕ АТАК ТИПА ПЕРЕПОЛНЕНИЕ БУФЕРА В 64-Х РАЗРЯДНЫХ UNIX ПОДОБНЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ

А. М. Суворов, А. Ю. Цветков

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

Атаки переполнения буфера используют уязвимости в стеке. Простейшая форма атак переполнения буфера принимает вредоносные пользовательские входные данные,

помещает их в стек и влияет на локальные переменные / возвращаемый адрес / аргументы, которые хранятся в стеке. Это может привести к изменению значений переменных или даже к изменению инструкций, которые вызывает программа. Худшие случаи таких атак могут привести к тому, что злоумышленники получат дистанционное управление вашей машиной по сети.

буфер, атака, UNIX, переполнение, ущерб, Linux, данные, информационная безопасность.

Введение

На сегодняшний день, переполнение буфера – это самая распространенная ошибка в приложениях и утилитах. В первый раз данная техника была применена в известном черве Роберта Морриса в 1988 г. [1]. С тех пор, данная уязвимость стала столь популярной, что число эксплоитов с каждым днем растет. Ежедневно обнаруживается огромное количество ошибок, связанных с переполнением буфера.

В общем, переполнение буфера является невероятно простым «багом», вытекающим из распространенной практики. Программы и утилиты часто работают с блоками данных, которые они берут с диска или читают с клавиатуры. Для работы с этими данными, программы выделяют блоки памяти с конечным размером – буферы. Переполнение буфера происходит в тот момент, когда записываются или читаются данные большего объема, чем вмещает буфер.

На первый взгляд, все это выглядит как очень глупая ошибка. Ведь, если программа знает размер это самого буфера, то должно быть не сложно удостовериться в том, что она никогда не положит в буфер больше, чем его размер. И это было бы правдой, если рассуждать таким образом. Однако, переполнение буфера продолжает усложнять жизнь специалистам по безопасности, а результаты такой атаки часто представляют огромную опасность для безопасности.

Для понимания почему происходит переполнение буфера и почему последствия могут быть плачевны необходимо знать, как программы используют память и как программисты создают свои утилиты.

Анализ

Необходимо уточнить, что переполнение буфера создает проблемы только в нативном коде, то есть в программах, которые обращаются к инструкциям процессора напрямую без посредников типа Java или Python.

Как уже было сказано, переполнение буфера – это большая проблема. По статистике она занимает 35–40 % [2] обнаруженных последнее время уязвимостей.

Разработчики Windows изменили свой подход к безопасности после двух основанных на переполнении буфера эксплойтов в начале двухтысячных. А в UNIX подобных системах были введены системы защиты. Такие как:

Стек canary – является случайным числом, размещенным в стеке сразу же перед указателем возврата стека. В случае переполнения буфера стека, значение canary будет перезаписано и программа сделает исключение.

Предотвращение выполнения данных (NX/DEP) – использует возможность контролировать исполняемый поток путем выполнения пейлоада, который хранится в стеке программы. DEP просто блокирует разрешение на выполнение стека программы, делая пейлоад невыполнимым и бесполезным [3].

Address Space Layout Randomization (ASLR) – рандомизирует пространство памяти программы таким образом, чтобы перезаписывание адресной ссылки команд с фиксированным местоположением в памяти не являлось таким полезным, т. к. будет отличаться каждый раз, когда программа запускается и не будет указывать на то, что могло бы быть показано для пейлоад или ROP приспособления [4].

Главным отличием переполнения буфера в системах с разрядностью 64 – это размер буфера программы. В следствии чего, эксплойду приходиться вносить больше данных в буфер программы для его переполнения. Пример стека представлен на рисунке.

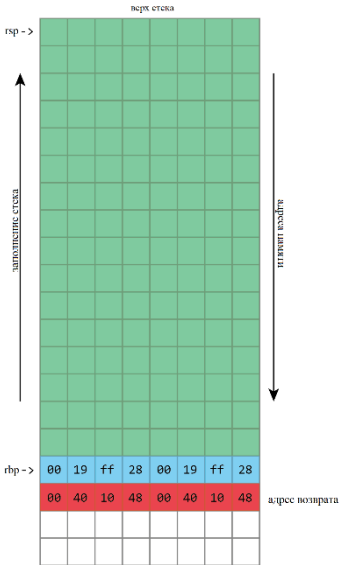


Рисунок. Буфер 64-х разрядной программы

Данные в такой стек записываются снизу-вверх. Внизу стека расположены адреса самого стека и адрес возврата, который и является целью атакующего. Этот адрес указывает на того, кто вызвал функцию или программу с данным стеком данных. По завершению работы, управление возвращается к вызывающему. Перезапись данного адреса даст злоумышленнику шанс перенаправить права управления на написанный им эксплойт, который выполнит необходимые действия и завершиться [5].

В общем имеется три регистра для программ. Эти регистры считаются основными. Понимание их значений является, по сути, основным фундаментом в понимании техники переполнения буфера.

Регистр RIP – служебный регистр. Указывает на текущую исполняемую инструкцию процессора.

Регистр RSP – это регистр, с помощью которого можно перемещаться по стеку. Т. е. обращаться к какому-либо адресу в стеке.

Регистр RBP – это регистр, который дает нам возможность прямого обращения к данным, находящимся в стеке [6].

Выводы

Таким образом, можно сказать, что переполнение буфера было, есть и в ближайшем будущем будет достаточно большой проблемой безопасности.

Если неумелый пользователь будет запускать программы с правами администратора, то злоумышленник может получить полный доступ к системе с привилегиями администратора. Это может повлечь за собой непоправимые последствия. От потери данных и их искажения, до полного удаления системы и выхода из строя компьютера.

Для предотвращения плачевного исхода необходимо вводить новые системы защиты. К примеру, в новом ядре Ubuntu x64 при переполнении регистров и попытке переписать адрес возврата он подменяется на стандартный адрес заложенный в систему. При таком сценарии управление будет передаваться операционной системе, а атакуемая программа будет завершаться с ошибкой, что никак не повлияет на работоспособность системы и целостность данных, хранимых на компьютере.

Но, как и всегда, основной проблемой будет оставаться беспечность пользователей, которые устанавливают непроверенные программы и запускают их с правами администратора. Следовательно, необходимо каким-то образом, не в ущерб комфорта пользователя, ограничивать его доступ к системным функциям, так что бы запускаемые им программы не имели прямого доступа к инструкциям процессора.

Список используемых источников

1. Переполнение буфера для чайников [Электронный ресурс]. URL: https://www.securitylab.ru/contest/212095.php

2. Как устроены дыры в безопасности: переполнение буфера [Электронный ресурс]. URL: https://habrahabr.ru/post/266591/

3. Локальное переполнение буфера в GNU Linux [Электронный ресурс]. URL: https://xakep.ru/2004/03/09/21497/

4. Переполнение буфера в ядре Linux [Электронный ресурс]. URL: https://xakep.ru/2005/03/29/26047/

5. Erick Leona, Stefan D. Brudaa. Counter-measures against stack buffer overflows in GNU/Linux operating systems [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S1877050916303039

6. Feng-Yi TANG, Chao FENG and Chao-Jing TANG. Memory Vulnerability Diagnosis for Binary Program. College of Electronic Science and Engineering National University of Defense Technology Changsha, China.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.3.05

ОБ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СИСТЕМАХ СТАЦИОНАРНЫХ УЗЛОВ СВЯЗИ

И. Г. Суржиков

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В данной статье обозревается состав и особенности инженерно-технических систем стационарных узлов связи в рамках подготовки решения по повышению эффективности их функционирования в части разработки и испытания автоматизированных систем мониторинга параметров инженерных сетей специальных объектов.

инженерно-технические системы, система электроснабжения, категории надежности, мониторинг.

Эффективность работы стационарных узлов связи (СУС) определяет надежность и качество функционирования телекоммуникационных сетей, их способность выполнять поставленные задачи и напрямую зависит от организации управления узлом связи, технической эксплуатации средств связи, автоматизированных систем управления (АСУ) и инженерно-технических систем (ИТС).

Условно ИТС можно разделить на подсистемы электроснабжения и освещения, вентиляции и кондиционирования воздуха, водоснабжения и канализации, отопления и горячего водоснабжения, сети кабельной канализации и структурированную кабельную систему, а также системы безопасности.

Основу функционирования ИТС составляет подсистема электроснабжения, отказ в работе которой приведет к отключению других подсистем и технологического оборудования СУС, прерыванию процессов обработки и передачи информации, а снижение качества электроснабжения может приводить к сбоям в работе отдельных систем и технологических процессов. Надежность электроснабжения обеспечивается совместной работой систем внешнего и внутреннего электроснабжения.

Система внешнего или общего электроснабжения включает в себя электроустановки, обеспечивающие электрическую связь с районом электрических сетей или магистральными электрическими сетями, и является основным источником электроэнергии СУС.

Система внутреннего электроснабжения представляет собой совокупность электроустановок для выработки, преобразования, распределения, передачи и потребления электрической энергии в границах балансовой

принадлежности и эксплуатационной ответственности СУС. В состав системы внутреннего электроснабжения входят автономные источники электроэнергии, установки гарантированного питания, распределительные устройства, преобразователи рода тока, напряжения и частоты, линии электропередачи и другие устройства.

Комбинирование работы данных систем позволяет обеспечить функционирование системы гарантированного энергоснабжения (СГЭ) и системы бесперебойного электроснабжения (СБЭ).

Потребители электроэнергии узла связи в зависимости от требований надежности электроснабжения подразделяются на три категории.

I категория – потребители, непосредственно обеспечивающие функционирование узла связи, прекращение электроснабжения которых может привести к нарушению связи либо создать опасность для жизни личного состава.

В зависимости от продолжительности допустимого перерыва в электроснабжении потребители I категории делятся на три группы:

1) группа I-А – потребители, абсолютно не допускающие перерыва в электроснабжении;

2) группа I-Б – потребители, допускающие перерыв в электроснабжении на время автоматического переключения источника электроэнергии;

3) группа I-В – потребители, допускающие перерыв в электроснабжении на время автоматического запуска и включения дизель-генератора.

II категория – потребители, перерыв в электроснабжении которых допускается на время, необходимое для включения резервного источника питания действиями личного состава дежурной смены.

III категория – все остальные потребители, не подпадающие под определение первых двух категорий.

Особенностью категорий I-А и I-Б является организация работы СГЭ и СБЭ. Питание потребителей I и II категорий должно осуществляться от двух независимых источников электроэнергии. Потребители III категории могут питаться от одного источника электроэнергии.

На случай падения мощности автономных источников электроэнергии на узле связи разрабатывается принудительный график нагрузки по электропитанию потребителей узла связи.

При питании от системы внешнего электроснабжения нормы качества электроэнергии определяются ГОСТ 32144-2013. При питании от системы внутреннего электроснабжения определяются требованиями эксплуатационной документации узла связи [1].

Система вентиляции и кондиционирования воздуха включает в себя воздухозаборные устройства, водяные или электрические калориферы, шумопоглощающие устройства, вентагрегаты, воздуховоды, кондиционеры, запорно-регулирующие устройства. Система предназначена для созда-

ния и поддержания необходимого температурно-влажностного режима и подразделяется на технологическую и общеобменную.

Система технологической вентиляции обеспечивает наиболее благоприятные параметры воздушной среды для осуществления технологического процесса. Система общеобменной вентиляции и кондиционирования воздуха предназначены для создания и поддержания внутри помещений микроклимата, благоприятного для самочувствия и работоспособности персонала. Требуемый температурно-влажностный режим обеспечивается работой систем вентиляции и кондиционирования воздуха по установленному графику.

Система водоснабжения включает в себя водозаборные сооружения, резервуары, насосы, подающие и отводящие трубопроводы, запорно-регулировочную арматуру, контрольно-измерительные приборы и другие устройства. Предназначена для обеспечения бесперебойной подачи воды потребителям необходимого количества, под заданным напором и требуемого качества.

Система отопления включает в себя источник теплоснабжения, подающие и отводящие трубопроводы, нагревательные приборы, запорно-регулировочную арматуру, устройства для удаления воздуха из системы и другие аппараты. Предназначена для создания в служебных и вспомогательных помещениях температурных условий, необходимых для нормальной деятельности личного состава и обеспечения требуемого температурного режима.

Требуемые температурно-влажностные параметры воздуха в помещениях узла связи нормируется по ГОСТ 12.1.005-88.

Для поддержания постоянной технической готовности средств связи, ИТС узла связи к использованию по предназначению выполняется ряд технических мер:

– своевременное и качественное проведение технического обслуживания, ремонта средств связи, АСУ, ИТС и контроль за их техническим состоянием;

– своевременное выявление и устранение причин, которые могут привести к нарушению или ухудшению качества связи, неисправности техники и линий связи, средств АСУ и ИТС;

– проведение плановых измерений параметров аппаратуры, каналов связи, средств АСУ, ИТС и доведение их до эксплуатационных норм;

– сбор, обобщение и анализ данных о состоянии технической эксплуатации на узле связи и разработку практических мероприятий по ее улучшению.

В целях организации эксплуатации составляются годовые планы эксплуатации и ремонта техники связи, средств АСУ и ИТС, плана подготов-

ки и проведения годового технического обслуживания техники связи, средств АСУ и ИТС [2].

Для обеспечения функционирования, мониторинга и управления оборудованием инженерных систем обычно применяют специализированные АСУ либо системы на базе универсальных промышленных контроллеров. Специализированные системы, как правило, ориентированы на управление конкретными технологическими системами освещения, отопления, вентиляции и кондиционирования и т. д. Алгоритмы управления процессами при этом определяются в программном обеспечении оборудования. За счет применения специализированных систем упрощается процесс управления отдельной подсистемой, однако это же делает более сложной интеграцию специализированного оборудования в единую систему централизованного мониторинга и управления.

Системы на базе универсальных программируемых промышленных контроллеров могут применяться как вместо специализированных систем, так и совместно с ними. Однако применение универсальных решений требует их адаптации к конкретной структуре и составу ИТС. Их задачей является автоматизация нестандартного оборудования и использование в качестве систем для мониторинга и управления разнородным инженерным оборудованием, которое по своим техническим характеристикам не обладает возможностью обмена информацией с внешними системами.

В настоящее время проблема обеспечения комплексного мониторинга параметров ИТС СУС является одной из наиболее актуальных при решении задачи по повышению надежности и эффективности функционирования СУС. Вопросы применения универсальных и специализированных систем мониторинга параметров ИТС, их адаптации, апробации предлагается решать с использованием разрабатываемого испытательного стенда для мониторинга параметров инженерных сетей.

Список используемых источников

1. Баринов М. А., Будко П. А., Виноградeнко А. М., Морозов Р. В., Бурлаков А. А. Электропитание устройств и систем телекоммуникаций : учебник для курсантов вузов связи / Под ред. проф. А. В. Мякотина. СПб. : ВАС, 2015. 470 с.

2. Кордюков Е. А., Кириллов В. М., Шакуров Б. Ф. Электроснабжение стационарных узлов связи. Ч. I–II. Л. : ЛВВИУС, 1988. 152 с.

Статья представлена научным руководителем, кандидатом технических наук, старшим научным сотрудником Е. В. Казакевич.

УДК 004.052.42+ 004.056.2

МЕТОД ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ НА ОСНОВЕ ВЕЙВЛЕТНЫХ КОДОВ

С. В. Таранов

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Коды, ориентированные на безопасность, занимают важное место в обеспечении целостности современных средств хранения и обработки информации. Одним из перспективных методов обеспечения целостности являются вейвлетные коды, способные обнаруживать алгебраические манипуляции. Данный метод способен не только выявлять внесенные злоумышленником ошибки любой кратности, но и обладает устойчивостью при неравномерных распределениях входных кодовых слов.

целостность, теория кодирования, надежные коды, вейвлет-преобразование.

Рассматриваемые в данной статье конструкции основаны на теории вейвлетных преобразований над конечными пространствами. Основы теории вейвлет-преобразований над конечными полями, в том числе для полей характеристики 2, представлены в [1, 2]. Разнообразные приложения вейвлетов над конечными полями можно найти в [3, 4, 5, 6]. Вейвлетное преобразование может быть рассмотрено как отображение исходного потока V_{m-1} на аппроксимирующую $V_{m-1} \to V_m$ и детализирующую $V_{m-1} \to W_m$ составляющие. Данные отображения зависят от коэффициентов масштабирующих и вейвлетных функций, что в итоге позволяет представить вейвлет-преобразование в виде двух циклических матриц:

$$H = cir_d(h_1, h_2, \dots, h_N),$$

$$G = cir_d(g_1, g_2, \dots, g_N),$$

где $h_1, \dots, h_N$ – коэффициенты масштабирующих функций, а $g_1, \dots, g_N$ – коэффициенты вейвлетов, d – сдвиг, равный порядку вейвлета.

Для матриц H и G, определяющих вейвлет-преобразование, необходимо определить еще ряд условий, при которых преобразование будет возможно. Рассмотренные матрицы должны удовлетворять:

1) условию биортогональности:

$$\begin{cases} \bar{H}H^T = I \\ \bar{G}G^T = I \\ \bar{H}G^T = 0 \\ \bar{G}H^T = 0 \end{cases}$$

где I – единичная матрица; $\bar{H}, \bar{G}$ – матрицы, состоящие из коэффициентов масштабирующих и вейвлетных функций и необходимые для обратного вейвлетного преобразования, то есть процессу реконструкции.

2) условию точного восстановления:

$$H^T \bar{H} + G^T \bar{G} = I.$$

Опишем алгоритм генерации кодовых слов для линейного вейвлетного кода. Обозначим исходную информационную часть как $x = (x_1, x_2, \dots, x_N)$. Кодовое слово, получившееся после преобразования, обозначим $c = (v, r)$, где $v = (v_1, v_2, \dots, v_{N/2})$ – информационная часть, а $r = (r_1, r_2, \dots, r_{N/2})$ избыточная часть.

При выполнении вышеописанных условий, множество всех кодовых слов линейного вейвлетного кода может быть задано с помощью порождающей матрицы, которая имеет вид:

$$c = x(H^T + aG^T J),$$

тогда проверочная матрица вейвлетного кода будет иметь вид:

$$c(\bar{H}^T + bJ^T \bar{G}^T) = 0,$$

где a, b некоторые вектора, принадлежащие полю $GF(q)$ и удовлетворяющие условию $ab = (p-1)\ mod\ p$, $p \in GF(q)$, $J = cir(0,1,0,\dots,0)$ – матрица размерности $N/2 \times N/2$.

Предлагаемый в данной статье метод обеспечения целостности в своей основе содержит описанную конструкцию линейного кода, применяемую совместно с преобразованием входных значений и дополнительным нелинейным преобразованием для избыточной части. Общая схема метода представлена на рис. 1.

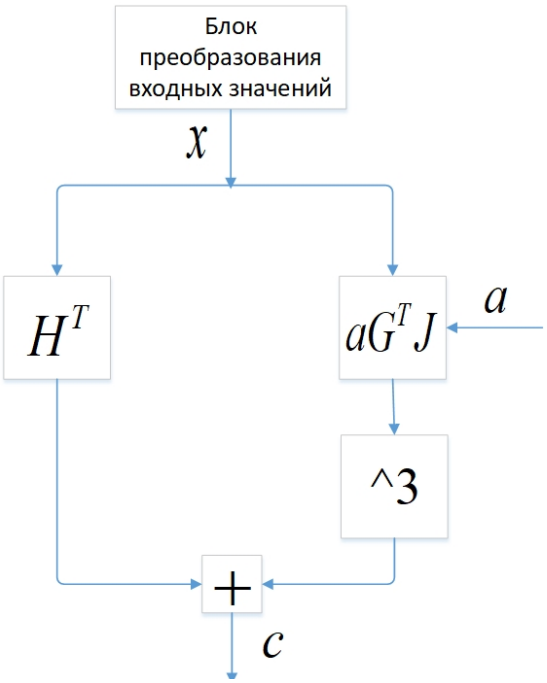


Рис. 1. Схема метода обеспечения целостности на основе вейвлетного кода

Для кодов, ориентированных на безопасность, используются отличные от принятых в теории кодирования критерии эффективности, а именно:

– количество необнаруживаемых ошибок. Данный параметр оценивает ошибки, которые не могут быть обнаружены помехоустойчивым кодом из-за особенности его структуры;

– вероятность маскировки ошибки. Вероятность маскировки ошибки e обычно обозначается как $Q(e)$ и определяется следующим образом:

$$Q(e) = \frac{\{x|x \in C, x + e \in C\}}{M},$$

где C – анализируемый код, x – кодовое слов из кода C, M – количество кодовых слов, $\{x|x \in C, x + e \in C\}$ – обозначает количество кодовых слов в коде C, возникновение ошибок в которых не будет обнаружено помехоустойчивым кодом. Вероятность маскировки ошибки ограничена неравенством $0 \leq Q(e) \leq 1$.

Коды, ориентированные на безопасность, обычно определяются через понятие *алгебраической манипуляции*, под которой понимается модель активного злоумышленника, имеющего возможность внедрять аддитивную ошибку в некоторое абстрактное устройство хранения. Внедряемая ошибка может быть любой кратности, а также может коррелировать с входными данными. При такой атаке в качестве метода обеспечения целостности принято использовать коды, ориентированные на безопасность, которые способны обнаруживать ошибки любой кратности. Данные коды обычно строятся на основе совершенно нелинейных или почти совершенно нелинейных функций, однако, вероятности маскировки в данных кодовых конструкциях могут расти при некоторых неравномерных распределениях. Сравнение производилось для программной модели системы обработки и сжатия видео ADV612. В данной системе уязвимыми к алгебраическим манипуляциям является содержимое оперативной памяти и регистров процессоров. В связи с тем, что входные значения для данной системы имеют неравномерное распределение, конструкции, являющиеся аналогами, уступают по параметру Q(e). На рис. 2 (см. ниже) представлено сравнение максимумов Q(e) для различных кодовых конструкций, применяемых для защиты от алгебраических манипуляций.

Как видно из рис. 2, при неравномерном распределении эффективность AMD кода на основе функции Маорана-МакФарланда [8, 9] (красная пунктирная линия) снижается. Вместе с тем вейвлетный AMD код [6] сохраняет характеристики, которые он имел при равномерном распределении, благодаря тому, что его информационные символы отличны от общепринятых комбинаций. Вейвлетный кубический код, описанный в данной статье. имеет более явные отклонения от своего поведения при равномерном распределении, однако, по-прежнему дает лучшие показатели $Q(e)$, чем его аналог – код на основе мультипликативного обратного [10]. При неравномерном распределении в некоторых конструкциях слабых AMD кодов таких, как код на основе мультипликативного обратного, могут появляться необнаруживаемые ошибки при больших значениях r (например, при r = 4). Однако конструкция кубического вейвлетного кода для рас-

сматриваемого распределения входных кодовых слов, свойственного системе ADV612, не имеет множества пропускаемых ошибок, что является ее преимуществом в данных условиях.

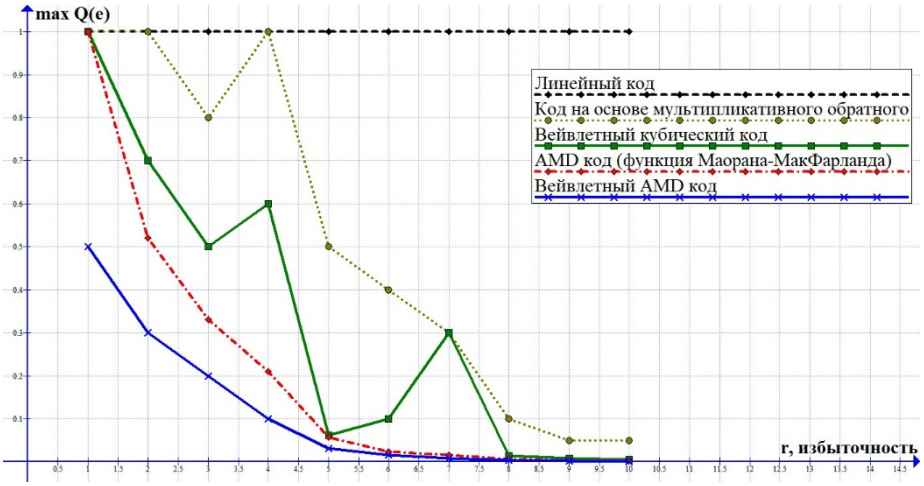


Рис. 2. Сравнение максимумов Q(e) при неравномерном распределении кодовых слов. Распределение составлено на основе наиболее вероятных регистров и вызовов функций в системе ADV612

Заключение

Метод обеспечения целостности на основе вейвлетных кодов, представленный в данной работе, учитывает большинство существующих уязвимостей, свойственных методам защиты, применяемым в модели алгебраических манипуляций. Блок преобразования входных кодовых слов, вместе с настройкой параметров a и b, позволяют подстроиться под возможные изменения входных кодовых слов и избежать снижения $Q(e)$, свойственного аналогичным конструкциям.

Список используемых источников

1. Caire G., Grossman R. L., Poor H. V. Wavelet Transforms Associated with Finite Cyclic Groups // IEEE Trans. Inf. Theory. 1993. Vol. 39. N. 4. pp. 1157–1166

2. Fekri F., Mersereau R. M., Schafer R. W. Theory of wavelet transform over finite fields, Acoustics, Speech, and Signal Processing // Proceedings IEEE International Conference on. 1999. Vol. 3. pp. 1213–1216.

3. Fekri F., McLaughlin S. W., Mersereau R. M., Schafer R. W. Double Circulant Self-Dual Codes Using Finite-Field Wavelet Transforms // Applied Algebra, Algebraic Algorithms and Error Correcting Codes Conference, Lecture Notes in Comput. Sci. 1999. Vol. 1719. pp. 355–364.

4. Fekri F., McLaughlin S. W., Mersereau R. M., Schafer R. W. Error Control Coding Using Finite-Field Wavelet Transforms // Center for Signal Image Processing, Georgia Institute of Technology. 1999. N. 30332. pp. 1–13.

5. Carlet C., Levina A. B., Taranov S. V. Algebraic manipulation detection codes with perfect nonlinear functions under non-uniform distribution // Научно-технический вестник

информационных технологий, механики и оптики. 2017. Vol. 17. No. 6 (112). pp. 1052–1062.

6. Levina A. B., Taranov S. V. New Construction of Algebraic Manipulation Detection Codes Based on Wavelet Transform // Proceedings of the 18th Conference of Open Innovations Association FRUCT. 2016. pp. 187–192.

7. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution // Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology. 2015. pp. 7060125.

8. Karpovsky M. G., Taubin A. New class of nonlinear systematic error detecting codes // IEEE Transactions on Information Theory. 2004. V. 50 (8). pp. 1818–1820.

9. Cramer R., Dodis Y., Fehr S., Padro C., Wichs D. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors // Lecture Notes in Computer Science. 2008. V. 4965. P. 471–488.

10. Wang Z., Karpovsky M. New error detecting codes for the design of hardware resistant to strong fault injection attacks // Proc. Int. Conference on Security and Management, SAM. Las-Vegas, USA, 2012.

Статья представлена научным руководителем, кандидатом физико-математических наук, доцентом А. Б. Левиной.

УДК 621.371

АНАЛИЗ РАЗВИТИЯ ВНЕШНЕЙ ПОЛИТИКИ В КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ ВОЙНЫ

М. А. Топкасов

Военная академия связи им. Маршала Советского Союза С. М. Будённого

За последние десятилетия многие страны в корне пересматривают формы и способы ведения войны. Приблизительно 20 лет назад, театр военных действий разделялся на две составляющих: обычное пространство и информационное, где предпочтение отдавалось обычному пространству, сейчас же, как отмечают военные эксперты этих стран, информационное пространство все больше рассматривается в качестве основной сферы военных действий.

информационная безопасность, средства защиты, связь, защита информации.

Специалисты и по сей день не знают, когда именно появилось словосочетание «информационная война» и когда впервые информацию стали рассматривать в качестве оружие. В связи с этим возникает ряд вопросов: когда возник термин и что он означает; какими средствами ведется информационная война и какие при этом ставятся цели?

Впервые термин «информационная война» употребил американский эксперт и советник по науке министерства обороны и Белого дома Томас Рона в своем отчете для компании “Boeing” под названием «Системы оружия и информационная война» в 1976 г. [1]. Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики [2]. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Публикация отчета послужила началом активной кампании в СМИ. Сама постановка проблемы весьма заинтересовала американских военных и уже с 1980 г. ВВС США начали активно обсуждать этот предмет. В дальнейшем термин начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г. в Ираке, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

В США под информационной войной понимается комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных для Соединенных Штатов решений, а в ходе войны полностью парализовало структуру управления противника. Одновременно с наступательным воздействием информационное противоборство предполагает обеспечение надежной защиты национальной информационной инфраструктуры США.

В настоящее время четко просматриваются два основных уровня реализации концепции информационной войны: государственный и военный (рис., см. ниже)

Как видно из схемы, информационная война включает в себя не только компьютерную войну, но и более широкий комплекс известных и нетрадиционных мероприятий по воздействию на противника.

Во время войны между Россией и Грузией в 2008 г., противостояние США и России в информационной войне резко обострилось. Каждая из сторон выдавали совершенно разные версии событий, что и продолжилось при государственном перевороте и гражданской войне на Украине в 2014 г., и при начале военных действий России в Сирии (по просьбе действующего президента Башар Асада) в 2015 г., которые длятся и сегодня. США и Россия развязали информационную войну, которая демонстрирует концепцию США в действии на государственном уровне и частично военном. Самые яркие примеры этого: политические, дипломатические и экономические санкции, и активная пропаганда против России, как угрозы безопасности Европы и Запада, а то и всему мировому сообществу.

Рисунок. Концепция информационной войны в США

Развитие и изучение проблемы информационных войн в нашей стране происходит в основном только в научных кругах. На государственном уровне данная проблема практически не разработана. Так, в «Концепции национальной безопасности Российской Федерации» всего лишь констатируется возможность угрозы национальной безопасности России в информационной сфере [3].

В «Концепции внешней политики Российской Федерации» особо подчеркивается, что в отношениях между государствами все большую роль играют, в том числе, информационные факторы, постепенно создается единое общемировое информационное пространство [4]. И, несмотря на это, в данном документе также отсутствует понятие информационных войн, нет упоминаний о политики информационных войн в отношении

других государств. Подводя итоги вышеизложенному, можно сделать два главных вывода:

1. На сегодняшний день не существует единого подхода к определению термина «информационная война», что в свою очередь говорит о важности изучения данного феномена.

2. В России на государственном уровне проблема информационных войн не достаточна разработана в правовых актах, что в дальнейшем может неблагоприятно сказаться на национальной безопасности России. Необходимо не просто законодательное закрепление понятия «информационная война», а также разработка мер противодействия информационному влиянию, направленному против Российской Федерации.

Список используемых источников

1. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. 2001. № 1. С. 2–9.

2. Колесов П. Ведение Соединёнными Штатами информационных войн. Концепция «Стратегических коммуникаций» // Зарубежное военное обозрение 2010. № 6. С. 9–14.

3. Панарин Н. Н. Информационная война за будущее России. М. : Горячая линия – Телеком, 2008. 256 с.

4. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно психологической войны. 2-е изд., стереотип. М. : Горячая линия – Телеком, 2007. 203 с.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 004.051

ЭРГОНОМИКА В WEB-ДИЗАЙНЕ

Е. С. Хайбрахманова, А. А. Шиян

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

Статья посвящена взаимосвязи эргономики и web-дизайна. Эргономика позволяет сформировать принципы и требования к web-интерфейсу. Благодаря чему web-ресурс становится эффективным человеко-машинным интерфейсом.

эргономика, информационный ресурс, дизайн, человеко-машинный интерфейс.

Человеко-машинный интерфейс является широкой концепцией. Чтобы понять эту концепцию, необходимо выяснить, что представляет собой понятие интерфейс. Слово интерфейс (от англ. – поверхность раздела, перегородка) определяет место или способ соединения, соприкосновения, связи. Это слово стало популярным в эпоху компьютеризации, но его смысл относится к сопряжению интерактивных систем. Интерфейсы являются основой для взаимодействия всех современных информационных систем. Если интерфейс любого объекта (персонального компьютера, программы, функции) не изменяется (стабилен, стандартизирован), он позволяет изменить сам объект, не заменяя принципы взаимодействия с другими объектами, из чего вытекает концепция пользовательского интерфейса [1]. Пользовательский интерфейс представляет собой набор ресурсов, в которых пользователь взаимодействует с различными устройствами. Разобрав понятие интерфейс можно перейти к человеко-машинному интерфейсу. Так что же представляет собой человеко-машинный интерфейс? Человеко-машинный интерфейс – это широкое понятие, которое включает в себя инженерные решения, обеспечивающие взаимодействие оператора с управляемыми им машинами.

Создание систем человеко-машинного интерфейса тесно связано с эргономикой. Эргономика (или человеческий фактор) – это научная дисциплина, занимающаяся изучением взаимодействия между людьми и другими элементами систем, и профессия, которая использует теорию, законы, данные и методы конструирования в целях обеспечения здоровья человека и оптимизации общего функционирования системы. Эргономичный сайт – это сайт, созданный на основе научных знаний об устройстве и работе человеческого глаза, просматривающего, собирающего информацию (для последующего анализа) с источника излучения определённой спектральной интенсивности, ограниченного по полю обзора. Эргономичный сайт обеспечивает необходимые удобства посетителю, сохраняет его силы, здоровье и работоспособность (рис. 1). А это, в конечном итоге, повышает эффективность сайта.

Для того, чтобы правильно организовать информацию на странице, рекомендуют использовать несколько стандартных и отработанных приемов, чтобы визуально разделить элементы на страницы и использовать принцип контраста. Это может быть цветовой контраст, контраст шрифтов, фонов и другие. Использовать в web-дизайне приемы композиции промышленного дизайна и выравнивать все элементы страницы (текст, графику) по визуальным направляющим осям (вертикальные и горизонтальные). Так же не стоит забывать о пустом пространстве (так называемый воздух), во избежание загруженности страницы визуальной информацией. Целесообразно при верстке макета использовать модульную сетку (рис. 2).

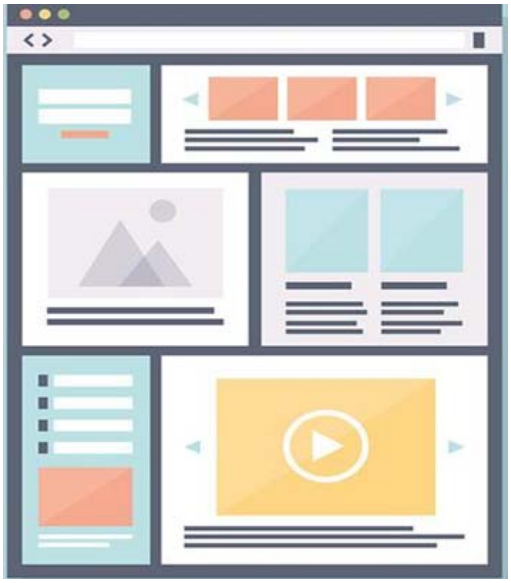


Рис. 1. Пример правильного макета сайта

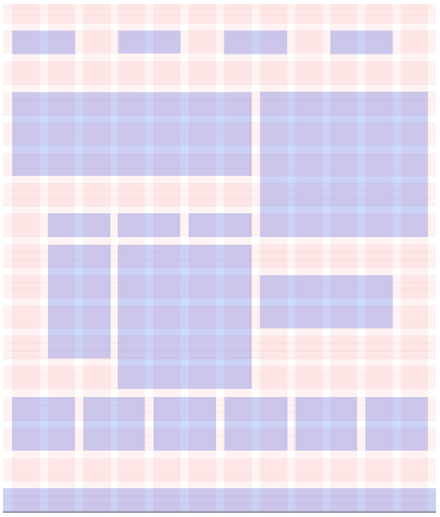


Рис. 2. Модульная сетка

Совместной задачей дизайна и эргономики является построение простого и функционального информационного ресурса. В первые 5–10 секунд формируется отношение пользователя к информационному ресурсу, благодаря чему пользователи в дальнейшем делятся на два вида, которые остаются на сайте и находят нужную им информацию, и другая категория, которая уходит с сайта, потому что им не понравилось. Основными критериями эргономики и web-дизайна для построения информационного ресурса являются:

– лаконичность (простота, не перегруженность). Лаконичный сайт укрепит доверие к организации. Не рекомендуется использование анимированных изображений, они должны быть закреплены за важными сообщениями, так как привлекают внимание пользователя;

– четкость (ясность, расположение, однородность структуры, осязаемость информации). Доказано, что печатный текст труднее читать с монитора, чем с бумаги (занимает на 25 % больше времени). Таким образом, текст должен быть достаточно разграничен, структурирован по параграфам и заглавиям для облегчения текста. Информация должна быть расположена по степени важности. Важная информация должна находиться вверху страницы, с применением иерархии Z и F паттернов. URL страницы должен быть видимым и понятным, что позволяет знать, где ты находишься и легко вернуться на эту страницу. Информация должна иметь такие данные, как имя автора, дату последнего обновления и дату публикаций;

– скорость (время загрузки, оптимизация графического контента). Хорошей идеей является оптимизация размера изображений, выбирая подходящий размер и цвета. Рекомендуется не загружать изображения более

30–40 Кб (можно предложить скачать изображения более высокого качества);

– взаимодействие (гипертекстовые ссылки, сегментация информации, содействие взаимодействию). Интерактивность – это возможные взаимодействия между пользователем и web-сайтом. Гипертекстовые ссылки предлагают пользователям широкие возможности в этой области и дают посетителям несколько путей, которые они могут использовать по своему усмотрению;

– адаптивность (изменение размера шрифта). Разработчику рекомендуется не использовать шрифты, размерность которых выражена абсолютно.

– доступность (всеобщий доступ, взаимодействие, принцип прозрачности, подпись изображений, правильность использования стилей, контраст, выбор цвета). Доступность означает возможность любым пользователям, включая слабовидящих и слепых людей, иметь доступ к web-сайту, то есть придерживаться определенных правил доступности, чтобы дать доступ большему количеству людей, независимо от их аппаратных средств. Вместо изображений должна присутствовать подпись. Это необходимо для того, чтобы слабовидящие люди поняли смысл изображения. Цвета должны быть подобраны таким образом, чтобы люди с недостатком зрения (не различающие некоторые цвета) могли с легкостью распознать, что изображено на сайте. Информация должна быть доступна даже без стилей. Между цветом, фоном и текстом должен быть достаточный контраст, чтобы слабовидящие люди могли прочитать текст. Размер шрифта не должен быть настолько мал, чтобы утомлять глаза и делать текст неразборчивым [1].

Эргономика и web-дизайн являются одним целым, поскольку основным признаком качества информационной системы является дружественный интерфейс по отношению к пользователю. Многие разработчики придерживаются мнения, согласно которому основное внимание при создании нового информационного ресурса следует уделять функциональному удобству, а эстетическая привлекательность является желательным, но не обязательным свойством, однако практика показывает, что между красотой и удобством существует самая непосредственная связь, более того, визуальная привлекательность в некоторых случаях способна компенсировать неудобства использования. Ничем не привлекательная с эстетической точки зрения программа может не найти дороги к широкому пользованию.

Список используемых источников

1. Уолтер А. Эмоциональный веб-дизайн. М. : Иваноф и Фербер, 2012. 160 с.

2. Кузнецов А. М., Мартынов В. В. Требования к графическому дизайну и юзабилити образовательных порталов. М. : Просвещение, 2003. 320 с.

УДК 004.057.5

КОМПЛЕКТ ПЕРЕНОСИМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОДДЕРЖКИ ПРЕПОДАВАНИЯ ИНФОРМАЦИОННЫХ ДИСЦИПЛИН

М. П. Чаунин

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

Предлагается вариант создания переносимого программного обеспечения, которое может быть использовано в преподавании дисциплин информационного цикла. Предлагаемый пакет содержит, в частности, средства разработки приложений на языках C/C++, Java, Python, Perl. Он не требует установки в операционной системе Windows и может быть размещен на локальном жестком диске или любом съемном носителе.

переносимое (автономное) приложение, оболочка операционной системы, переменные среды.

Преподавание дисциплин, связанных с использованием программного обеспечения (ПО), предполагает, что соответствующее ПО установлено, настроено и не требует специальных разрешений для эксплуатации, например, привилегий администратора. В реальности административный персонал, отвечающий за предоставление подобных услуг, по разным причинам не всегда может их предоставить. В этом случае для обеспечения приемлемого качества учебного процесса преподаватель вынужден не только готовить методические материалы курса, но и собственный комплект переносимого программного обеспечения. Условимся, что переносимое программное обеспечение – это ПО, которое не требует установки для своего запуска, может запускаться с различных носителей (USB флеш-диска, жесткого диска), вносит минимальные изменения в операционную систему и максимально приближено по функционалу к инсталлируемой версии. Сложность реализации переносимого приложения зависит от операционной системы. Ограничимся рассмотрением операционных систем семейства Windows, как наиболее распространенных.

Сформулируем требования к переносимому приложению, учитывая условия его возможного применения.

– Приложение не требует процедуры установки и может полностью храниться на любом носителе информации.

– Приложение является некоммерческим – не имеет лицензионных ограничений на его использование.

– Приложение может работать в условиях ограничений, налагаемых групповой политикой, таких как: *Запретить использование командной строки, Запретить обработку сценариев в командной строке*.

– Используются готовые решения, не требующие разработки собственного программного кода.

Сформулированные требования порождают следующую группу вопросов:

– Какие приложения можно сделать переносимыми?

– Какие средства существуют для преобразования инсталлируемого приложения в переносимое?

– Существуют ли доступные источники готовых к использованию переносимых приложений?

– Как настроить среду для выполнения уже имеющихся переносимых приложений?

Приложения Windows существенно различаются по готовности к преобразованию в переносимый формат. Значение имеют, например, следующие характеристики приложения: сохраняет ли приложение свои настройки в системном реестре или профиле пользователя, использует ли конфигурационные *ini*-файлы, можно ли изменить настройки приложения во время запуска при помощи параметров командной строки.

Некоторые приложения изначально спроектированы как переносимые, другие можно преобразовать в переносимый формат, используя принцип выявления внесенных изменений в системе. В виртуальной среде (*VMware Player, Oracle VirtualBox*) создаются снимки состояния системы до и после установки приложения. В результате сравнения снимков выявляются ресурсы (разделы реестра, системные папки), необходимые для запуска приложения. Если возможно, создаются виртуальные аналоги этих ресурсов для обеспечения работы автономного приложения. Наибольшие трудности возникают при создании виртуальных ресурсов для следующих типов приложений [1]:

– приложения, изначально спроектированные для иной операционной системы, например, Linux;

– дополнительные модули, в том числе библиотеки dll, которые встраиваются в приложение другого производителя, расширяя его функциональность;

– приложения, взаимодействующие с системными службами Windows;

– приложения, требующие установки драйверов устройств;
– приложения с аппаратной защитой от копирования.

Для создания переносимых приложений на рынке имеется множество программных средств, часть которых доступна для свободного некоммерческого использования: VMware ThinApp [2], Cameyo [3], Evalaze [4], Enigma Virtual Box [5] и др.

В сети Интернет существуют сервисы переносимых приложений, предоставляющие готовые решения, наиболее известным из которых является PortableApps.com [6]. Проект PortableApps.com предлагает более 300 готовых переносимых приложений и платформу для управления ими. Платформа поддерживает собственный формат переносимого приложения и включает менеджер, управляющий установкой, обновлением и запуском приложений. Кроме указанного сервиса в сети существует множество других источников переносимых приложений.

Многие переносимые приложения требуют дополнительной настройки, в частности задания переменных среды. Переменные среды задаются в реестре Windows. Каждая переменная среды хранит некоторую информацию о системе, например, переменная PATH содержит набор каталогов, в которых расположены исполняемые файлы.

Пользователь запускает приложение, в том числе и переносимое, используя оболочку – интерфейс для взаимодействия с функциями операционной системы. В операционных системах Windows существуют две оболочки: процесс Explorer с графическим интерфейсом пользователя и приложение cmd.exe с интерфейсом командной строки.

Процесс Explorer предоставляет пользователю визуальную среду управления, включающую в себя *Рабочий стол, Меню Пуск, Панель задач*, а также функции управления файлами. Процесс Explorer получает свой набор значений переменных среды во время его запуска и не может менять эти значения.

Приложение cmd.exe – интерпретатор командной строки – предназначено, в основном, для запуска консольных приложений, которые хранятся в каталогах, определенных в переменной среды PATH. При помощи команды set, запущенной в интерпретаторе команд cmd.exe, можно задать новую переменную среды или изменить значение существующей. Системные администраторы часто из соображений безопасности средствами групповой политики запрещают запуск приложения cmd.exe. В этом случае основная трудность в настройке комплекта переносимых приложений заключается в отсутствии интерфейса командной строки и невозможности задать необходимые значения переменных среды. Оба препятствия можно преодолеть путем использования следующих переносимых приложений.

– Эмулятор терминала ConEmu [7].
– Файловый менеджер Far [8].

Эмулятор терминал ConEmu изначально был создан для поддержки файлового менеджера Far. Он представляет графический интерфейс для запуска консольных приложений, каждое приложение в отдельной вкладке окна ConEmu. Для каждого консольного приложения, запускаемого в ConEmu, весь ввод и вывод перехватывается и перенаправляется в окно ConEmu. Одновременно может быть запущено несколько консольных приложений в разных вкладках. Приложения с графическим интерфейсом также можно запускать при помощи эмулятора ConEmu, в этом случае окно приложения будет «привязано» к вкладке ConEmu. Важным свойством приложения ConEmu является возможность задать при его запуске набор переменных среды, которые будут наследоваться всеми приложениями, запускаемыми в ConEmu.

Файловый менеджер Far – консольный файловый менеджер, обладающий многими полезными свойствами, расширяемыми за счет дополнительных подключаемых модулей. Он предоставляет пользователю интерфейс командной строки, независимый от интерпретатора cmd.exe.

На основании вышеизложенного процесс создания и использования переносимого пакета ПО может состоять из следующих шагов.

– Подготовить необходимый набор переносимых приложений, используя готовые решения или доступные инструментальные средства.

– Включить в состав набора приложения ConEmu и Far.

– Задать создание необходимых переменных среды при запуске ConEmu. Настроить ConEmu на запуск по умолчанию приложения Far.

– Запускать отдельные приложения из файлового менеджера Far или в отдельных вкладках эмулятора ConEmu.

Описанный подход апробирован автором. В состав переносимого пакета были включены средства для разработки приложений на языках C/C++, Java, Python, Perl и множество служебных программ.

Список используемых источников

1. Принципы работы Portable-программы и подготовка компьютера к её созданию [Электронный ресурс]. Режим доступа: http://servis2010.ru/portabelizatsiya/3147-printsipy-raboty-portable-programmy-i-podgotovka-kompyutera-k-ejo-sozdaniyu.html (дата обращения 27.03.2018).

2. Virtualize Applications with ThinApp and Streamline App Delivery and Management [Электронный ресурс]. Режим доступа: https://www.vmware.com/products/thinapp.html (дата обращения 27.03.2018).

3. Application Virtualization [Электронный ресурс]. Режим доступа: https://www.cameyo.com/ (дата обращения: 27.03.2018).

4. Evalaze application virtualization [Электронный ресурс]. Режим доступа: http://www.evalaze.de/en/home/ (дата обращения: 27.03.2018).

5. The Enigma Protector – Software Protection, Software Licensing and Software Virtualization system [Электронный ресурс]. Режим доступа: http://www.enigmaprotector.com/en/aboutvb.html (дата обращения 27.03.2018).
6. PortableApps.com – Portable software for USB, portable, and cloud drives. [Электронный ресурс]. Режим доступа: https://portableapps.com/ (дата обращения 27.03.2018).
7. ConEmu – Handy Windows Terminal [Электронный ресурс]. Режим доступа: https://conemu.github.io/ (дата обращения 27.03.2018).
8. Far Manager Official Site [Электронный ресурс]. Режим доступа: https://www.farmanager.com/ (дата обращения 27.03.2018).

УДК 004.031.42

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНА ВОЕННОГО УПРАВЛЕНИЯ

Д. М. Шадрин, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В данной статье рассматриваются основные принципы построения систем поддержки и принятия решений, их структура, возможности и решаемые ими задачи. Также рассматривается возможность применения систем поддержки принятия решений для организации информационного взаимодействия должностных лиц военного управления.

системы поддержки принятия решения, информационное взаимодействие, военное управление, информационные технологии.

В настоящее время практически все процессы, связанные с управлением, в той или иной мере осуществляются с использованием компьютерных автоматизированных систем. Особенно актуальным использование таких систем становится в процессе оперативного военного управления, поскольку такие системы позволяют за короткий срок получить полую и актуальную сводку информации по интересующему вопросу, что ведёт к значительному повышению обороноспособности страны.

Системы, предназначенные для помощи должностным лицам, принимающим решение в сложных условиях для полного и объективного анализа предметной деятельности, называются системами поддержки принятия

решений (СППР). Использование таких систем предполагает применение комплекса технических, программных, организационных и прочих методов и средств с целью полного или частичного высвобождения человека от непосредственного участия в получении, передаче, хранении, обработке и использовании материалов, энергии и информации.

СППР помогает людям, принимающим решения, на разных этапах этого процесса, включая исследование проблем, формулирования, определения альтернатив решения и ограничений решений, а также структурирования предпочтений и суждений о компромиссах. При этом окончательное решение выносится именно человеком, а компьютерная система лишь даёт собирает информацию, необходимую для принятия решения. Она освобождает пользователей от деталей технической реализации, позволяя им сосредоточиться на основополагающих суждениях.

Всю структуру СППР, несмотря на её высокую сложность, можно разделить на несколько основополагающих подсистем, которые составляют основу классической структуры СППР, отличающей ее от других типов информационных систем:

– интерфейса пользователя, который дает возможность лицу, которое имеет право принимать решения, проводить диалог с системой, используя разные программы ввода, форматы и технологии вывода;

– подсистемы, предназначенной для ввода, сохранения, управления, выбора, отображения и анализа данных;

– подсистемы, которая содержит набор моделей для обеспечения ответов на множество запросов пользователей, для аналитических задач.

С точки зрения потока данных и их преобразования, структуру СППР можно представить следующим образом [1]:

1. Подсистема сбора – загрузка и консолидация данных из разнородных ресурсов:

– сбор и структуризация нечетких сведений;

– загрузка данных приложений, корпоративных и наследуемых систем;

– измерительная информация объектов контроля в РМВ;

– выделение наиболее значимых данных;

– очистка (фильтрация), повышение качества, достоверности данных, сжатие (формирование существенных) наборов данных.

2. Подсистема хранения – оперативное и долговременное хранение:

– разделение информации для оперативной обработки и решение задач интеллектуального анализа;

– оптимизация данных;

– формирование базы данных информации;

– наполнение базы знаний;

– использование единой системы справочников, классификаторов.

3. Подсистема обработки и анализа – интеллектуальный анализ данных (ИАД):

– информационно-поисковый анализ;

– оперативная аналитическая обработка (OLAP – *On-line Analytical Processing*);

– комплексное имитационное моделирование;

4. Подсистема прогнозирования и предиктивной аналитики:

– анализ текущих и исторических данных с целью прогноза;

– определение критериев, влияющих на прогнозируемые события;

– построение модели предиктивной аналитики;

– аналитика «по запросу».

5. Подсистема генерации решений – генерация и выбор решений, генерация планов, объяснительная возможность:

– логический вывод рекомендаций на основе онтологии предметной области;

– выбор оптимальных альтернатив решений;

– обоснование сформированных выводов и решений.

6. Подсистема визуализации и отчетности – интерпретация знаний:

– интерактивная визуализация (инфографика), таблицы, тренды, диаграммы,

– 2D-, 3D-мнемосхемы;

– пространственная визуализация (интеграция с ГИС);

– использование инструментальных панелей;

– использование типовых форм отчётности

Для реализации полноценной СППР должны быть решены следующие задачи [2]:

– создание единого признакового пространства и показателей, характеризующих состояния объекта управления на базе централизованного информационного хранилища данных, обеспечивающего накопление, хранение и доступ к экспертным и историческим данным;

– интеграция существующих локальных баз данных в рамках централизованного информационного хранилища данных;

– сбор, накопление и применение знаний опытных экспертов в распределенных базах знаний для формирования выводов и рекомендаций;

– постоянный мониторинг (комплексный анализ) текущей ситуации;

– прогнозирование (сценарное и целевое) развития ситуации;

– повышение оперативности и качества управленческих решений на основе использования аналитических и прогнозных инструментальных средств;

– автоматизация процессов подготовки аналитической отчетности;

– визуализация данных с использованием средств когнитивной графики (в том числе с применением геоинформационных систем и пр.);

– инструментальная и информационная поддержка экспертно-аналитической деятельности ЛПР и экспертов.

Однако, построение полноценной СППР, включающую все вышеперечисленные подсистемы, сопряжено с рядом трудностей, вызванных как организационными причинами, так и техническими. С одной стороны, не всегда существует возможность подобрать достаточное количество источников оперативной информации, которые подходили бы по всем требованиям, предъявляемым к данным. С другой стороны, многие методы анализа и сравнения, не вызывающие затруднения у человека, достаточно сложны в реализации в виде алгоритма, доступного для исполнения в рамках СППР. Также разработке СППР присущи следующие трудности [3]:

– классические методы поддержки принятия решений в большинстве своем хоть и разработаны довольно давно и получили широкое распространение, но не имеют под собой четкого математического обоснования, что влечёт трудности при их алгоритмической реализации;

– в хранилищах данных отсутствуют, или находятся в зачаточном состоянии методы очистки «грязных данных»;

– многие интеллектуальные методы анализа данных требуют большого количества данных для анализа.

Тем не менее, в России уже существуют системы, которые могут быть отнесены к классу СППР. Одна из наиболее совершенных СППР в Министерстве обороны Российской федерации создана в ситуационно-аналитическом центре в рамках проекта «Интегра» (интегрированная инструментальная система для проведения комплексного военно-экономического анализа и экспертизы мероприятий строительства и развития ВС РФ) [4].

Таким образом, можно утверждать, что возможности систем поддержки принятия решений достаточно широки и могут успешно применяться для организации информационного взаимодействия должностных лиц органа военного управления. Если построить СППР, решающую все вышеперечисленные задачи и включающую все указанные подсистемы, а также обеспечить ей должное снабжение оперативной информацией, она может значительно повысить эффективность информационного взаимодействия всех органов военного управления.

Список используемых источников

1. Автамонов П. Н., Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Актуальные научно-технические проблемы разработки и внедрения взаимосвязанного комплекса унифицированных интегрированных систем поддержки принятия решений (СППР)

в АСУ объектами военно-государственного управления // Известия ЮФУ. Технические науки. 2014. № 3 (152). С. 14–27.

2. Ларичев О. И., Петровский А. Б. Системы поддержки принятия решений: современное состояние и перспективы развития // Итоги науки и техники. 1987. Т. 21. С. 131–164.

3. Узденёва Т. А. Некоторые проблемы систем поддержки принятия решений // Молодой ученый. 2010. Т. 1. № 5. С. 103–106.

4. Трофимец В. Я. Автоматизированные системы поддержки принятия решений в области военно-экономического анализа и экспертиз // Вооружение и экономика. 2009. N 3 (7). С. 111–114.

Статья предоставлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 004.416.6

ИССЛЕДОВАНИЕ ПРОЦЕССОВ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ НАУЧНОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТЬЮ ВВУЗОВ МО РФ

Н. В. Шамров, В. Е. Ширяев, М. Е. Ширяев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Процесс автоматизации систем планирования, контроля и оценки научной деятельности, как и любой другой процесс автоматизации, в той или иной сфере являлся одной из основных проблем повышения эффективности, оперативности, работоспособности системы. Решение для данной проблемы всегда является индивидуальным и требует индивидуального подхода создания решений автоматизации.

автоматизация, программное обеспечение, ASP.NET WebForms, SQL, сервер, C#.

Разработка модулей программного обеспечения для совершенствования автоматизированной системы планирования, контроля и оценки научной деятельности – одна из решаемых научно прикладных задач в рамках исследования процессов управления научной и образовательной деятельности ввузов МО РФ.

Главной целью автоматизации управления является повышение эффективности использования потенциальных возможностей объекта управления. Таким образом, можно выделить ряд целей:

– Предоставление лицу, принимающему решение (ЛПР), релевантных данных для принятия решений.

– Ускорение выполнения отдельных операций по сбору и обработке данных.

– Снижение количества решений, которые должно принимать ЛПР.

– Повышение уровня контроля и исполнительской дисциплины.

– Повышение оперативности управления.

– Снижение затрат ЛПР на выполнение вспомогательных процессов.

– Повышение степени обоснованности принимаемых решений.

Одним из процессов, требующих автоматизации, послужил процесс создания событий сотрудников, таких как убытие в командировку, отсутствие по болезни, наряда, отпуска. Данный процесс необходим для автоматизации поскольку, требуется контроль за сотрудниками и оперативное представление начальникам информации об отсутствии сотрудников, а также причины отсутствия, время отсутствия.

Основные функциональные требования данного модуля программного обеспечения:

– отдельная страница на сайте «Портал научной работы»;

– дружелюбный и понятный интерфейс;

– валидация заполнения данных пользователем;

– связь с сервером SQL.

Основные системные требования к условиям написания данного модуля:

– среда разработки Visual Studio;

– использование шаблонов проектирования ASP.NET Web Forms [1];

– язык программирования C#;

– работа данного модуля в связи с SQL [2, 3].

Использование технологии ASP.NET WebForms можно рассматривать как некоторую надстройку над классическим принципом web-программирования «запрос-ответ». Данная технология является примером концепции RAD (*rapid application development* – быстрая разработка приложений), позволяя разработчикам максимально быстро и комфортно создавать рабочие приложения.

К достоинствам ASP.NET WebForms можно отнести:

– хорошие возможности для RAD (быстрой разработки приложений);

– возможность декларативного создания страниц;

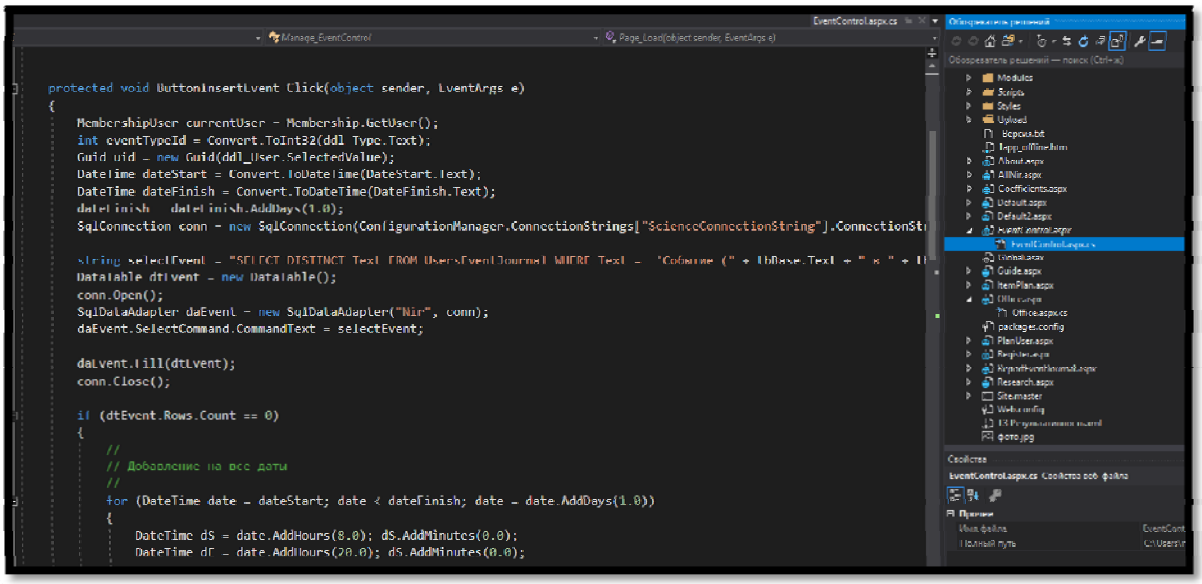
– простота разработки бизнес-приложений, работающих с большими объемами данных и завязанных на данных;

– привычная концепция событий, знакомая разработчикам настольных приложений, что позволяет быстро начать работать с таким подходом;

– большое количество библиотек сторонних разработчиков.

Для создания интерфейса формы была применена таблица каскадных стилей CSS Bootstrap 3.3.7. Bootstrap это свободный набор инструментов

для создания сайтов и веб-приложений. Включает в себя HTML- и CSS-шаблоны оформления для типографики, веб-форм, кнопок, меток, блоков навигации и прочих компонентов веб-интерфейса, включая JavaScript-расширения (рис. 1–3).



```
protected void ButtonInsertEvent_Click(object sender, EventArgs e)
{
    MembershipUser currentUser = Membership.GetUser();
    int eventTypeId = Convert.ToInt32(ddl_Type.Text);
    Guid uid = new Guid(ddl_User.SelectedValue);
    DateTime dateStart = Convert.ToDateTime(DateStart.Text);
    DateTime dateFinish = Convert.ToDateTime(DateFinish.Text);
    dateFinish = dateFinish.AddDays(1.0);
    SqlConnection conn = new SqlConnection(ConfigurationManager.ConnectionStrings["ScienceConnectionString"].ConnectionSt
    string selectEvent = "SELECT DISTINCT Text FROM UsersEventJournal WHERE Text = 'Событие (" + ddBase.Text + " " + t
    DataTable dtEvent = new DataTable();
    conn.Open();
    SqlDataAdapter daEvent = new SqlDataAdapter("Nir", conn);
    daEvent.SelectCommand.CommandText = selectEvent;

    daEvent.Fill(dtEvent);
    conn.Close();

    if (dtEvent.Rows.Count == 0)
    {
        //
        // Добавление на все даты
        //
        for (DateTime date = dateStart; date < dateFinish; date = date.AddDays(1.0))
        {
            DateTime dS = date.AddHours(8.0); dS.AddMinutes(0.0);
            DateTime dF = date.AddHours(20.0); dS.AddMinutes(0.0);
```

Рис. 1. Фрагмент кода модуля EventControl

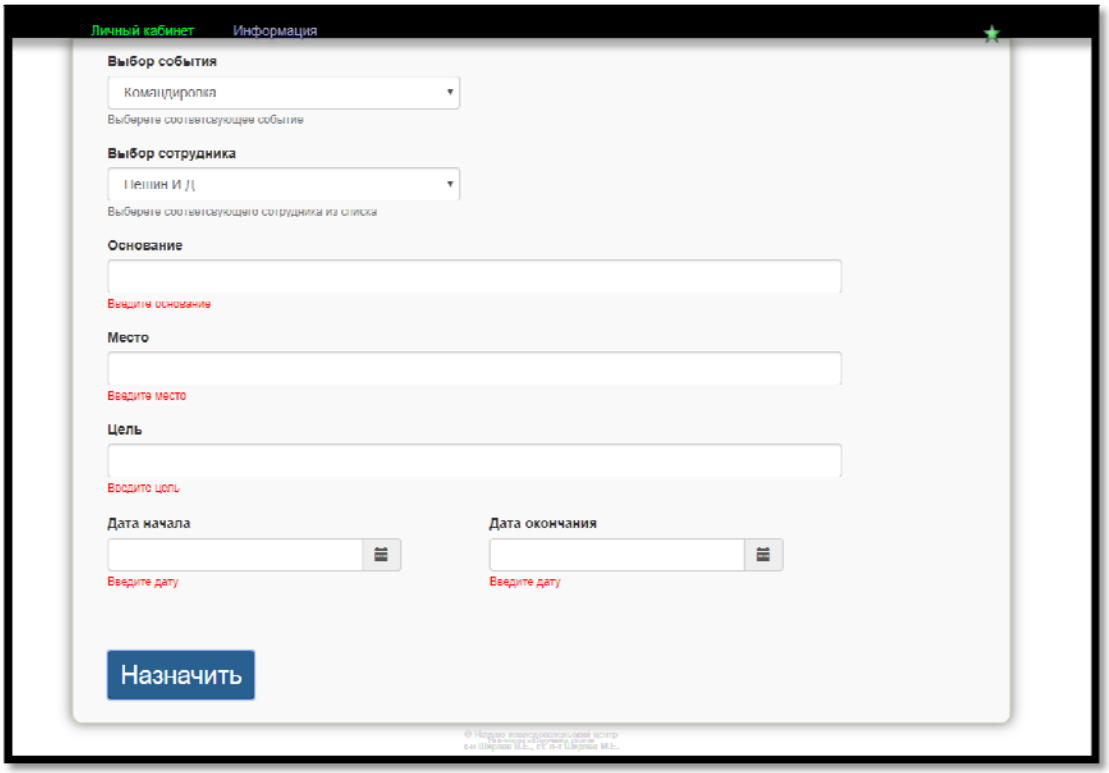


Рис. 2. Форма ввода. Проверка заполнения полей

```
<asp:Content ID="HeaderContent" runat="server" ContentPlaceHolderID="HeadContent">
    <link href="/Content/bootstrap.css" rel="stylesheet" type="text/css" />
    <script src="/Scripts/bootstrap.min.js" type="text/javascript"></script>
    <link rel="stylesheet" href="Content/bootstrap-datetimepicker.min.css" />
    <script src="/Scripts/jquery-1.9.1.min.js"></script>
    <script src="/Scripts/moment-with-locales.min.js"></script>
    <script src="/Scripts/bootstrap-datetimepicker.min.js"></script>
```

Рис. 3. Подключение CSS и JavaScript`ов

Список используемых источников

1. Фримен А. ASP.NET MVC 4 с приемами C# для профессионалов. М. : APress, 2013. 688 с.

2. Бьюли А. Изучаем SQL. М. : Символ-Плюс, 2016. 312 с.

3. Петкович Д. Microsoft SQL Server 2012. Руководство для начинающих. М. : БХВ-Петербург, 2013. 792 с.

Статья предоставлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 004.94

ПРОБЛЕМЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ВОЕННЫХ ДЕЙСТВИЙ

А. С. Шершнёв

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Моделирование в военной сфере имеет огромную значимость. Для получения адекватных результатов, моделируемая система и её модель должны соответствовать друг другу по критериям и признакам, необходимым для достижения цели исследования, но помимо этого существует целый ряд проблем, затрудняющий процесс создания модели.

математическое моделирование, моделирование военных действий.

На текущий момент проблема создания математических моделей является всё более актуальной, из-за появления и развития нового оружия и военной техники. Для решения данной проблемы необходимо использовать модели, наиболее полно описывающие деятельность командиров.

Из-за различных факторов данная задача не решена. В настоящее время математические модели разрабатываются задолго до реальных боевых

действий и представляют из себя аналог общевойскового боя, основное внимание в котором нацелено на организацию структуры войск, количественный состав и военно-географические условия [1]. Данные характеристики рассматриваются как у союзных, так и у вражеских войск. В реальности боевые действия никогда не совпадают с типовыми. Если брать во внимание изменение условий, таких как состав войск и их организация, ценность разработанных моделей постоянно теряется.

Так же одной из наиболее значимых проблем разработки моделей является предъявление требований. Это связано с тем, что разработчикам необходимо учитывать всевозможные факторы, влияющие на организацию и ведение военных действий. В результате чего, увеличивается исходный объём информации. Поэтому данный модели применяют в целях исследования, но ни в коем случае для работы управляющих лиц или организаций при планировании боевых действий [2].

И наконец последняя проблема создания моделей заключается в разработке моделей боевых действий специалистами военного дела. Данные разработчики описывают только часть, которая касается разработки словесной модели в виде формирования дерева возможных решений враждующих сторон. Исходная информация вносится в модель заранее, а для полноценной работы модели, недостающая информация динамически уточняется или выбирается из так называемой постоянной информации.

Штабные модели тоже не остались без недостатков. Данные модели плохо оценивают использование или создание факторов, ослабляющих противника, такие как отвлекающие манёвры и др. Такие действия помогают не только увеличить усилия войск в необходимый момент времени, но и значительно ослабить противника. Ещё один недостаток заключается в том, что при использовании данных моделей производится оценка всего лишь одной стороны военного мастерства командующего, а именно организацию войск в целях максимального использования их возможностей.

На основании вышесказанного можно сделать вывод о том, что модель необходимо уточнять командиром и его штабом на основе информации, располагаемой в данный момент выработки и принятия решения. Разработка модели должна иметь следующий порядок [3]:

1. Определить соотношения сил сторон в районе проведения боевых действий к моменту их начала, так же необходимо учесть множество вариантов замыслов действий как своих, так и вражеских войск.

2. Выбрать критерий оценки замыслов.

3. Рассчитать ожидаемые результаты при всевозможных комбинациях вариантов их замыслов с использованием критерия, выбранного в предыдущем пункте.

4. Произвести анализ полученных результатов и выбор наилучшего замысла.

При определении вариантов действий сторон, необходимо учесть где, когда и как создать превосходство над противником. При изменении ответа на один из этих вопросов, порождает новый вариант замысла действий для данной стороны.

В качестве выбираемого критерия оценки можно использовать вероятность нанесения поражения противнику или коэффициент соотношения сил сторон в определённый момент боя.

Анализ результатов лучше всего производить с помощью теории игр. При этом стоит помнить, что будут формироваться такие варианты замыслов, используя которые борющиеся стороны не рискуют проиграть больше или выиграть меньше, чем это возможно по выбранному критерию в данной обстановке.

Если рассмотреть вариант, когда противник сильнее или равен по каким-либо параметрам, тогда необходимо помнить о том, что никакой из представленных вариантов замыслов не сможет обеспечить достижения поставленной цели. В предлагаемом методе моделирования боевых действий, необходимо отображать только те варианты замыслов, при которых создаётся максимальное превосходство в определённые моменты времени. Конечно же это очень рискованно, но без учёта данных факторов, победить превосходящего противника просто невозможно. Поэтому из всех предоставленных вариантов необходимо выбирать с лучшим по критерию, установленному командиром, вырабатывающим замысел.

В заключение необходимо отметить, что внимания заслуживает ещё один подход к разработке моделей данного типа – тестирование модели с применением искусственного интеллекта. В результате использования данного подхода, командиру предоставляется возможность «сыграть шахматную партию» с компьютером, имитирующим противника. Этот подход довольно сложный, но перспективный с точки зрения повышения эффективности обучения офицеров военному искусству.

Список используемых источников

1. Моделирование в военном деле // Сайт Минобороны России. Энциклопедия. Режим доступа: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13579%40morfDictionary.

2. Выпасняк В. И., Калиновский Д. Б., Тиханычев О. В. Моделирование вооружённого противоборства: перспективы развития // Военная мысль. 2009. № 7. С. 12–20.

3. Чуев Ю. В. Исследование операций в военном деле. М. : Воениздат, 1970. 256 с.

Статья представлена научным руководителем, кандидатом технических наук Д. О. Федосеевым.

УДК 004.4

АНАЛИЗ СИСТЕМ МОДЕЛИРОВАНИЯ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ

В. Е. Ширяев, М. Е. Ширяев, И. А. Шляхов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Статья посвящена анализу моделирования транспортных сетей связи. В ней рассмотрены основные средства моделирования транспортных сетей связи и произведена их оценка.

транспортная сеть, моделирование, протокол, Cisco Packet Tracer, AnyLogic, BGP.

Эффективность моделирования транспортных сетей связи стала чрезвычайно актуальной задачей, особенно в условиях недостаточного финансирования информационных технологий на предприятиях. Поэтому, целесообразно создавать не реальную физическую сеть, а ее модель, на основании которой уже можно будет судить о производительности внутри сети и принимать решение о том, стоит ли разрабатывать данную модель или нет. Актуальность моделирования систем связи для военной области также не подлежит сомнению.

Вопросы моделирования транспортных сетей связи рассмотрены многими авторами, в том числе: Гудов А. М., Семехина М. В. [1], Стройкин А. Н. [2], Тарасова Е. А., Захарова О. И. [3]. Однако, в данных работах в недостаточной степени представлены конкретные средства моделирования транспортной сети связи и условия успешности их применения.

Целью данной работы является выявления достоинств и условий применения различных систем моделирования транспортной сети связи.

Для достижения указанной цели необходимо будет решить следующие задачи:

– охарактеризовать такие понятия как транспортная сеть, протоколы и моделирование транспортных сетей связи;

– проанализировать современные системы моделирования транспортных сетей связи;

– выявить возможности и недостатки каждой из приведённых систем моделирования.

Транспортная сеть – часть сети связи, охватывающая магистральные узлы, междугородние станции, а также соединяющие их каналы и узлы (национальные, междугородные). Главным требованием, предъявляемым к транспортным сетям, является выполнение сетью основной

функции – обеспечения пользователям возможности доступа ко всем разделяемым ресурсам сети.

Транспортная сеть, формирующая проводные каналы связи между удаленными беспроводными сетями, представляет собой совокупность:

– проводных линий связи (*links*), по которым передаются цифровые электрические или оптические сигналы;

– сетевых узлов (*network nodes*), осуществляющих ретрансляцию сигналов (включая их мультиплексирование/ демультиплексирование) из одних проводных линий в другие посредством коммутаторов.

Для общего представления о структуре транспортной сети связи была разработана общая схема транспортной сети связи, представленная на рис.

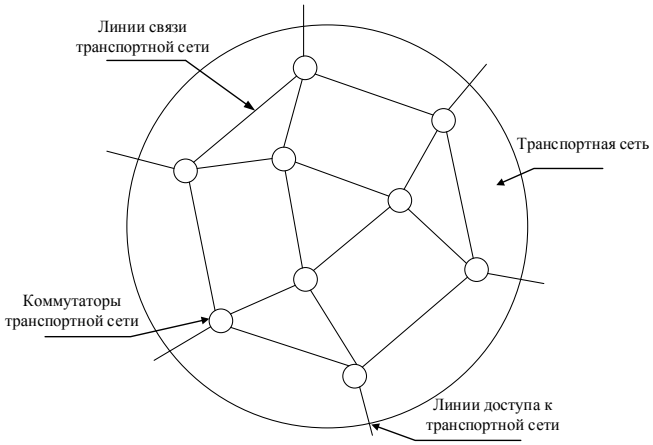


Рис. 1. Общая схема транспортной сети связи

На рисунке показана структура транспортной сети, содержащая 9 коммутаторов, соединенных между собой 15-ю линиями связи.

Для соединения и обмена данными между двумя или более устройствами, включенными в вычислительную сеть, используются протоколы.

В транспортных сетях связи используются такие протоколы, как:

– iSCSI, internet Small Computer System Interface – протокол для установления взаимодействия и управления системами хранения данных, серверами и клиентами;

– PPP, Point-to-Point Protocol – протокол «точка-точка»;

– HDLC, High-level Data Link Control – высокоуровневый протокол управления на уровне звена передачи данных;

– IP – протокол негарантированной доставки данных;

– ATM – пакетно-ориентированный режим переноса информации, использующий метод асинхронного временного разделения;

– BGP – протокол динамической маршрутизации и др.

Использование каждого протокола можно рассматривать с учетом разных моделей построение сетей. Протоколы PPP, RPR, HDLC, GFP

в транспортных сетях выполняют функции согласования информационных данных от источников нагрузки с транспортными структурами с целью повышения эффективности использования ресурсов этих структур, например, виртуальных контейнеров в сети SDH или оптических каналов в сети OTN, или физических ресурсов кадров передачи сети Ethernet.

Целью моделирования транспортной сети связи является определение оптимальной топологии, адекватный выбор сетевого оборудования, определение рабочих характеристик сети и возможных этапов будущего развития.

При построении модели транспортной сети связи стоит вопрос, какую систему моделирования транспортных сетей связи использовать для построения модели. В данное время, существует немалое количество симуляторов и эмуляторов для построения моделей сетей связи, известно множество программ для моделирования транспортных сетей связи, которые предоставляют пользователю возможность быстрого и удобного развертывания прототипов компьютерных сетей традиционной архитектуры, а также позволяют оценить изменение параметров функционирования сети при заданной активности сетевых приложений и сервисов. Для сравнительного анализа средств моделирования локальных вычислительных сетей были выбраны три наиболее популярные на сегодня среды моделирования: Cisco Packet Tracer, GNS3, Boson NetSim, Anylogic. Рассмотрим каждую из них в отдельности.

Cisco Packet Tracer

Одной из наиболее распространённых и популярных на сегодняшний день сред моделирования компьютерных сетей является Cisco Packet Tracer, которая позволяет экспериментировать с поведением сети, настраивая её под поставленные задачи, и создавать сеть с неограниченным числом оборудования.

Graphical Network Simulator-3

Следующая среда моделирования Graphical Network Simulator-3 (GNS3) – графическая сеть Тренажер-3 представляет собой программный эмулятор сети, который позволяет сочетать виртуальные и реальные устройства, используемые для моделирования сложных сетей.

Boson NetSim

Следующей рассмотрим среду моделирования Boson NetSim, которая является инструментом сетевого моделирования и эмуляции сети используются для сетевого проектирования и планирования.

AnyLogic

AnyLogic программное обеспечение для имитационного моделирования сложных систем и процессов, разработанное российской компанией Экс Джей Текнолоджис (англ. *XJ Technologies*). Программа обладает графической средой пользователя и позволяет использовать язык Java для разработки моделей. Преимущества и недостатки систем моделирования представлены в таблице.

ТАБЛИЦА. Сравнение систем моделирования транспортных систем связи

Система моделирования	Преимущества	Недостатки
Cisco Packet Tracer	Дружелюбность, понятность и логичность графического интерфейса, возможность работать в режиме реального времени, поддержка двух моделей построения сетей логической и физической.	Отсутствие создания сценариев для автоматизации работы устройств, возможность возникновения сбоев.
Graphical Network Simulator-3	Поддержка эмуляции Cisco IOS, возможность построения гетерогенных сетей, возможность моделирования различных технологий (Ethernet, ATM, Frame Relay).	Количество платформ ограничено, невозможность полноценного использования коммутаторов Catalyst, при использовании большого количества устройств заметно падает производительность, возможность сбоев.
Boson NetSim	Использование виртуальных пакетов для симуляции трафика, поддержка множества различных технологий,	Дорогостоящая.

Рассмотрев преимущества и недостатки каждой из сред моделирования локальных вычислительных сетей, можно сделать вывод:

– Если хочется просто попрактиковаться в создании компьютерных сетей, то больше всего подойдёт система моделирования Boson NetSim, которая представляет собой сборник лабораторных работ, помогающая студентам в процессе обучения.

– Если необходимо создать достаточно сложную сеть, которую в дальнейшем можно сделать реально рабочей, то необходимо установить программу Graphical Network Simulator-3, которая представляет собой программный эмулятор сети, позволяющий сочетать виртуальные и реальные устройства, используемые для моделирования сетей.

– Если же необходимо построить модель работы компьютерной сети небольшого предприятия, то совсем не нужно тратить деньги на приобре-

тение дорогостоящих сред для моделирования, и можно выбрать бесплатную среду моделирования Cisco Packet Tracer.

В статье рассмотрены наиболее распространённые на сегодняшний день среды моделирования. Таким образом, проанализировав приведённые три системы моделирования локальных вычислительных сетей, можно сделать вывод, что каждая из рассмотренных сред моделирования подходит для реализации конкретных задач. Выбор среды моделирования зависит от знаний и умений пользоваться данной средой, от функционала, предоставляемого каждым программным продуктом и от сложности того или иного средства [3].

Список используемых источников

1. Гудов А. М., Семехина М. В. Имитационное моделирование процессов передачи трафика в вычислительных сетях // Управление большими системами: сб. тр. 2010. №. 31. С. 20–25.

2. Стройкин А. Н. Моделирование локальных вычислительных сетей электротехнического производства авиастроительного предприятия // Известия Самарского научного центра Российской академии наук. 2013.Т. 15. № 6–4. С. 15–18.

3. Тарасова Е. А., Захарова О. И. Сравнительный анализ средств моделирования локальных вычислительных сетей // Форум молодых ученых. 2014. № 10. С. 10–15.

Статья представлена научным руководителем, доктором технических наук, профессором И. Б. Паращуком.

УДК 007.51

АВТОМАТИЗАЦИЯ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА ЗАПОЛНЕНИЯ КОРОБА ПРОДУКЦИЕЙ НА ПОЛИГРАФИЧЕСКОМ ПРОИЗВОДСТВЕ

С. Л. Ширяев, А. А. Шиян

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

На российских полиграфических производствах используется много неквалифицированных рабочих. Международные компании, работающие в этой сфере, стремительными темпами внедряют роботизированные производственные линии, которые позволяют резко повысить производительность труда и сократить число рабочих, занятых на фабрике. Преодоление отставания отечественных компаний в этой среде возможно только за счёт модернизации существующих производственных мощностей путем внедрения полностью или частично роботизированных конвейерных линий.

автоматизация производственных процессов, полиграфические предприятия, роботизированные конвейерные линии.

При разработке автоматизированной системы для производственных процессов полиграфии можно выделить две основные задачи: доработка существующего информационного программного обеспечения и выбор технического комплекса для осуществления работы всего механизма. Решение этих задач автоматизации позволит повысить пропускную способность производства и уменьшить расходы на персонал.

Актуальность автоматизации системы заполнения короба определяется несовершенством существующей технологической модели [1]. Рассмотрим текущую ситуацию.

Все начинается с автоматического формирования короба, которое осуществляется с помощью Case Erector Soco BTS-2300. Работник берет сформировавшийся короб и вкладывает прокладочный лист на дно. Это действие объясняется техническими требованиями к продукции. Короб по конвейерной системе двигается в специальную машину Japack (производства компании *Heidelberg*), которая накладывает продукцию. При присутствии в схеме укладки нескольких слоев, необходимо класть разделительный лист между каждым из них, во избежание порчи продукции при транспортировке.

Решение подобной задачи можно было бы свести к использованию небольшой пневматической станции по выбрасыванию листа в короб, используя датчики. Однако, согласно технического задания, требуется укладка продукции в гофрокороб в 2 ряда. Поэтому между рядами размещаются прокладки во избежание перемешивания продукции во время транспортировки.

На текущий момент в программном обеспечении исследуемого объекта (*Gluing machine Diana Pro*) используется следующая информация по части конструирования короба:

- количество продукции в коробе;
- количество слоев;
- размеры короба;
- схема укладки на поддон;
- примечание.

В примечании пишется специальная информация для производственного департамента. В том числе и схема укладки внутрь короба. Исходя из предлагаемой теории, этих информационных данных недостаточно для автоматизированной системы, так как, силами автоматизации невозможно извлечь такие неточные данные из примечания.

Для решения исследуемой задачи по автоматизации производственного процесса предложено использовать следующий алгоритм работы с данными для информационной автоматизированной системы в 3S.

3S – многофункциональная система управления ресурсами предприятия, построенная на базе Microsoft Dynamics AX. Существующая ERP система позволяет просматривать, сохранять и анализировать данные, которые собираются как в автоматическом, так и полуавтоматическом режиме (вбивая содержимое в базу данных) во время всего процесса производства.

После размещения заказа на производство в специальном модуле программного обеспечении 3S, он должен быть передан в конструкторский отдел для рассмотрения детальной проектировки внутреннего содержания короба. Данные должны содержать следующее:

- количество продукции в коробе;
- количество слоев;
- количество рядов;
- размеры горизонтальной и вертикальной прокладок;
- схема укладки прокладочных листов;
- размеры короба;
- схема укладки на поддон;
- примечание.

Предложенный алгоритм заполнения 3S позволит автоматизированной системе с легкостью вкладывать необходимые прокладочные листы внутрь гофрокороба, ориентируясь на заполненные данные.

Для автоматизации с технической точки зрения предлагается использовать робототехнические средства (рис. 1).

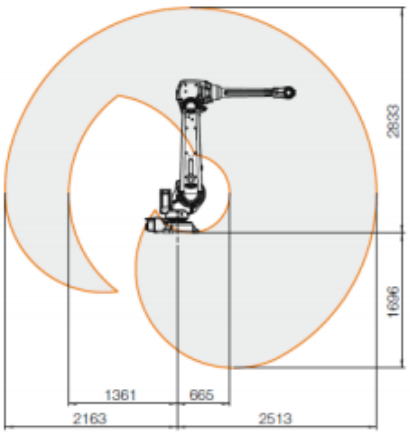


Рис. 1. Робот-манипулятор

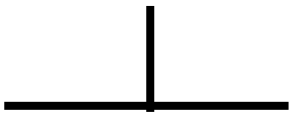


Рис. 2. Структура использования прокладочных листов в настоящий момент

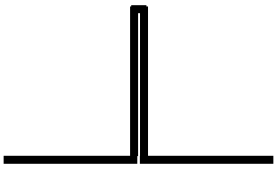


Рис. 3. Предложенная структура использования прокладочных листов

В дополнение необходимо изменить принцип использования специальных вертикальных прокладок (рис. 2).

Как видно на рис. 2, в данное время для применения специальной укладки прокладочных листов используется две части, которые не соединены между собой. На формирования такого рода конструкции у человека уходит 4 движения:

– работник берет горизонтальный прокладочный лист;

– перемещает его в короб;

– гофрокороб наполняется продукцией, после чего попадает к сотруднику;

– работник берет вертикальный прокладочный лист и вставляет между рядами продукции.

Изменив структуру прокладочного листа, представленную на рис. 3 (см. выше), появляется возможность использовать робототехнические средства для формирования.

Для создания данного типа укладки необходимо использовать специальный захват для робототехнического средства, с вакуумными присосками [2]. Способ формирования основан на силе инерции, которая помогает листу сложиться.

Для работы всего механизма необходима предварительная подготовка материала для формирования специальных прокладочных листов – создание на картоне перфорации, необходимой для гарантированного складывания материала в нужном месте, а также во избежание проблем со сгибанием.

Т. к. при формировании объект сталкивается с проблемой силы упругости, которая старается вернуть его в исходное положение, необходимо подбирать размер заготовки прокладочного листа таким образом, чтобы после создания предложенной структуры его размеры были на 0,5 см меньше, чем размеры короба. В данном случае, гофрокороб не даст картону разогнуться.

Предлагаемый алгоритм использования захвата, обеспечивающий формирование заданной структуры прокладочного листа (рис. 3):

– робот, имея запрограммированный сценарий, выполняет движение к месту, где хранятся заготовки для прокладок, которые необходимо переносить в короб;

– манипулятор опускается, включаются вакуумные присоски, которые обеспечивают плотное нахождение листа на захвате;

– начинается резкое движение вверх;

– резкая остановка движения с одновременным закрытием створок, которые находятся на местах перфорации картона.

– робот, используя сценарий, выполняет движение к коробу, после чего кладет прокладку непосредственно в него.

Используя алгоритмы заполнения ERP системы и складывания прокладки, появляется возможность полностью автоматизировать процесс заполнения короба.

Расчет PBT (*Pay Back Time*) осуществляется исходя из двух смен в сутки. Средняя заработная плата производственного человека, работающего на данном участке равна 30 000 рублей в месяц. Применив предложенный алгоритм предоставляется возможность сократить двух рабочих. Стоимость системы $P = P_r + P_g$, где P_r – стоимость робота, а P_g – стоимость пневматического захвата. Используя среднюю стоимость подходящих роботов по рынку, получаем стоимость проектируемой системы примерно 1 100 000 рублей.

$$PBT = \frac{1100000}{60000} = 18{,}3.$$

Предлагаемый алгоритм использования четкого структурирования программного обеспечения и робототехнических средств позволяет сократить расходы на персонал, исключить человека из производственной цепочки на данном участке, а также повысить пропускную способность линии. Расчетное время окупаемости составит 18,3 месяца.

Список используемых источников

1. Стефан Стефанов. Полиграфия от А до Я. Энциклопедия. М. : URSS, 2014. 560 с.

2. Козырев Ю. Г. Применение промышленных роботов. М. :КноРус, 2017. 488 с.

A N N O T A T I O N S

INFORMATION SYSTEMS AND TECHNOLOGY

Averchenkov R., Akimov S., Verkhova G. Models and Algorithms for Automated Profiling of Vacancies and Labor Market Analysis. – PP. 4–7.
The article highlights the relevance and expediency of developing a system for finding vacancies and analyzing the labor market. Basic implementation problems and methods for their solution are considered. Descriptions of the basic models and structures that best reflect the contents of the vacancies and skills of the applicant in the presented analysis system. The main stages of the system's operation are identified, and a variant of its further development is presented.
Key words: artificial intelligence, natural language processing, profiling, mathematical statistics, labor market.

Avramenko V., Bobreshov-Shishov D., Malikov A. The Analysis of Computer Incidents of Safety with Application of Artificial Neural Networks. – PP. 7–11.
For the accurate analysis of computer incidents caused by security breaches, we need an integrated approach to processing and interpretation of results used in the information systems of automation and information protection. For the implementation of classification of computer incidents by classes of characteristics of security violations one of the possible options is the use of the apparatus of artificial neural networks.
Key words: computer incident, violation of safety of information, artificial neural networks, analysis, means of protection.

Avramenko V., Bobreshov-Shishov D., Malikov A. The Way to Identify the Vulnerabilities of the "Zero Day" Based on the Analysis of the Behavior of the Exploit. – PP. 11–14.
Development of methods, methods and means of information protection in modern infocommunication systems from attacks using new exploits and vulnerabilities for the defending party is an urgent task. This article proposes a technology of protection against such attacks, based on the analysis of processes generated by the exploit.
Key words: exploits, vulnerability, computer attacks, information protection.

Aduevsky A., **Belous K., Pilikina E.** Development of Mobile Robotic Engineering Complex for Automated Monitoring of the Environment in the District of Dangerous Objects. – PP. 15–17.
A prototype of a mobile robotic complex based on the Arduino hardware platform is presented. The basic algorithms of the robot operation are considered, the robot control channels are analyzed.
Key words: monitoring, automation, Arduino, harmful production, management.

Akimov S., Verkhova G., Khoder H. Automation Support of Lifecycle of Modular Systems. – PP. 17–21.
At the present time, modular technology in design of technical complex systems is becoming more in demand due to the flexibility and the ability to quickly aggregate systems from standardized modules. In this paper, we present special multi-aspect models for automation support of lifecycle of modular systems, such as marketing research, design, production, exploitation with the preparation of an electronic passport of the product.
Key words: modular technology, complex systems, automation, lifecycle, CAD/PLM, multi-aspect modeling, complex model.

Akimov S., Verkhova G., Polpudnikova N. Automated System of Monitoring of Computers. – PP. 21–25.
The report presents the results of developing a prototype of an automated system for monitoring computer facilities. The developed system provides collection and processing of information about computers, including configuration, location, data on service. The automated system is implemented as a web service and involves integration into a single cyber environment of the postindustrial society. The current prototype of the system is written in the C # programming language as an ASP.NET application. The service can be used by the SaaS model (software as a service), which provides easy maintenance, as it does not require the user to install additional security.
Key word: automation monitoring, computing, ASP.NET, web service.

Akimov S., Kuptsov A., Fyodorov N., Hvostov M. Genetic Algorithms in Optimization of Technological Processes. – PP. 25–28.
A program for optimizing the movement of the working head of the CNC machine using genetic algorithms is presented. Genetic algorithms, as a kind of bio-inspired methods, allow to optimize complex processes with a lot of factors with high efficiency. In this case, we consider the optimization problem, which can be reduced to solving the Traveling Salesman Problem (TSP), which is NP-complete.
Key words: optimization, genetic algorithms, programming, travelling salesman problem, evolutionary algorithms, bio-inspired computing.

Almadatova A., Verdiyev S., Nagiyeva A. Cryptographic Method of Secret Sharing on Information Security. – PP. 29–33.
In this paper data transmission security systems and cryptographic methods of provision information systems safety, more concrete threshold scheme of Shamir is considered. It is also itemized attributes of cryptographic protocol. Cryptographic protocol of secret share and method of his use are described. As an example of implementation of threshold scheme computation of concrete task has executed. The result of those computations on the shape of graph has illustrated. The graph imagines threshold scheme when secret key is shared among 8 secret sharing scheme participants.
Key words: information security, security systems, data transmission, cryptography, secret sharing, secret keys, cryptographic protocol, threshold scheme.

Andreyev A., Belous K., Bychikhina A., Pilikina E. PJSC Pochta Bank Enterprise Analysis Activity. – PP. 34–39.
In the submitted article the creation reasons, the analysis of activity of the PJSC Pochta Bank enterprise, on the basis of the annual report for 2017 are considered. Advantages and shortcomings of his activity are reflected, suggestions for improvement of quality of rendering of services to clients of bank are made.
Key words: PJSC Pochta Bank, enterprise, client, deposits, credit.

Andreyanov Y., Andrianov V., Sergeeva I. Golovleva Yu. Safety Issues Standard Architectures of Government Information Systems. – PP. 40–45.
Abstract: The article considers the issues of security of state information systems, security issues, and information resources protection in information and communication systems of public authorities. The authors based their work from the fact that information security is the preservation of information resources and the protection of the legitimate rights of the individual and society in the information sphere, is the process of ensuring: confidentiality, integrity and availability.
Key words: GIS, Class of security, the level of importance of information, threats to information security.

Antonov V. Application of the Multi-Agent Approach for the Construction of Arom-Safety Systems. – PP. 46–48.
The article deals with the construction of an aromatic safety system using multi-agents. Application of such an approach will allow to build a universal information and monitoring system capable of making decisions and adapting to changing external conditions.
Key words: aromatic safety, multi-agent system, intelligent agents.

Artemieva V., Grishentcev A., Dikiy D., Korobeynikov A. Security problems of wireless touch and actuator in the environment of the Internet of things. – PP. 49–53.
The paper considers the problems of information security at the level of wireless touch and actuator in the environment of the Internet of things. The aspects of application of radio frequency identification technology and methods for increasing the level of security are considered. The problems of sensor networks security are described.
Key words: internet of things, security, actuator and touch devices, RFID technologies, wireless sensor networks.

Akhmedov N., Kurnosov V. Objective Metrics of the Quality of Stereo Images. – PP. 53–57.
Methods for assessing the perceptual quality of images and Serena Television systems began to develop almost simultaneously with Poly TV. Without the development of these methods impossible, the standardization of systems, which is the basis of industrial outputs, which include the device, and happy. Quality assessment is a key criterion in the projection and optimization of systems for transferring large video content. A number of industrial companies and research organizations proposed a metric to evaluate the quality perception of two-dimensional images. However, Menace much attention until recently was focused on the evaluation of ten prostate images. Meanwhile, the Assembly of 3D – islets Siro area in which the Intern as the entertainment industry, and numerous scientific applications
Key words: TV, 3D, quality.

Bagomedova A., Ushakov I., Tsvetkov A. Development of Methods of Verification of Virtualization Server Conformity to Safety Requirements under Standard GOST R 56938-2016. – PP. 58–63.
The article considers the basic requirements for the virtual infrastructure: methods of protection, and methods for implementing these methods based on GOST R 56938-2016, which will contribute to improving the level of information system security. The prototype of the algorithm of the developed automated solution for checking the requirements for virtualization servers will be analyzed in accordance with GOST R 56938-2016.
Key words: virtualization, hypervisor, GOST.

Belous K., Vachugova V. Development of an Information Panel Based on LED Matrix. – PP. 63–67.
Was developed the technical device, which in the form of crawline visualize various educational and organizational information, as well as messages about the condition of outdoor environment. The device itself is implemented on soft panel Node MCU with internal Wi-Fi modular block. In the function of visualization element, we used a LED module built on the basis of MAX7219 electronic chips.
Key words: LED matrix, information, database, Arduino, wifi.

Belous K., Grigorieva A. Software-Hardware System for Accounting of Material Values. – PP. 67–70.
A prototype of a client-server application designed to take into account information about material values that are on the balance sheet of an institution, enterprise or organization is considered. The analysis of a subject area on the basis of which the object model is designed is carried out. The programming language is C #. The basic technology of development was the technology ASP.Net. The data is stored in the relational database MS SQL Server. Implemented basic support for devices for reading barcode IDs, smart cards and RFID tags.
Key words: IPTV, caching, TV, time-shifted, the proxy.

Belous K., Ivanova V., Kulikova T., Pilikina E. Prospects of Development of the Payment System «Mir». – PP. 70–75.
The first Russian national payment system «Mir» which provides various money transfer services is examined in this article. The concept, structure, main characteristics are given and the reasons of creation of this payment service provider are defined. Advantages and shortcomings are reviewed, the prospects of its development are designed.
Key words: payment service provider, «Mir» card, NPCS.

Belosheeva P., Litvinov V. Study of Modern Environments of Simulation of Infocommunication Networks. – PP. 76–79.
Simulation modeling allows to obtain a visual picture of the system behavior, to consider different variants of the model that correspond to different components of the system functioning and possible structural transformations, to obtain the values of the required quantitative characteristics. Therefore, simulation is currently gaining ground in the study of complex technical systems and technological processes, including infocommunication networks.
Key words: simulation modeling, GPSS, AnyLogic.

Bogolepov G., Krasnov V. Analysis of Graphical user Interface Frameworks for Operation System Astra Linux. – PP. 80–83.
In this paper was considered the reasons for discussing this topic, give a brief reference on two widely used libraries of interface elements, give a comparative description and recommendations for their use in development for the operating system Astra Linux.
Key words: Astra Linux, graphical user interface (GUI), GTK+, Qt, framework, analysis.

Botyakov V., Shestakov A. Use of Spatial Data About Assets of the Enterprise in an Automated Accounting of Precious Metals. – PP. 84–89.
According to the analysis of the existing order and organization are regulated automated accounting of precious metals in fixed assets of the enterprise context and the objective conditions of transition to the digital economy of the country developed organizational and organizational-technical proposals for entering, processing and maintaining up to date spatial data about assets of the enterprise, containing precious metals, as well as their feasibility without significant changes to currently supported resource and assets of the company.
Key words: automated accounting, precious metals, enterprise context, spatial data.

Brechko A. Cyber-Attacks Protection Based on the Communication Network Mobility. – PP. 89–92.
The article discusses the typical stages of computer attacks on elements of a communication network, especially the bias placed on the analysis of the time indicators of attack, and the dynamics of changes of the network, its state and the States of its elements, on the basis of which offered the basis for the justification of the criteria of security for the network and its elements – the average time a quasi-stationary state of the network.
Key words: computer attack, network security, protection criteria.

Bulygin G., Kozlova L. Multithreading and Concurrency in UNIX-like OS on an X86 Platform. – PP. 93–96.
The article will consider one of the most fundamental abstractions in UNIX-like systems after a file – the process (the main components of the process, methods of parallel execution of programs both within one and many processes). It is here, in process management, that the vision and durability of the original Unix concept is most clearly demonstrated. In the Unix concept, the creation of a new process is separated from the loading of a new binary image, in most cases these actions are performed together, separation allows you to experiment and opens up opportunities for the development of each task. The conclusions about the parallelism at the level of commands of the processor based on the x86 architecture.
Key words: process, thread, x86, UNIX, CISC, RISC, system call, concurrency.

Vaganov A., Kochmarik N. Method of Designing the Path of Primary Signal Processing Based on Linear Impulse Systems. – PP. 97–101.
This article discusses the method of designing the path of primary signal from transmitters in process control system based on integral linear impulse systems (LIS). A mathematical model of the tract subject to frequency ratio clocking LIS and upper bounds of the useful signal is not less than one hundred. Performed modeling of a fragment of a signal processing in a specialized CAD.
Key words: signal processing, linear impulse systems, interference.

Vaganov A., Chistyakov A. Recognition of the Aperiodoc Pulse Sequence of the Neuron Network of NARX Type. – PP. 102–106.
The article describes a neural network of the type NARX, designed to detect a pulsed aperiodic sequence that simulates the signal from the ACS transmitter, against background noise. The process of forming sets of test data, on the basis of which the network is trained, is considered. The architecture of the NARX network is substantiated, which provides the possibility of reliable detection of a pulse signal against a background of white noise, sinusoidal interference and simultaneous interference of both types of interference. The problem of determining the minimum pulse width at which it can be detected by a noisy signal is considered. Recommendations are being formulated to select the parameters of the neural network with minimal resource costs for its implementation based on programmable analog integrated circuits.
Key words: artificial neural networks, signal recognition, pulse sequence, interference.

Vasilev I., Trifanov M., Uss V. Methods of Scanning the Surrounding Space by Means of a Triangulation Laser Range Finder Using a Diffraction Grating. – PP. 106–110.
In this paper, use to consider methods for measuring distance using laser range finders, methods for constructing a terrain map and determining the position. The novelty consists in the use of a triangulation laser and a diffraction grating as a new method of collecting information about objects in space, determining their shape and distance. This method makes it possible to scan and map the map in several planes at the expense of the diffraction grating, aligning the flat contours along the Z axis makes it possible to create from these contours a volumetric shape of the surrounding space.
Key words: Diffraction grating, triangulation laser, scanning, space, shape, map of the area.

Vashurina E., Gagarin Y., Lauta O., Soloviev D. Protection of the Control Channel of Robotized Complexes. – PP. 110–115.
Annotation: to date, research in the field of robotic is very relevant. Robotic complexes can improve productivity at times, without making mistakes due to human factors. Such complexes are referred to as cyber physical systems. An integral part of cyber physical systems is the management system.This system, as well as any information channel, must be protected from computer attacks in order to avoid interception of cyber physical systems by intruders. In the article a robotic system and a system that allows to manage this complex using a reliable cryptographically stable connection. The main element of this system is a cryptographic chip stm32f415. It allows you to reduce the load on the central processor to perform control algorithms, freeing it from cryptographic operations, thereby guaranteeing the gain in time.
Keywords: control channel, cyber physical systems, robotic systems, cryptographic algorithms.

Velikanov A., Viksnin I., Komarov I., Marenenkov E., Tkachenko S. Contradiction to the Destructive Information Influence of the Self-Registering Group of UFAs. – PP. 115–120.
The most important way to overcome the technological barriers identified in the National Technology Initiative related to the use of multi-agent self-organizing unmanned systems is the problem of ensuring secure information interaction between agents. The paper propos-

es a method for ensuring information security of information interaction of the self-organizing group of unmanned flying apparatuses under the destructive information impact.
Key words: information security, multi-agent self-organizing unmanned systems.

Verhova G., Iofik A. Models and Algorithms of Automatized Management of Scientific and Technical Information. – PP. 120–124.
The report considers models and algorithms for managing scientific and technical information. These models can be used to automate the planning, execution and analysis of scientific research and development work, as well as in the "electronic edition" system. Application of these models and algorithms will improve the quality of planning directions and scope of scientific work, ensure a rational choice of the team of performers, reduce the amount of routine work when creating reports. The proposed models and algorithms are oriented towards the use of a post-industrial society within the framework of a single cyber environment.
Key words: model, scientific and technical information, Internet, life cycle.

Verkhova G., Pletnev Y. Unified Software and Hardware Platform for Sensory Layer for IIoT. – PP. 124–127.
The results of research in the field of creating a concept of the software and hardware platform of the touch layer for industrial Internet of things are presented. The goal of creating a software and hardware platform is to unify the interaction of sensors of physical quantities within the sensory layer of the unified cyber environment of the postindustrial society. The possibility of using the technology of virtual enterprises for creating the infrastructure of the Internet of things is shown. Presented are options for using technology to monitor any man-made objects, both industrial and domestic.
Key words: internet of things, sensors, IIoT infrastructure, monitoring.

Verkhova G., Frolova K. Electronic Forms of Communication in the General Educational Institution Based on the Cyber-Environment of a Virtual enterprize. – PP. 127–131.
The problem of informatization for the general educational institutions of Saint Petersburg was taken in view. It showed some flaws of existent systems for the communications among pupils, teachers and parents. The ways of evolution for these systems have been proposed in order to develop modern educational processes.
Key words: educational institutions, electronic learning, cyber-environment, distance learning, social network.

Vinogradov U., Rogachev V. Investigation of the Possibilities of Infrared Computer Vision Systems. – PP. 131–134.
To measure the parameters of infrared systems, a computer system was designed and developed. The purpose of this system is to measure the characteristics of infrared systems. The system is built on a microcomputer "Raspberry Pi" and an infrared CSI camera. Some characteristics of the system have been measured.
Keywords: infrared systems, microcomputer “Raspberry Pi”, infrared CSI camera.

Vinokurov M., Koryakin D. The Architecture of the Special Software for Controlling and Managing Devices of the Network and Applicable Software Technologies in JAVA. – PP. 135–139.
Currently, the military forces are actively working on a way of automation such things as monitoring and managing the nodes of various distributed digital systems. The nodes structure and inner nodes hierarchy organization of such systems (for example, the mobile transport communication network) is a complex task considering the system development, the developments of a set of systems, thus such a system requires a responsive graphical interface implemented as information system and aimed to provide the efficient management of this a system. The service-oriented web-application development is proposed in order to implement such system providing the responsive and efficient user interface.
Key words: service-oriented architecture, web-application, Vaadin, Spring.

Vitkova L, Gerling E., Golovlyova Y., Kovzur M. The Convergence of Information Technologies for Increase of Efficiency of Management of the Information Space. – PP. 140–142.
This article addresses the transformation of the concept of convergence of information technologies, issues of increase of efficiency of management of the information space, information security risk management, and some aspects of optimization in the information security management system: efficiency, resource intensity and validity of optimization processes.
Key words: convergence of information technologies, management of the information space, information security management system.

Vitkova L., Dudnikova M., Petrova A. Questions of Management of Information Security. – PP. 143–146.
At the moment there are settled techniques of technical protection, but the modern state standard specifications on management in information security do not solve the current problems. In this article authors will consider need up-dating of techniques for control of information security and use of process approach.
Key words: information security, control system of information security, security policy.

Vitkova L., Dudnikova M., Petrova A. Research and Assessment of Vulnerabilities of Information Security of Electronic Banking for Natural Persons by Delphi Method. – PP. 147–152.
Development of IT technologies generated the infinite number of conveniences, both for physical, and for legal entities. The relevance of this article is caused by the fact that with growth of services which are provided on the Internet there was a new sector of economy – electronic commerce which part is electronic banking. In this article the existing vulnerabilities, threats and methods of protection in the sphere of electronic banking are analyzed.
Key words: information security, threats, vulnerability, electronic banking.

Vitkova L., Dudnikova M., Petrova A. Determination of Probability of Violation of Critical Properties of the Data Asset on the Basis of CVSS of Metrics of Vulnerabilities. – PP. 152–156.
In this report authors develop a method for determination of probability of violation of critical properties of a data asset on the basis of Common Vulnerability Scoring System version

of 3.0 metrics of vulnerabilities. On a basis risk - the oriented approach offered by the ISO/IEC 27005 standard. On the basis of the developed method the formula for assessment of vulnerability of data assets is given.
Key words: information security, CVSSv3.0, valuation method of risk.

Vitkova L., Dudnikova M., Petrova A., Investigation and Assessment by CVSSv3.0 of Incidents of Information Security During the Exploitation of Zero-day Vulnerability. – PP. 157–161.
In this report, the authors analysis the cryptographic virus in the target attack. The virus signatures are shown; the code of the executable file is given; the process of the no_more_ransom virus operation is described; consequences of infection and ways to prevent infection of the computer are described; Vulnerability assessment is given by the common vulnerability scoring system version 3.0 method.
Key words: virus, CVSSv3.0, 0-day attack, target attack, Information Security.

Vitkova L., Dudnikova M., Petrova A. Management of Information Security of the Distributed Systems of Storage and Processing of Money. – PP. 162–167.
In today's world of online banking, electronic cash, wallets and other innovations, create the illusion of confidence that the money earned is safely tucked away from intruders. However, the evolution in the banking sector gave impetus to the development of methods of illegal profit, and other threats of financial fraud, so the relevance of this topic is increasing day by day. The authors explore the concepts of distributed storage and processing of funds. Describes the concepts, type's electronic submission of funds and consider existing the most typical vulnerabilities and threats to information security.
Key words: data - storage systems, distributed systems, e-money, big data.

Vlasenko M., Ivanov D., Kuznetsov S., Lauta O. Security of the Management of Roboticed Systems with Application of Neural Networks. – PP. 167–171.
Annotation: the article describes the approach to securing the control channel of the robotic complex based on the analysis of the exchange between the operator and the complex using packet data protocols. For the analysis, it is proposed to use different types of neural networks. In the article typical problems solved by various types of neural networks are considered, and questions of reducibility of these problems to the problem of detecting anomalies during the exchange of control data between the robotic complex and the operator.
Key words: robotic complex, control system, wireless control, protocol control, security information, neural network.

Voloshinov D., Kantarbaev R., Sosnovskikh A. Use of Modern Information Technologies of Augmented Reality to Create a Mobile Application. – PP. 171–175.
The development of mobile applications for the past 10 years is one of the most promising and fast-growing software markets. Using the technology of displaying various objects on the device screen allows the user to receive information not only in textual form, but also in geometric, which has certain advantages. In this article, an alternative process of displaying three-dimensional objects with the help of graphic labels is considered.
Key words: argument reality, 3D, unity, virtual reality.

Voloshinov D., Seleznev V. Investigation of Graphical Modeling Algorithms for Visualizing Data. – PP. 175–180.

The actual problem today is the creation and support of various geometric algorithms in various CAD systems. In most modern CAD systems, almost identical data views are used. In the upper part there are assemblies, with details at the bottom and separate drawings. The parts are defined either parametrically or explicitly with their topology, determined using the solid boundary representation model, consisting of NURBS surfaces (non-uniform rational spline). These surfaces are tightly connected to each other using these tolerances. Everything is complicated by the fact that different CAD systems handle tolerances in different ways. Most often, when you transfer a file from one system to another, the receiving system skips certain tolerances, which leads to a model with holes or gaps. The model will often appear in the form of surface patches, which you then control, and see if the program can sew these surfaces into a solid model. The reason why CAD systems have tolerance problems is primarily due to inaccuracies in mathematical algorithms written for geometric modeling kernels.

Key words: geometric algorithms, model, data, system.

Voloshinov D., Sklyarova E. A Study of the Stylistic Peculiarities of the Logos in the Commercial Area, to Optimize the Design of the Corporate Style. – PP. 180–184.

To date, the concept of corporate identity has steadily become a lexicon of both designers and advertisers. Logo is the basis of corporate identity. The logo should reflect the main activity of the company, be recognizable everywhere and on any scale. The logo is an "unspoken" advertisement and has a great influence on the emotional attachment of consumers. This article is devoted to solving problems related to the problems of improving the concept of logo creation by means of information systems.

Key words: Corporate identity, logo, design.

Volshchukov M., Mamedov S. Features of Providing Services for Technology "Smart Home" Based on Cloud Computing. – PP. 184–189.

At the present time, information technology has started to unite a large number of different information systems. They become interpenetrating, in this connection new opportunities arise. Providing services to consumers is one of the most urgent tasks in the world of information technologies. With the advent of a large number of diverse systems, services and technologies, the problem of their interaction, integration and use arises. Optimize information resources and manage them more flexibly with a variety of technologies, in particular today, to solve such problems, the technology of cloud computing is widely used.

Key words: network infrastructure, technology, smart home, heterogeneous environment, information system, IT.

Volynkin P. Features temporal information encryption. –PP. 190–194.

The article discusses the technology of message encryption based on AES technology, based on a unique combination of keys, each of which has its own identification number. We investigated the temporal efficiency of the algorithm compared to the static methods of forming the keys.

Key words: information security, encryption, multimedia, graphic files, audio information, steganography.

Volynkin P., Gyandzhiev E. Research of Methods of Formation of Frequency Portraits. – PP. 195–202.
Each person is characterized by a unique set of features of speech behavior, which can be used for identification. Methods of such analysis can be divided into two large groups – expert and formal. By means of mathematical methods and algorithms it is possible to form a so-called frequency portrait of the author of the text. From the point of view of the presentation logic, the algorithm of frequency analysis methods is based mainly on the auto-examination, a mathematical model of the sequence of letters of the text is used. The article considers the prerequisites for creating an algorithm for determining the authorship of the text, as well as identifying the non-belonging of the text to a particular author.
Key words: frequency portrait, chart, frequency of letters, frequency bigrams, statistical analysis, lingvoanalyzer.

Volynkin P., Sevostyanova A. A Study of the Principles of Encryption of the Multimedia Information in Graphic Files. – PP. 203–206.
Currently, the issues of information security are the most relevant, as unauthorized access to data is actively developed. In order to protect information, there are various methods of encryption. This article discusses the principle of encryption of multimedia information in graphics files. The main objective of this method is the final presence in the usual image of a voice message, music or sound. Perhaps, if you are creating can be difficult with the size of the media file, but the implementation of this method will help to reduce the risk in vulnerability information from intruders.
Key words: information security, encryption, multimedia, graphic files, audio information, steganography.

Voronov V., Voronova L., Genchel K. Application of Parallel Algorithms in Neural Network for Sign Language Recognition. – PP. 207–212.
The article describes the features of communication between people with hearing impairment through the sign language, the development of a convolutional neural network for recognition by dactyl, the stages of creating a training set for a neural network, and the appropriateness of using parallel algorithms to optimize its learning and work.
Key words: IAD, sign language, data mining, machine learning, neural networks, parallel computing.

Vostrykh A., Shurakova D. Components of Special Information Technology for Optimal Routes Construction. – PP. 213–218.
The problem of optimal routes construction of emergency rescue units of fire and rescue garrison is considered on the example of the Kostroma city. Special information technology as a tool for its solution is proposed. The technology contains 3 stratified components, each of which is included in the work when it is not possible to solve the problem at the previous level (step), which provides a guaranteed opportunity to solve the problem in real time and in different settings.
Key words: emergency rescue units, routes, special information technology, simulation modeling, Dijkstra's algorithm, clusterization.

Gavrilov A., Glukhovsky M., Kuznetsova A., Peshkov A. Interregional interaction for increasing the level of information security. – PP. 219–223.
Today, raising the level of information security is one of the most important aspects of national security. In this paper, the authors consider the stages of import substitution of foreign software for the Russian analogue, as well as some other solutions that will provide information security for the executive bodies of state power. Information and communication technologies have already become an integral part of modern management systems in all spheres of public administration and state security.
Key words: import substitution, information security, threats, vulnerabilities, distributed networks, interregional interaction, information systems.

Gaifulina D., Feforchenko A. Overview of the Network Traffic Representation Formats for the Security Assessment of the Cyber-Physical Systems. – PP. 223–228.
The paper devoted to analysis of the network traffic representation formats for the cyber physical systems. The goal of the research is determination of the advantages and disadvantages of existing ways for network activity information representation in the tasks of information gathering, transfer, storing and further processing. In the paper the most used in practice semi-structured and stricter formats are analyzed. The comparison of standards considering their complexity, usability, resource consumption and other parameters is provided. Besides the paper reviews the possibility of normalization of a source information for compatibility and correct interpretation of network traffic data.
Key words: network traffic formats, network traffic analysis, security assessment.

Gatchin Y., Chistyakov P. Features of Development of DoS-Attacks Applications. – PP. 228–231.
By highlighting DoS-attacks patterns and vulnerabilities used, you can understand how to reduce threats, i.e. what measures and means need to be implemented to protect the information and information system in an open network. Understanding the development and implementation of software for DoS-attacks allows you to understand their algorithms and structure, which will help in the creation of software protection tools. This will help in creating protection against DoS-attacks, such as the development and implementation of a traffic analyzer (sniffer), which is necessary to detect network attacks (including DoS).
Key words: computer networks, network attacks, software development.

Gvozdkov I., Kozhanov Y., Likar A. Handling of Multimedia Streams with Priority Queueing. – PP. 232–236.
Different services in the IP network needs precise values to delivery packages "from end to end." Estimation delays for multimedia streams on the interface of the router using priority queueing were done.
Key words: router, priority service, load, average residence time.

Golutvina Y., Ptitsyna L. Ontological Approach for Organization Information Exchange in Multiagent System of Service-Oriented Complexes – PP. 236–241.
We describe objective reasons for relevance of application of ontological approach for organization information exchange in multiagent system of service-oriented complexes. Analyze

known paradigms for constructing ontologies. Presents formalization of the description of ontologies for intelligent information systems. Offer paradigm for organization information exchange in multiagent system of service-oriented complexes. Refine key elements for a formal description of the generated ontology. It revealed methods for the invariant organization of information exchange.
Key words: ontology, intelligent information system, service-oriented systems, multiagent systems.

Grishentcev A., Elsukov A., Korobeynikov A. Modeling a secure the broadband messaging device. – PP. 241–246.
The publication is devoted to modeling of the transceiver system of broadband radio communication of the sub-noice of messaging. The implementation of the mathematical model was carried out in the environment of Simulink (Matlab). Broadband signals were formed using complex matrices with a special form of autocorrelation function. For the transceiver system, adaptive synchronization using the offset window method was used, which allowed to reduce the computational costs of receiving messages at times. Also, the model was studied for the stability of data transmission when the transmitted signal is distorted by additive white Gaussian noise. If the signal is distorted by the multiplicative noise and the multipath noise, the transmission stability is determined by the synchronization method used in the transceiver system.
Key words: Broadband radio communication, subnoise radio transmission, signal processing, radiosteganography, mathematical modeling.

Grishentcev A., Zhitkov K., Korobeynikov A. Expert System for Auditing Information Security in the Enterprise. – PP. 246–249.
In today's world, it is difficult to imagine an organization in which information technology would not be tightly integrated into business processes. To ensure effective protection of information in the enterprise, timely audit of information security is necessary. One of the tools for conducting the audit is expert systems. This article describes the author's implementation of such a system, the structural diagram and the algorithm of work are given.
Key words: expert system, fuzzy logic, information security audit.

Gromov V. Microcomputers of Traffic Police of Russia. – PP. 250–253.
It is dedicated to the development of information systems of traffic police in Russian Federation. It reveals the fundamental questions of the formation of distributed data bases and advanced cloud technology to create systems with on-line and off-line queries. Formalizes the main reasons that may have a negative impact on the implementation of tasks to create a single information space.
Key words: corporate computer networks, client-server model.

Gubin A., Litvinov V., Litvinov D., Filippov F. Analysis of Methods of Designing user Interfaces on the Basis of Domain Ontology. – PP. 253–257.
The development of technologies and the emergence of new requirements for the development of information systems lead to a partial complication of interfaces, associated not only with the increase in the set of functions of information systems, but also with various changing

conditions for their operation. In this paper, the concepts of extensibility of tools for designing and implementing the user interface within the framework of the ontological approach are considered.
Key words: user interface, domain ontology.

Gubin A., Litvinov V., Filippov F. Choice of Parameters at the Development of Recursive Digital Smoothing filters. – PP. 258–262.
The question of the location of the zeros of the characteristic polynomial of recursive digital smoothing filters within a given region remains open, although their position has a significant effect on the variance of the random error at the output of the filter. In this paper, we consider the solution of the problem of selecting the zeros of the characteristic polynomial of digital filters in the process of their optimization.
Key words: digital filters, variance of random error, observation time, characteristic polynomial.

Gubin A., Litvinov V., Filippov F. A Set-Theoretic Approach to Information Retrieval in RDF Storage. – PP. 262–266.
A method of the formalized description of triples, RDF repositories, based on the use of set theory and which allows to reduce time of information search due to the replacement procedures for SPARQL set operations available in a programming language.
Key words: data retrieval, set theory, data warehouse, RDF.

Gubin A., Matveev A. Problems of Implementing Cloud Services in the Corporate Structure. – PP. 266–270.
The article gives an overview of cloud information technologies. The main models of providing cloud computing services are considered. An assessment of the benefits of implementing cloud services in various corporate infrastructures is being conducted. Normative documents regulating methods and means of protecting confidential information are given.
Key words: cloud services, information infrastructure, information security.

Gudkov M., Kotsynyak M., Nechepurenko A., Suetin A. Cyberphysical Systems and Methods of Impact on Them. – PP. 270–275.
In the article the approach allowing to define the probability-time characteristics of the targeted computer attack aimed at robotic systems is considered. For this, the article proposes using the method of topological transformation of stochastic networks and constructing a profile model of a targeted computer attack.
Key words: model, probability-time characteristics, targeted cyber attacks, method of topological transformation of stochastic networks.

Gunina E., Stepanov A. Development of Algorithm for Optimization of Synthesis of Graphic Elements. – PP. 275–278.
The article is devoted to the modern problem of optimizing the creation of graphic elements of vector graphics in design. Designers when creating vector graphic elements such as icons,

patterns, etc. faced with the inability to promptly make changes to the created vector drawing. The problem of finding new solutions to simplify the work with graphic elements is touched upon. A variant of optimization is proposed with the help of algorithm development in the Simplex program.the ratio of requests processed by the server cache to the total number of requests.
Key words: optimization, graphic elements, design, vector graphics, new solutions, algorithm development, Simplex, interface, process.

Gunina E., Yakovlev S. Methods for Automating the Synthesis of a Modular Grid for Design. – PP. 279–283.
The article deals with the automation of the creation of modular grids. Some possible ways of creating grids, using various software and systems of labor automation of designers, represented on the market and having a positive experience of using the specialists of the industry. A variant of design presents, with the help of a given algorithm, the process of creating and editing a grid becomes dynamic and capable of generating multivariate solutions.
Key words: design, module, modular grid, algorithm, automation, software.

Gurianov S., Lipatnikov V., Litvinov A., Sazonov A. The Method of Controlling the Data Processing Network Intrusion Detection and Analysis of the Dynamics of the Offender's Actions. PP. 283–288.
The method of controlling the data processing network intrusion detection and analysis of the dynamics of the offender's actions on the basis of the tree classifier and Kohonen maps. The function of the control algorithm: observation and feature extraction of digital streams with data transfer protocols, entering computer information network and a dedicated server, detection of intrusion, the choice and implementation of means of protection.
Key words: computer information network, protecting information; the tree classifier, and the Kohonen self-organizing map.

Gusev D., Ptitsyna L. Determination of the Time Profile of Critical Situations in the Multi-Agent Information Security System. – PP. 288–292.
The reasons for the demand for multi-agent information protection systems in distributed infrastructures are considered. The methods for determining critical situations in a multi-agent information security system are described. A generalized class of models of a multi-agent system is presented. Methods for determining the time profile of critical situations in a multi-agent information security system are given. The methods of increasing the variations in determining the time profile of critical situations are shown. Methods for their invariant determination are proposed.
Key words: information security, system of information protection, multi-agent protection system, threats to information security.

Davydova E., Makarova K. Peculiarities of Storage and Processing of Personal Data of Clients of the Bank. – PP. 293–297.
The software and hardware components providing business processes in the banking sphere are considered. The issues of ensuring the safety and security of personal data of private bank customers are analyzed. The analysis of the possibilities of using the "CryptoPro" system

for their protection is carried out. The requirements for the technical and technological components of data reception and processing are considered taking into account their safety and security.
Key words: Client, information, protection, private client, corporate client, business process, personal data security, CryptoPro, bank secrecy.

Danilova E., Lauta O., Mitrofanov M., Rakichkij S. Computer Attacks and Their Characteristics. – PP. 297–301.
An attack on elements of the information and telecommunications network are implemented in the form of purpose ful in fluences, leading to disruption or decrease in the efficiency of process cycles in a telecommunications network. The most common computer attacks «The Logical disconnection of subscribers». Computer attacks have probabilistics-time characteristics, determination of which allows to assess the degree of risk, select and implement protection measures.
Key words: computer attacks, the Logical disconnection of subscribers, probabilistics-time characteristics.

Desnitsky V., Meleshko A. Modeling Security Incidents in a System for Water Supply Control. – PP. 301–306.
Modeling security incidents is carried out within the framework of a model of a cyberphysical system for water supply control. The developed simulation testbed is based on microcontrollers of Arduino platform, level and water flow sensors, electric cranes and Python based software for centralized security monitoring and system management. The choice of specific software and hardware for building a simulation stand is substantiated. The paper demonstrates feasibility of tracking data on physical security events at the program-information level with the subsequent formation of security incidents of a certain type.
Key words: security incident, modeling, cyber-physical system, water supply control, Arduino.

Dzhusupov R., Fedoseev D. Features Portability of Source Code of Object-Oriented Programming Language Java. – PP. 306–309.
Java provides the simplest and most familiar form of portability-source code portability. This means that java programs should produce the same results regardless of the main processor, operating system, or compiler.
Key words: java, cross-platform programming, monitoring, data base.

Dobroselskij M., Kurnosov V., Larin A. On the Issue of Creation and Application of the Information Management Catalog for the Nomenclature of Basic Telecommunication Equipment. – PP. 309–313.
An analysis of methods and approaches to the construction of an information management catalog for the management of the nomenclature of supplies in the communications industry is given. The choice of the model of the NPS control system operation based on the application of the information management catalog (IAU) is substantiated. The method of choosing the rational composition of information included in the standard formats for the description

of supplies is outlined, and proposals are given for a list of functional tasks, the solution of which is expedient with the use of the IAU of the cataloging system for supply items.
Key words: information-management catalog, rational composition, nomenclature of supplies, functional tasks.

Dombrovski Y., Lepeshkin O., Fialkin I. The Objective Function of the Functionally Role Model of Access Control. – PP. 313–316.
The effectiveness of the access control system can be determined by the ability of the system to provide secure access to users to objects, while preserving the many accesses necessary for users of the system to perform their functional duties (accessibility). As a target function of the effectiveness of the access control system, you can use a linear combination of the function and the availability of information and the confidentiality function of the information.
Key words: access control system, automated information system, objective function, information accessibility function, confidentiality of information.

Dymchenko A., Kozlova O. System of Processing of Graphic Information. – PP. 316–320.
Nowadays the automated processing of graphic information has wide circulation in many branches of human activity. Indeed any intellectualized system contains in itself the module working with graphic data. In this direction it is possible to allocate the system of technical sight especially. In article will be reviewed the components connected with the systems of recognition of graphic images.
Key words: computer sight, recognition of images, analysis of the image, algorithm.

Erhshov A., Tsanyan A. Designing a Digital Three-Dimensional Terrain Model Based on Structural Lines and Elevations. – PP. 320–324.
For a digital three-dimensional model of relief defined by structural lines and elevation marks, a new type of constraint is introduced, allowing more fully to take into account the influence of contours on the relief shape. An effective algorithm for constructing a digital three-dimensional model based on triangulation with constraints of this type is proposed.
Key words: Digital three-dimensional model of a relief, triangulation, weak restrictions, strong restrictions.

Zharkimbekova A., Ospanova A., Sagindykov Kh., Sauanov B., Tuleuov B. Raspberry Pi (3 Model B) Microcomputer and Practical Perspectives of its Usage. – PP. 324–329.
In the paper the single-board Raspberry Pi minicomputer winning the increasing popularity among developers and users is described. The principal necessary hardware-software components for booting and working of the computer and also for extending of opportunities of its usage are described (for Raspberry Pi 3 Model B the latest model at the moment). Examples of projects and sources devoted to Raspberry Pi are reviewed. The algorithm on assembly of mobile device on basis of it and a software installation are given, the appropriate practical recommendations are provided. Some perspectives on Raspberry Pi usage are described.
Key words: Raspberry Pi, (single-board) microcomputer, expansion boards, hardware moduls.

Zhikhorev I. Application of the LabVIEW Program for Automation of Processes of Management and Control of Remote Equipment. – PP. 329–332.
Increasing informatization of society increases the importance of computer technology in managerial processes. Application of the capabilities of modern computer technology to automate the process of information processing can increase the productivity of labor, increase productivity and accelerate the exchange of management information.
Key words: automation of information processing, LabVIEW, virtual instrument.

Zemskov R., Shershnev A. Investigation of Applications of Unity3d Multimedia Platform. – PP. 332–336.
Unity3D is a cross-platform professional game engine, which is very popular in recent years. Its graphic, audio and video resources, lighting, physical effects can mimic a real environment, so you can improve the efficiency of game designers. In addition to the gaming industry, the products released with the Unity3D platform are used in various gonts of life. This article explored the application of Unity on the 3D display, virtual roaming and modeling systems.
Key words: Unity3D, cross-platform game engine, modeling systems, virtual roaming.

Zemskov R., Shershnev A. Using of Decision Support System in Military Communication. – PP. 336–339.
Decision Support System is a computer-based automated system whose purpose is to help people who make decisions in difficult conditions for a complete and objective analysis of the subject-matter activity. Decision support systems have emerged as a result of the merger of management information systems and database management systems.
Key words: decision support systems, military communications.

Zolotov, O., Yakubov N. Conservation Structures in Management Systems. – PP. 339–342.
Usually, the automatic control system is designed based on the fact that the parameters of objects and controllers (operators, transfer functions) are unchanged. However, in reality, we often deal with changes in these parameters. The article discusses the possibility of stabilizing the structures of objects and regulators, which will improve the quality of control systems. It is theoretically proved that the stabilization of structures is possible due to the use of the universal principle of feedback. The variants for cases of change of operators of one and two elements are considered. The notion of increment structure, thus considered only the additive option.
Key words: structure, management, preservation, feedback.

Ivanov D., Kotsynyak M., Lauta O., Murtazin I. Methodology of Cybernetic Sustainability under the Influence of Targeted Cybernetic Attacks. – PP. 343–346.
The article deals with a set of measures to study the impact of a targeted cybernetic attack on elements of the information and telecommunications network and conduct a logical and probabilistic method for assessing the danger of a targeted cybernetic attack, which allows choosing the option of protecting elements of the information and telecommunications network.
Key words: targeted cyber-attack, impact, vulnerability, information and telecommunications network, hierarchy analysis method.

Ivanov D., Kotsynyak M., Lauta O., Khokhlacheva E. Heuristic Model of the Targeted Cybernetic Attack. – PP. 346–351.
The article examines the model of the impact of a targeted cybernetic attack on the information and telecommunications network, which allows choosing a differentiated approach to protecting the information and telecommunications network and its elements.
Keywords: targeted cyber attack, impact, synthesis of defense system.

Izotova Y., Yurkin D. Probabilistic Approach Modeling for Performance of Certification Tests. – PP. 351–355.
The paper covers issues of effectiveness increase in automated systems evaluation for compliance with cybersecurity objectives. The approach is based on Signal Flow Graphs (SFG). SFG is a tool for analysis and modeling of discrete-time systems. Automated systems compliance with cybersecurity objectives evaluation is modeled. Branches from the graph represent evaluation (tests) and nodes refer to a state of a process (cybersecurity objectives). This approach is based on function weighting and conversion rule implementation. Average time and evaluation success probability are the factors for effectiveness increase.
Key words: automated systems, cybersecurity, Signal Flow Graph, transition function, course-of-value function, function weighting, path, circuit circle graph conversion, probabilistic temporal method.

Ilina O., Kupchinenko O., Skoropad A. About Mechanisms of Discretionary Differentiation of Access in Operating Systems of a Special Purpose. – PP. 356–360.
Automated systems implemented with the use of operating systems of a special purposes provide protection of different types of information from unauthorized access. Use of special modes of user rights restriction in operating systems of a special purpose allows to build a more flexible and reliable mechanism of information security in automated systems.
Key words: automated system, operating system of a special purpose, information security, unauthorized access, discretionary model of differentiation of access.

Kaznacheevava E., Shiyan A. "Smart home" for Disabled People. – PP. 360–365.
Modern life sets us a special rapid rhythm, but despite this, the daily life of any person should be comfortable. And the life of people with disabilities should not only be cozy, but also safe. Now a lot of attention is paid to this group of people and thanks to the smart home technology one can make his life comfortable.
Key words: smart home, algorithms, intelligence.

Kanatev D. Improving the System of Technical Condition of Electric Equipment of Systems. – PP. 365–369.
In article the way of control of technical condition of electric equipment of systems of power supply and also increase in efficiency, on a basis to which the method of contactless monitoring of technical condition is offered is offered. The scheme of development of a hardware and software system of a control system and monitoring of system of power supply is described.
Key words: monitoring of technical condition, system of power supply, automation.

Kapitonov N., Filippov F. Determination of Ways to Increase the Quality of Computer Vision Systems. – PP. 369–373.
Modern trends in the development of computer vision systems have been singled out. The prospective application of the neural network approach to the improvement of computer vision systems is grounded. A class of convolutional neural networks is chosen as a mathematical basis for computer vision systems. A parametric space for the description of convolutional neural networks is presented in the context of their application in computer vision systems. Sets of experiments on the study of ways to improve the performance of computer vision systems are described.
Key words: convolutional neural network, computer vision, pattern recognition.

Karachinskaya E., Ptitsyna L. Modeling Service-Oriented Systems for the Organization of Communicative Processes of Counterparties. – PP. 373–378.
The importance of communicative processes of counterparties is described at strengthening of influence of global economy on a technological way of society. The modern state of technological support of communicative processes of counterparties is analyzed. Prospective ways of its development are outlined. The advantages of using service-oriented systems for the organization of communicative processes of counterparties are presented. A basis of formalizations for their modeling is proposed. The methods of applying the results of modeling service-oriented systems for the organization of communicative processes of counterparties with a view to their relevance to high significance are disclosed.
Key words: technological structure, counterpart, communicative process, service-oriented system, modeling.

Karpov A. The Model of the Information Leakage Channel at the Information Object. – PP. 378–382.
Simulation of information leakage channels is essentially the only way to sufficiently study their capabilities with a view to the subsequent development of ways and means of protecting information. It is necessary to develop a model of the information leakage channel on the information object, which determines the conditions for their occurrence for a given object. The model is used for the design evaluation of information security from leakage or continuous monitoring of object parameters during its operation.
Key words: information Leakage Channel, informatization object, logical-probabilistic method, logical model, probabilistic function, information Security System.

Kireev S., Lauta O. Application of Artificial Intelligence Methods in Tasks of Computer Attack. – PP. 383–389.
The article describes an approach to detect network computer attacks on information and telecommunication networks based on the analysis of network activity and the selection of signs of abnormal behavior using machine learning techniques and artificial intelligence. As a mathematical apparatus for the implementation of the proposed approach, artificial neural networks that solve classification and prediction problems are considered, and possible applications of artificial neural networks for detecting abnormal behavior in the information network are considered.
Keywords: information-computer network, computer attacks, intrusion detection systems, artificial intelligence, machine learning, neural networks.

Kirillov V.,Kokaeva R., Moshak N. Formalization of the Authentications Idle Time Protocols in Multiservice Network on Ip-QoS Technology. – PP. 389–293.
Creation of the protected national multiservice communication network is a relevant task of the modern informational society. Use of mechanisms of protection demands formalization of their work and assessment of influence on characteristics of basic multimedia streams taking into account maintaining of the required quality of an upkeep. Models of protocols of simple authentication of an equal logical object and the sender of data in multiservice network allow to solve this problem partially.
Key words: Multiservice communication network, infotelecommuncation transport system, protocols of authentication, information security.

Kirillov V., Kokaeva R., Moshak N. Formalization of Protocols of Rigorous Authentication on the Basis of Asymmetric Algorithms of Enciphering in Multiservice Network on IP-QoS Technology. – PP. 393–398.
Use of mechanisms of protection demands formalization of their work and assessment of influence on characteristics of basic multimedia streams taking into account maintaining of the required quality of an upkeep. Models of protocols of rigorous authentication on the basis of asymmetric algorithms of enciphering in multiservice network allow to solve this problem taking into account an importation of temporary, legal and data-flow redundance in a network environment of network.
Key words: Multiservice communication network, infotelcommunication transport systemы, protocols of rigorous authentication, information security.

Kozin A., Ostrovsky Y. Software Analysis of Virtual Augmented Reality. – PP. 399–402.
"Augmented reality" (AR) is one of the latest achievements of science and technology. The technologies of augmented reality include those projects that are aimed at supplementing reality with virtual objects. This technology has a wide application in architecture, in marketing, in computer games, in military affairs.
Key words: AR, Augmented reality, displaying tactical information, single information space.

Kozlova L., Nikolaenko V. Methods and Means of Visualizing the Interface for the Automated System "Smart House" on the Basis of UX and UI Design. – PP. 402–405.
The data visualization is considered as a system for transferring complex ideas and data in a form that ensures the most effective work of a person. In the modern information society, visualization is an important aspect of information representation and the process of optimizing the operation of various systems with the user and a powerful tool of thoughtful saturation of the design in any of its forms.
Key words: smart house, interface, information technology, UX design, UI design, economy, comfort.

Kolesnichenko O., Kolesnichenko Y., Mazelis A., Mazelis L., Smorodin G., Yakovleva D. Technology of Spread Academic Research in Data Analysis. – PP. 405–408.
Justified and practically confirmed the possibility and relevance of research in the field of data analysis by employees of several universities – academic partners of Dell EMC.

The system of correlation of project proposals and competencies of academic teams was developed. Based on the pilot projects, the most popular research topics were identified: globalization of economic processes and data analysis in the field of medicine. The proper level of the obtained results was confirmed by testing the results at the English-speaking IEEE conferences and including publications in the international science metric databases.
Key words: distributed academic research, data analysis, global studies, academic partnerships.

Kolmykov M, Shiryaev V. Shiryaev M. Application of Modern Technologies of Automation and Management of the Official Activity of Students of Scientific Research Organizations. – PP. 409–412.
The use of modern automation and performance management technologies, like any other automation process, is one of the main objectives for increasing the efficiency, efficiency, and efficiency of the system used by employees of research organizations.
Key words: automation, software, C #, Windows Forms SQL.

Koltashev M. Using of Interpolation Method. – PP. 412–418.
For operational sets of values, getting an experimental test, it is required to build a function on which other values can be superimposed. Interpolation is a kind of approximation, in which the curve the constructed function passes through the estimates. If the function is too complicated for productive computations, then its value must be calculated at several points, and also to interpolate a simpler function, which will reduce in many cases the error in the results of calculations.
Key words: Interpolation, function, Lagrange method, Aitken method, Newton's method

Komarova A., Korobeynikov A., Menshchikov A. The Development of Asymmetric Algorithms in the Electronic Digital Signature Protocols and Their Further Application Prospects. – PP. 418–421.
In the modern information society every year more and more attention from government and private companies begins to be paid to the encryption of transmitted information, to the personal data protection, to authentication of users on the Internet and to other information security aspects. Asymmetric cryptography algorithms or public key cryptography find more and more wide application in the creation of modern information-secure society.
Key words: asymmetric cryptography, digital signature, factorization problem, discrete logarithm problem, post-quantum cryptography, security protocol, theory of lattices.

Kondratev D., Nosov M. Modern Data Storage Systems and Network Protocols. – PP. 422–427.
The article discusses the issues of data storage systems in relation to enterprises and organizations operating communication networks. The analysis of modern storage devices and network protocols is carried out. The advantages of using flash drives in data storage systems are shown.
Key words: single information space, data storage system, flash drives, network protocols.

Konkov D. Computer Model Channel Information. – PP. 427–432.
The theoretical and practical aspects of the development of a computer model of information transmission channel.
Key words: discrete and continuous transfer of information over the communication channel.

Korotkova M., Litvinov V., Sokolova K. Research of Machine Training Algorithms for the Analysis of Text Tonality in Social Media Resources. – PP. 432–436.
The article considers algorithms of machine learning that allow analyzing the tonality of a text in social media resources. Various types of classifications of the tonality of the text are considered. The features of some approaches to the classification of the text tonality are shown. Methods and algorithms of machine learning for analyzing the content of social media resources are offered, such as machine learning with a teacher and without a teacher.
Key words: machine learning algorithms, text tonality, social media resources, content, machine learning with the teacher.

Korotkova M., Litvinov V., Sokolova K. Application of Machine Training Tools in Internet Marketing Problems. – PP. 436–441.
In the article the concept of Internet marketing is formulated, the main provisions of intellectual marketing policy are given. The main tools and strategies of Internet marketing are considered, key components and its main advantages are revealed. The concepts of neural network and machine learning are presented. The main directions of the development of machine learning in the problems of Internet marketing are considered. Possible tools for implementing these tasks are described.
Key words: machine learning, precedent training, deductive training, artificial neural networks, Internet marketing, Internet marketing tools, Internet marketing strategies.

Kotlova M., Ptitsyna L. Analysis of Hybrid Cloud Solutions for Management of Data Storage Systems. – PP. 441–444.
The article considers the ideas of data center formation. The specifics of the functioning of systems ensuring the reliability of distributed information storage are analyzed. The analysis of modern infrastructure of multilevel data storage is carried out and the main problems of synergy between different levels are determined. The integration of cloud technologies into data storage systems is considered.
Key words: data center, data storage system, cloud solution, distributed file system, consensus algorithm.

Kotlova M., Ptitsyna L. Modern Methodologies of Organization of Long-Term Storage of Archival Data. – PP. 444–448.
An analysis of the current state and trends in the development of technological processes for the organization of long-term storage of information was carried out. The main problems are considered and requirements for methodologies for archival data preservation are formed. The main components of the science-based core of methodologies are presented. Architectural solutions for long-term information storage are described. Based on the analysis, trends in the development of storage technologies for archival data are determined.
Key words: storage system, storage standards, data storage formats, storage architecture.

Kuz'kin A., Kutsakin M., Lapko A., Ryabokon V. To the Problem of Transition to a Free Software. – PP. 448–452.

The state policy aimed at import substitution, including in the information sphere, implies the development and implementation of free software of domestic production in all areas of human activities. This issue is especially acute in the framework of state organizations and services. At the same time, the problems associated with the expenditure of material and time resources, with the rapid and effective training of personnel to primary skills in such software or operating systems of the Unix family, remain important. Also, the issue of transferring all information processes of an organization to Unix-systems is especially acute. In this paper, the procedure for acquiring primary skills in operating systems of the Unix family is briefly presented, as well as the composition and version of the stand for practicing practical tasks.

Key words: operating systems, Unix, Linux, staff training.

Kurnosov V., Polyakov Yu. Protection of Information in the Local Computer Network of the Enterprise of Contact. – PP. 452–455.

The analysis of the problem of information protection from unauthorized access in the local area network (LAN) is presented. The conceptual model of differentiation of access to information resources is considered. The evaluation of the effectiveness of decisions to protect against unauthorized access to information resources is given. Proposals on the organization of information security in the LAN of the communications enterprise are formulated.

Key words: information security, probable attacker, unauthorized access, local computer network, access control.

Kutsakin M., Lapko A., Ryabokon V. Fuzz Testing for Communication Protocol Security Flaws Detection. – PP. 456–460.

Network fuzz testing is an effective mechanism to ensure the security and reliability of communication protocols. However, such testing is still conducted in an ad-hoc manner with manual efforts, which is due to the unavailability of formal protocol model. In this paper we present our work of developing an automated protocol fuzz testing approach that uses a formally synthesized approximate formal protocol specification, guiding the testing process. Also preliminary results of using this method to implementations of the clients pidgin and aMSN are presented.

Key words: fuzzing, security testing, communication protocol.

Kutsakin M., Lapko A., Ryabokon V. Developing Database of Radiofrequency Applications Parameters Accounting in the Spectrum Management Problem. – PP. 461–466.

The article is devoted to the developing database of radiofrequency applications parameters accounting. Revealed the place of data accounting in the spectrum management problem. Described in detail the results of radio frequency applications analysis for the functional dependencies presence. Presented database logical structure scheme providing the selected objects relationship. Issues ensure database consistency.

Key words: database, data accounting, radiofrequency application, radiofrequency spectrum management.

Lebedeva A., Ptitsyna L. The Mathematical Support for System of Acquiring Knowledge About the Impact of Active Infrastructure on Quality of Functioning of Intelligent Information Agents. – PP. 466–470.
The article substantiates the necessity of development of for system of acquiring knowledge about the impact of active infrastructure on quality of functioning of intelligent information agents. The typical profile of agent's quality is highlighted. The functional problems of the considered mathematical support are defined. Activity of infrastructure in critical situations of agent's operation is formalized. Functional model's classes of intelligent information agents and methods of their analysis are described. The method for calculating quality indicators in the active infrastructure is developed.
Key words: information intelligent agent, object-oriented model, active information and communication environment.

Likar A., Morozov S. The Subsystem for Monitoring the Volume of Rooms Based on WiSee Technology. – PP. 471–474.
Passive infrared (IR) detectors are most often used as bulk detectors for closed rooms due to a combination of their relatively low cost and, at the same time, good functional characteristics. However, these detectors are characterized by a number of well-known characteristic shortcomings arising from the principles of work. To compensate for these shortcomings, two types of detectors are used, including two independent detection methods: passive IR and microwave detection. But the cost of detectors of combined type is much greater than that of passive infrared, which makes it difficult to use them massively. As a solution to this problem, it is proposed to use regular passive infrared detectors in combination with a WiSee technology detection sub-system.
Key words: bulk detector, WiSee.

Lovina V., Shiyan A. Use the Capabilities of the Cloud Service Bitrix24 for Collaboration of the Web-Development Team. – PP. 474–477.
Cloud computing service Bitrix24 developed by 1C-Bitrix is relevant for companies, where employees work remotely from diffferent places. Shared access to cloud tools among all the co-workers significantly increases the efficiency of their work.
Key words: cloud computing service, Bitrix24, web-developers.

Makarenkov K., Shestakov A. Automated Processing of Market Data to Evaluate Customer Loyalty Service Providers and Credit Institutions. – PP. 478–482.
Monitoring operators ensure agreements service level agreements (SLAs) for certain categories of consumers can be significantly enhanced through the methods of machine processing of commodity exchanges. The proposed solution will improve the business attractiveness in NGOSS intelligent data analysis tools for electronic trading that is compatible with existing software products BOSS, CRM and ERP systems.
Key words: the loyalty of the consumer, the electronic processing of data.

Makarov L., Pilikina E., Protasenya S. Mobile Network ZigBEE. – PP. 483–487.
Questions of the organization of robotic network on the basis of the ZigBEE technology providing remote control of serially released devices on cleaning of rooms in the extensive

territory with continued support of the modes of monitoring of quality of the performed works are considered.
Key words: ZigBEE network, robotic complex of devices.

Margaritova J., Ptitsyna L. The Concept of the Analysis of the Influence of Methods and Means of Extracting Knowledge on the Safety of Personal Data. – PP. 487–491.
The main aspects of the importance of confidentiality of personal data are considered. Methods and means of knowledge extraction are classified. The requirements for information protection are described. Formalized the idea of the relationship between methods and means of extracting knowledge with the protection of personal data in the environment of information infrastructures. The key provisions of the concept of research on the influence of methods and means of extracting knowledge on the safety of personal data are disclosed.
Key words: information security, confidentiality, extraction of knowledge, invasion, neural networks, data mining.

Medvedev V. Probabilistic Characteristics of Binary Sequence. Ending. – PP. 491–494.
Is considered a binary sequence as model various its implementations in which the value can be one of two possible values. Demonstrates how to determine the probabilities of reams of zeros and ones based on the probabilities of independent samples of one or several positions of the binary sequence. Shows the formula ratio.
Key words: the binary sequence, model P-the probability, G-probability.

Moskalenko N., Osinkin D. Technologies of Tracking Objects in a Video Stream Based on Particle Filter. – PP. 495–497.
The task of tracking objects in a video stream is an integral part of many application areas, such as building video surveillance systems, creating human-computer interfaces, programs for transferring or compressing video, and more. When solving the task of tracking an object in a video stream, it is necessary to process a huge amount of data, frames, which increases the processing power and also increases the processing time. This is especially true if the location of an object in a stream is not normal, multimodal, or generally of an arbitrary nature.
Key words: tracking objects, video processing, particle filter, object recognition.

Nesterov A. Transport FOCL as Spectral Transmission Agent. – PP. 498–500.
The article is devoted to the use of terminology for the modeling of multi-agent systems, which makes it possible to present FOCL as a set of interrelated elements (agents) depending on the functions performed by them, such as: spectral transmission agent; transport medium agent.
Key words: FOCL, interrelated agents, modeling of multi-agent systems.

Novruzov A., Shiryaev V., Shiryaev M. PHP or ASP.NET. – PP. 501–504.
In the article the problems of choosing a programming language for developing a web site are discussed. There is a rich choice of which language to use: Perl, PHP, ASP, ASP.Net, JSP, Coldfusion. The most common today are PHP and ASP.NET. In the article, a comparative analysis was made between these platforms.
Key words: PHP, ASP.NET, programming, web site, database, framework.

Olimpiev A. Methods of Synthesis of Operational and Technical Monitoring System with a Functionality Metacontrol. – PP. 505–510.
One of the problems associated with the synthesis of the system of operational and technical monitoring is the need for predictation of the adaptation processes to the conditions of application, which will happen at the stage of application support. The article proposes a method of synthesis of operational and technical monitoring, in which the problems of adaptation are solved at the stage of technical design.
Key words: monitoring, informational system, functionality metacontrol.

Ospanova A., Tuleuov B. Perspectives of Usage of Microcomputer Raspberry Pi in Effective Digitalization on the Example of Kazakhstan. – PP. 510–515.
The popular among developers single-board computer Raspberry Pi is considered. The research projects on the basis of Raspberry Pi 3 Model B and Raspberry Pi Zero models providing, according to authors, rational decisions in the fields of activity requiring use of specialized hardware-software support or the considerable hardware computing resources are offered and described.
Key words: Raspberry Pi, (single-board) microcomputer, mobile (automated) experts workplace, hardware computing resources, the universal computer class

Ostrovsky Y., **Tiridatov S.** Application of Neuro-Computer Interfaces for Controlling a Perfect Platform for Special Purpose. – PP. 515–519.
The article deals with the issues related to the use of neurocomputer interfaces (NCI) for the management of a mobile special purpose platform, based on the recognition of actions mentally presented to the servicemen. The general structure with the stages of the collection and processing of the EEG signal is presented, as well as the rationale for choosing the hardware.
Key words: neurocomputer interface, brain-computer, mobile platform, driver of electric motors, radio control equipment.

Ostrovsky Y., **Shaisultanov M.** Neuro Computer Interface for Training Systems for Military Purpose. – PP. 520–524.
The method of constructing the hardware-software module of a neurocomputer interface with biofeedback is considered in order to increase the efficiency of training systems based on the introduction of modern information technologies. A general structure is presented with the steps of collecting and processing the signal of the encephalogram (EEG), as well as the rationale for choosing the hardware.
Key words: neurocomputer interface, biological feedback, encephalogram.

Pantjuhin O., Paraschuk I.B., Saenko I. The Analysis of State of the Art on Information Access Control Simulation in Cloudy Infrastructures of Crucial Information Systems. – PP. 524–529.
The paper proposes systematized results of the detail analysis of state of the art in area of information access control taking into account the specifics peculiar to cloudy data storage systems which are components of crucial information systems. Analysis results of a state of the art are given in a scope of methods of artificial intelligence for optimization, verifica-

tions and reconfigurations of access control policies. Use of results of this analysis will allow one to increase validity of decision-making in the development areas and applications of perspective access control models for the purpose of clearing up of opportunities and methods of their implementation in cloudy infrastructures.
Key words: crucial system, information system, access control policy, cloudy infrastructure, information security.

Pesikov E. Automated System of Diagnostics and Forecasting the Financial State of the Enterprise with the Use of Methods of Research of Operations, Discriminant Analysis and Neural Networks. – PP. 530–535.
An approach is considered to improve the quality of forecasting the bankruptcy of an enterprise, which makes it possible to provide the required level of strategic management decisions. Analytical tools are offered for diagnostics and financial solvency forecasting, based on the application of the analytic hierarchy process, discriminant analysis with subsequent refinement of forecasting results using a neural network. The results of computational experiments on the solution of the problems under study are discussed.
Key words: enterprise, forecasting, bankruptcy, analytic hierarchy process, discriminant analysis, neural network, multi-layer perceptron.

Polpudnikova N., Shestakov A. Proposals for Automated Maintenance of the Original Design Documentation of the Enterprise Communications Based on the Technology of Distributed Registries. – PP. 535–540.
The questions of maintaining originals of design documentation of the enterprise-developer of means of communication both paper, and electronic design documentation at various stages of a product life cycle are considered. In order to provide integrated approaches in the conditions of change and development of technologies in records management and document flow by electronic documents and to increase the security of information of originals of design documentation, approaches to the use of technology of distributed registers are proposed, taking into account the existing and used in enterprises software and hardware-software management of product data and product life cycle.
Key words: the original design documentation, PDM/PLM systems, technology of distributed registries.

Ptitsyna L., Tarabarov A. Analysis of Methods for Integrating Information Security Tools. – PP. 541–544.
The urgency of improving the quality of functioning of complex information security systems is substantiated. The main directions of improving information security technologies are presented. A system for classifying methods for integrating protective equipment is described. Extended profiles of the quality of complex information security systems were chosen. Basic classes of situational models for integrating protective equipment are formed. The mathematical apparatus for the analysis of base classes of situational models of complexing of protection means is opened.
Key words: information security, data protection, integration of funds, object-oriented model, feedback.

Ptitsyna L., Elsabayar Shevchenko N. Intellectual Integration of Cluster Segments of Service-Oriented Systems. – PP. 544–549.
Cluster segmentation of service-oriented systems of large corporations is actualized. The key features of the hard and soft segmentation of service-oriented systems are described. A multi-agent approach to the soft integration of cluster segments of service-oriented systems is proposed. Variations in the organization of action planning for the multi-agent integration system have been determined. A form of representation of the action planning algorithms for the multi-agent integration system is chosen. A mechanism for coordinating schedulers with an update of the technological basis of the multi-agent system has been singled out. The concept of comparative analysis of variations in the organization of a multi-agent system has been developed.
Key words: cluster segmentation, multi-agent approach to integration, planning actions, soft integration, self-organization.

Slivkov V., Khodanovich A. The Time Complexity of the Algorithms and Regression Analysis in Computer Modeling. – PP. 549–553.
Conceptual aspects of the complexity theory of algorithms in problems of computer simulation are considered. The threshold effect in time complexity of the algorithm is shown, as well as an example of hypothetical equivalence of classes of algorithmic problems. The time complexity of the algorithm in the computer model of a nonlinear dynamic system with discrete symmetry is estimated, as well as the result of regression analysis of the numerical solution.
Key words: algorithm, time complexity, computer model, regression analysis.

Starostin V. Singular Values of Fading Channel Matrix and Their Influence on a Vulnerability of Dean-Goldsmith Cryptosystem. – PP. 554–559.
Keyless cryptosystem proposed by Dean and Goldsmith is investigated. This cryptosystem was declared by its inventors as a very perspective one. However it was shown by group of authors in the paper published recently in "Proceedings of Telecommunication Institutions" that positive properties of this cryptosystem can be lost if the number of eavesdropper's antennas is only slightly more than the number of legal user's antennas. The current paper confirms this "paradox" and clarify it theoretically in terms of singular values of fading channel matrix.
Key words: physical–layer security, fading channel, cryptosystem, singular values.

Stepanov A., Shiryaev V., Shiryaev M. Design and Research of Acoustic Noise Generators. – PP. 559–562.
Acoustic channel of information exchange between persons is very important. This fact leads to invitation of measures for protection sensitive acoustic information. There are passive and active methods for protection against information leakage. Active methods include acoustic and vibroacoustic masking of voice.
Key words: acoustic channel, noise generator.

Strelkov O. The use of 3D Animation GIS for Military Purposes. – PP. 562–565.
In modern times, the decisive factor is the operational solution of the tasks and the correct use of modern means to achieve a positive result. Previously, two-dimensional paper maps

were used, which are still not taken into account, objects of the operational situation are manually applied to them and the results of any tactical decisions are calculated by formulas. The task is to demonstrate the movement of objects, indicating their real characteristics, which will reduce the time for decision-making.
Key words: 3D-animation, geographic information system, program, scenario, modeling, classifiers of three-dimensional models.

Strokov A., Shiryaev M., Shiryaev V. DBMS PostgreSQL and Its Application for Development of Databases in ACS of Special Purpose. – PP. 565–570.
An analysis of the existing problems of the use of special forces indicates that the information aspects come to the fore. Functional integration of PostgreSQL DBMS in Astra Linux is implemented in the interests of increasing the efficiency and security of the application of special purpose systems.
Key words: database management system, automated management system, PostgreSQL, Astra Linux.

Suvorov A., Tsvetkov A. The Study of Attacks Such as Buffer Overflow in a 64 Bit Unix Like Operating Systems. – PP. 570–573.
Buffer overflow attacks exploit vulnerabilities in the stack. The simplest form of buffer overflow attack is to accept malicious user inputs, stack them, and affect local variables / return address / arguments that are stored in the stack. This can lead to changing the values of variables or even the change of the instructions which causes the program. The worst cases of such attacks can lead to attackers gaining remote control of your machine over the network.
Key words: buffer, attack, UNIX, overflow, damage, Linux, data, information security.

Surzhikov I. About the Technical Systems of Stationary Communication Centers. – PP. 574–577.
In this article the structure and features of technical systems of stationary communication centers within preparation of the decision on increase in effectiveness of their functioning regarding development and test of the automated systems of monitoring of parameters of engineering networks of express objects is surveyed.
Key words: Technical systems, system of power supply, category of reliability, monitoring.

Taranov S.V. Integrity Method Based on Wavelet Codes. – PP. 578–582.
Security-oriented codes take an important place in integrity ensuring of modern storage and information processing systems. One of the perspective methods for the integrity ensuring is wavelet codes that can detect algebraic manipulations. Proposed method is able not only to detect errors of any multiplicity, but also is stable in case of nonuniform distributions of input codewords.
Key words: integrity, coding theory, robust codes, wavelet transform.

Topkasov M. Information War. – PP. 582–585.
Over the past decades, many countries are fundamentally reviewing the forms and methods of warfare. Approximately 20 years ago, the theater of military operations was divided into

two components: conventional space and information, where preference was given to the usual space, now, as military experts of these countries note, the information space is increasingly being viewed as the main sphere of military operations.
Key words: Information war, Russia, USA.

Khaibrakhmanova E., Shiyan A. Ergonomics in Web-Design. – PP. 585–589.
The article is devoted to the interrelation between ergonomics and web design. Ergonomics allows you to formulate principles and requirements for the web-interface. Thereby web-resource with becomes an ideal human-machine interface.
Key words: ergonomics, information system, design, human-machine interface.

Chaunin M. The Portable Software to Support the Teaching of Information Disciplines. – PP. 589–593.
An option is proposed for creating portable software, which can be used in the teaching of information cycle disciplines. The proposed package contains, in particular, tools for developing applications in C / C ++, Java, Python, Perl. It does not require installation in the Windows operating system and can be placed on a local hard disk or any removable media.
Key words: Portable, Shell, Environment variable.

Shadrin D., Shiryaev M., Shiryaev V. Research of the Possibilities of Decision Support Systems for Creation of Information Interaction of Officials of the Military Management Authority. – PP. 593–597.
This article discusses the basic principles of building decision support systems, their structure, capabilities and the tasks they solve. Also this article describes the possibility of using decision support systems to creation of information interaction of officials of the military management authority.
Key words: decision support systems, information interaction, military management, information technology.

Shamrov N., Shiryaev V., Shiryaev M. Research of Processes of Automation of Management of Scientific and Educational Activity of VUZ`s. – PP. 597–600.
The process of automating systems for planning, monitoring and evaluating scientific activity, like any other automation process, was one of the main problems of increasing the efficiency, efficiency, and efficiency of the system. The solution for this problem is always individual and requires an individual approach to creating automation solutions.
Key words: automation, software, ASP.NET WebForms, SQL, server, C #.

Shershnev A. Problems of Mathematical Modeling of Military Operations. – PP. 600–602.
Modeling in the military sphere is of great importance. In order to obtain adequate results, the simulated system and its model must match each other according to the criteria and attributes necessary to achieve the research goal, but in addition there are a number of problems that complicate the process of creating models.
Key words: mathematical modeling, modeling of military operations.

Shiryaev V., Shiryaev M., Shlyakhov I. Analysis Systems Modeling of Transport Networks. – PP. 603–607.
The article is devoted to analysis of modeling of transport communication networks. It considers the basic means of modeling transport communication networks and evaluated them.
Key words: transport network, simulation, protocol, Cisco Paked Tracer, AnyLogic, BGP.

Shiryaev S., Shiyan A. Automation of Production Process of Filling Carton Boxes by Production on Polygraph Factory. – PP. 607–611.
Many unskilled workers used in Russian printing industries. International companies working in this field are rapidly implementing robotic production lines that allow a sharp increase in labor productivity and redact in amount of workers employed in the factory. Overcoming the backlog of domestic companies is possible only by modernizing existing production facilities by introducing fully or partially robotic conveyor lines.
Key words: automation of production processes, printing enterprises, robotics.

АВТОРЫ СТАТЕЙ

АВЕРЧЕНКОВ
Роман Андреевич — магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, старший инженер-программист ООО «ВейвАксесс Сервис», averchenkov.r.a@gmail.com

АВРАМЕНКО
Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АДУЕВСКИЙ
Александр Михайлович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, sashabommm341@gmail.ru

АКИМОВ
Сергей Викторович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov-sv@yandex.ru

АЛМАДАТОВА
Айсел Фахраддин гызы — ассистент кафедры компьютерной инженерии и телекоммуникаций Азербайджанского Технологического Университета, almadatovaaysel@gmail.com

АНДРЕЕВ
Александр Дмитриевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex.an22@mail.ru

АНДРЕЯНОВ
Ярослав Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreyanov78@yandex.ru

АНДРИАНОВ
Владимир Игоревич — кандидат технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.andrianov@gmail.com

АНТОНОВ
Валерий Валентинович
старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antonler@rambler.ru

АРТЕМЬЕВА
Виктория Денисовна
студентка медицинского института Балтийского федерального университета им. Канта, vika_med2019@mail.ru

АХМЕДОВ
Нурбек Медетбаевич
магистрант кафедры автоматизации предприятии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, time_shift92@mail.ru

БАГОМЕДОВА
Алина Рашидовна
студентка группы ИКТЗ-43 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bagomed_alin@bk.ru

БЕЛОУС
Константин
Владимирович
кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kostos2@yandex.ru

БЕЛОШЕЕВА
Полина Владимировна
заведующая лабораторией кафедры информационно управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, belosheeva.polin@mail.ru

БОБРЕШОВ-ШИШОВ
Даниил Игоревич
курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, dbober94@gmail.com

БОГОЛЕПОВ
Григорий Сергеевич
заместитель начальника НИО-4 НИЦ Военной академии связи им. Маршала Советского Союза С. М. Буденного, bogolepov@inbox.ru

БОТЯКОВ
Вячеслав Витальевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wiseboy@yandex.ru

БРЕЧКО
Александр Александрович
адъюнкт кафедры Военной академии связи им. Маршала Советского Союза С. М. Будённого, sashabreck27@gmail.com

БУЛЫГИН
Григорий Александрович
магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gri9996@yndex.ru

БЫЧИХИНА
Алина Васильевна
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alisha.brusnika@mail.ru

ВАГАНОВ
Александр Валерьевич
старший преподаватель кафедры автоматизации предприятия связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut-ispiu@mail.ru

ВАСИЛЬЕВ
Иван Андреевич
старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivan3dgraphic@yandex.ru

ВАЧУГОВА
Виктория Алексеевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarakanovfers@gmail.com

ВАШУРИНА
Екатерина Михайловна
курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, vlasenko199@yandex.ru

ВЕЛИКАНОВ
Антон Михайлович
инженер-исследователь лаборатории факультета безопасные информационные технологии Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, i_krov@mail.ru

ВЕРДИЕВ
Сакит Гамбай оглу
доктор технических наук, профессор кафедры компьютерной инженерии и телекоммуникаций Азербайджанского Технологического Университета, info_tel@inbox.ru

ВЕРХОВА
Галина Викторовна
доктор технических наук, профессор, заведующая кафедрой автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina500@inbox.ru

ВИКСНИН
Илья Игоревич
аспирант кафедры проектирования безопасных компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, viksnin@corp.ifmo.ru

ВИНОГРАДОВ
Юрий Николаевич
магистрант кафедры информационных управляющий систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vinogradoffyuri@gmail.com

ВИНОКУРОВ
Марат Юрьевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, maratux@gmail.ru

ВИТКОВА
Лидия Андреевна — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iskinlidia@gmail.com

ВЛАСЕНКО
Максим Андреевич — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, vlasenko199@yandex.ru

ВОЛОШИНОВ
Денис Вячеславович — доктор технических наук, доцент, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis.voloshinov@yandex.ru

ВОЛЩУКОВ
Матвей Юрьевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neve75@mail.ru

ВОЛЫНКИН
Павел Александрович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavelas@mail.ru

ВОРОНОВ
Вячеслав Игоревич — доцент кафедры «Интеллектуальные системы в управлении и автоматизации» Московского технического университета связи и информатики, vorvi@mail.ru

ВОРОНОВА
Лилия Ивановна — доктор физико-математических наук, профессор, заведующая кафедрой «Интеллектуальные системы в управлении и автоматизации» Московского технического университета связи и информатики, voronova.lilia@yandex.ru

ВОСТРЫХ
Алексей Владимирович — старший инспектор группы информационного обеспечения деятельности МЧС России Главного управления МЧС России по Новгородской области, vostrykh.al@mail.ru

ГАВРИЛОВ
Александр Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, killervsspree@gmail.com

ГАГАРИН
Юрий Юрьевич — командир роты безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

ГАЙФУЛИНА
Диана Альбертовна — практикант Санкт-Петербургского института информатики и автоматизации Российской академии наук, студентка магистратуры Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, wing7803@yandex.ru

ГАТЧИН
Иван Юрьевич — ассистент кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, gatchin@rambler.ru

ГВОЗДКОВ
Игорь Вячеславович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gvozdkov@rambler.ru

ГЕНЧЕЛЬ
Ксения Владимировна — магистрант кафедры «Интеллектуальные системы в управлении и автоматизации» Московского технического университета связи и информатики, genchelkseniya@mail.ru

ГЕРЛИНГ
Екатерина Юрьевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com

ГЛУХОВСКИЙ
Михаил Дмитриевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikhail-glukhovsky@yandex.ru

ГОЛОВЛЁВА
Юлия Андреевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, golovlyova96@mail.ru

ГОЛУТВИНА
Юлия Александровна — студентка группы ИСТ-611м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, komsomolo4ka@gmail.com

ГРИГОРЬЕВА
Анастасия Алексеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kostos2@yandex.ru

ГРИШЕНЦЕВ
Алексей Юрьевич
доктор технических наук, доцент кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, grishentcev@ya.ru

ГРОМОВ
Владислав Витальевич
кандидат технических наук, доцент кафедры Инженерной графики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov_vladislav@hotmail.com

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

ГУДКОВ
Максим Андреевич
кандидат технических наук, начальник отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

ГУНИНА
Елена Викторовна
кандидат педагогических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v.gunina@yandex.ru

ГУРЬЯНОВ
Сергей Сергеевич
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, gurianov_ss_1995_06_01@mail.ru

ГУСЕВ
Дмитрий Сергеевич
студент группы ИСТ-611м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gusev999dima@gmail.com

ГЯНДЖИЕВ
Эмил Эльнурович
магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nexus.n8@gmail.com

ДАВЫДОВА
Екатерина Викторовна
старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Davydovaev1@yandex.ru

ДАНИЛОВА
Елена Ивановна
преподаватель кафедры Военной академии связи им. Маршала Советского Союза С.М. Буденного, S15136@mail.ru

ДЕСНИЦКИЙ
Василий Алексеевич
кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vasily.desnitsky@mail.ru

ДЖУСУПОВ
Руслан Алиханович
старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, 4s.bezdna@gmail.com

ДИКИЙ
Дмитрий Игоревич
аспирант кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, dimandikiy@mail.ru

ДОБРОСЕЛЬСКИЙ
Михаил Анатольевич
кандидат технических наук, доцент, главный научный сотрудник АО «НИИ «Рубин», dma@rubin-spb.ru

ДОМБРОВСКИЙ
Ярослав Аркадьевич
начальник факультета Военной академии связи им. Маршала Советского Союза С.М. Буденного, nina_vlasova_79@mail.ru

ДУДНИКОВА
Мария Николаевна
магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dudmashhh@gmail.com

ДЫМЧЕНКО
Александр Вячеславович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex.dym96@yandex.ru

ЕЛСУКОВ
Артем Игоревич
студент Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, инженер Научно-производственного объединения «Аврора», artemdeimon@gmail.com

ЕРШОВ
Александр Владимирович
начальник НИО-5 НИЦ Военной академии связи им. Маршала Советского Союза С. М. Буденного, aerchov@mail.ru

ЖАРКИМБЕКОВА Айжан — докторант кафедры информатики и информационной безопасности Евразийского национального университета им. Л. Н. Гумилева, o.ademi111@gmail.com

ЖИТКОВ Константин Дмитриевич — студент Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, zhitkovkostya@gmail.com

ЖИХОРЕВ Илья Сергеевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, sun72_69@mail.ru

ЗЕМСКОВ Руслан Андреевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, rus.zemskov@mail.ru

ЗОЛОТОВ Олег Иванович — кандидат технических наук, профессор, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oleg-1938@mail.ru

ИВАНОВ Денис Александрович — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

ИВАНОВА Валентина Афанасьевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iva.06@yandex.ru

ИЗОТОВА Юлия Олеговна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, izotova-4@yandex.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, доцент, старший преподаватель кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

ИОФИК Анна Леонидовна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anna-ifik@mail.ru

КАЗНАЧЕЕВА Екатерина Сергеевна — студентка группы ИСТ-612м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekaterina2694@mail.ru

КАНАТЬЕВ
Дмитрий Михайлович — оператор научной роты научно исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, dim.kan95@mail.ru

КАНТАРБАЕВ
Рафаэль Тимурович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kantraf@mail.ru

КАПИТОНОВ
Никита Сергеевич — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mof2k@mail.ru

КАРАЧИНСКАЯ
Елизавета Анатольевна — студентка группы ИСТ-711м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elizavetakarachinskayaa@gmail.com

КАРПОВ
Александр Владимирович — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, a.kar1986@yandex.ru

КИРЕЕВ
Сергей Хаирбекович — старший научный сотрудник Военной Академии Связи им. Маршала Советского Союза С. М. Будённого, gamlet8806@rambler.ru

КИРИЛЛОВ
Виталий Владимирович — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mr.kirillov.vitaliy@gmail.com

КОВЦУР
Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЖАНОВ
Юрий Федорович — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juriy.kozhanov@mail.ru

КОЗИН
Андрей Викторович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, Andrey-kolunev@mail.ru

КОЗЛОВА
Людмила Петровна
кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tigrenok59@mail.ru

КОЗЛОВА
Ольга Александровна
старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k_olga_a@mail.ru

КОКАЕВА
Регина Сославовна
магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kokaeva-R@gaz-is.ru

КОЛЕСНИЧЕНКО
Ольга Юрьевна
кандидат медицинский наук, главный редактор интернет-портала Security Analysis Bulletin, oykolesnichenko@list.ru

КОЛЕСНИЧЕНКО
Юрий Юрьевич
директор интернет-портала Security Analysis Bulletin, green-apple_2000@mtu-net.ru

КОЛМЫКОВ
Михаил Сергеевич
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, kolmihser@gmail.com

КОЛТАШЕВ
Максим Алексеевич
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, thisismax1@yandex.com

КОМАРОВ
Игорь Иванович
кандидат физико-математических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i_krov@mail.ru

КОМАРОВА
Антонина Владиславовна
аспирант кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, piter-ton@mail.ru

КОНДРАТЬЕВ
Дмитрий Михайлович
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, dk49911081@mail.ru

КОНЬКОВ
Денис Иванович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, den.konkov.94@mail.ru

КОРОБЕЙНИКОВ
Анатолий Григорьевич — доктор технических наук, профессор, заместитель директора по науке Санкт-Петербургского филиала Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук; профессор кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, Korobeynikov_a_g@mail.ru

КОРОТКОВА
Мария Игоревна — студентка группы ИСТ-611м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marikor168@gmail.com

КОРЯКИН
Денис Дмитриевич — командир научного взвода – младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, koryakinen@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

КОЦЫНЯК
Михаил Антонович — доктор технических наук, профессор кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

КОЧМАРИК
Нина Николаевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kochmarik.n@yandex.ru

КРАСНОВ
Виталий Иванович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, 9bublik7@gmail.com

КУЗНЕЦОВ
Сергей Иванович — кандидат технических наук, доцент кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, Ayaana95@mail.ru

КУЗНЕЦОВА
Александра Дмитриевна — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kyznyasha@icloud.com

КУЗЬКИН
Александр Александрович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, lev@academ.rsnet.msk.ru

КУЛИКОВА
Таисия Дмитриевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulikova.245@yandex.ru

КУПЦОВ
Алексей Владимирович — студент группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ileha@yandex.ru

КУПЧИНЕНКО
Ольга Павловна — преподаватель кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, k-olga102@yandex.ru

КУРНОСОВ
Валерий Игоревич — доктор технических наук, профессор кафедры автоматизации предприятии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, time_shift92@mail.ru

КУЦАКИН
Максим Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, max_kooks@mail.ru

КХОДЕР
Хабиб Мухссен — аспирант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, h.khoder@list.ru

ЛАПКО
Александр Николаевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, lan46@mail.ru

ЛАРИН
Александр Александрович — научный сотрудник АО «НИИ «Рубин», dma@rubin-spb.ru

ЛАУТА
Олег Сергеевич — кандидат технических наук, преподаватель кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, laos-82@yandex.ru

ЛЕБЕДЕВА
Анна Андреевна — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, annalebedeva4@mail.ru

ЛЕПЕШКИН
Олег Михайлович — доктор технических наук, старший преподаватель кафедры, доцент Военной академии связи им. Маршала Советского Союза С.М. Буденного, nina_vlasova_79@mail.ru

ЛИКАРЬ
Александр Иванович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, likar_a@mail.ru

ЛИПАТНИКОВ
Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник НИО-4 НИЦ Военной академии связи им. Маршала Советского Союза С. М. Будённого, lipatnikovanl@mail.ru

ЛИТВИНОВ
Алексей Андреевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, litvinovaa333@rambler.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-l@nm.ru

ЛИТВИНОВ
Даниил Владиславович — студент группы ИСТ-711м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, crazycat@nm.ru

ЛОВИНА
Валерия Витальевна — студентка группы ИСТ-612 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lovinavaleria@gmail.com

МАЗЕЛИС
Андрей Львович — кандидат физико-математических наук, доцент кафедры математики и моделирования Владивостокского государственного университета экономики и сервиса, andrey.mazelis@vvsu.ru

МАЗЕЛИС
Лев Соломонович — доктор экономических наук, заведующий кафедрой математики и моделирования Владивостокского государственного университета экономики и сервиса, lev.mazelis@vvsu.ru

МАКАРЕНКОВ
Кирилл Евгеньевич
магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, workmakarenkovke@yandex.ru

МАКАРОВ
Леонид Михайлович
кандидат технических наук, доцент кафедры автоматизация предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elfbio@gmail.com

МАКАРОВА
Ксения Сергеевна
Студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarovakseny@yandex.ru

МАЛИКОВ
Альберт Валерьянович
адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, albert4331@yandex.ru

МАМЕДОВ
Сахил Рафиг оглы
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stolsken@mail.ru

МАРГАРИТОВА
Яна Сергеевна
студентка группы ИСТ-711м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margaritova.yana@yandex.ru

МАРИНЕНКОВ
Егор Денисович
студент кафедры проектирования безопасных компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, mandarin-98@mail.ru

МАТВЕЕВ
Александр Сергеевич
магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Propala33@mail.ru

МЕДВЕДЕВ
Валерий Александрович
кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, medvedev.spb@list.ru

МЕЛЕШКО
Алексей Викторович
студент магистратуры Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, lexa.0710@gmail.com

МЕНЩИКОВ
Александр Алексеевич — аспирант кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, menshikov@corp.ifmo.ru

МИТРОФАНОВ
Михаил Валерьевич — кандидат технических наук, доцент, заместитель начальника кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, S15136@mail.ru

МОРОЗОВ
Сергей Константинович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, vmmm@mail.ru

МОСКАЛЕНКО
Николай Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, ice11.11@mail.ru

МОШАК
Николай Николаевич — доктор технических наук, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nnmoshak49@mail.ru

МУРТАЗИН
Ильдар Робертович — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

НАГИЕВА
Абабил Фахраддин гызы — старший преподаватель кафедры компьютерной инженерии и телекоммуникаций Азербайджанского Технологического Университета, a.naqiyeva@uteca.edu.az

НЕСТЕРОВ
Андрей Дмитриевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, kontr-x@mail.ru

НЕЧЕПУРЕНКО
Александр Петрович — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

НИКОЛАЕНКО
Вячеслав Константинович — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mooren55@gmail.com

НОВРУЗОВ
Ахмет Ровшанович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, Akhmet-Novruzov@yandex.ru

НОСОВ
Михаил Иванович — доктор технических наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, dk49911081@mail.ru

ОЛИМПИЕВ
Алексей Александрович — начальник сектора разработок информационно-управляющих технологий отдела информационных технологий АО «Институт инфотелекоммуникаций», lelik@iitc.ru

ОСИНКИН
Дмитрий Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, dm.osinkin@gmail.com

ОСПАНОВА
Адеми Бекжановна — кандидат физико-математических наук, доцент кафедры информатики и информационной безопасности Евразийского национального университета им. Л. Н. Гумилева, o.ademi111@gmail.com

ОСТРОВСКИЙ
Юрий Николаевич — старший преподаватель 12 кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, ostrovskii_urii@mail.ru

ПАНТЮХИН
Олег Игоревич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ПАРАЩУК
Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, сотрудник Международной лаборатории безопасности киберфизических систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, shchuk@rambler.ru

ПЕСИКОВ
Эдуард Борисович — доктор технических наук, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ed_pesikov@mail.ru

ПЕТРОВА
Айаана Николаевна
магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ayaana95@mail.ru

ПЕШКОВ
Андрей Иванович
кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ap2000@yandex.ru

ПИЛИКИНА
Елена Анатольевна
старший преподаватель кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, helenarh@yandex.ru

ПЛЕТНЕВ
Ярослав Андреевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pletnevyaroslav@gmail.com

ПОЛПУДНИКОВА
Наталья Викторовна
студентка группы ИСТ-441 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, santpetesburg521@yandex.ru

ПОЛЯКОВ
Юрий Юрьевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yura72_53_94@mail.ru

ПРОТАСЕНЯ
Сергей Витальевич
кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serj_p@pochta.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

РАКИЦКИЙ
Станислав Николаевич
кандидат военных наук, доцент кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, S15136@mail.ru

РОГАЧЕВ
Виктор Алексеевич
кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, rogachevv50@gmail.com

РЯБОКОНЬ
Владимир Владимирович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, mimicria@mail.ru

САГИНДЫКОВ
Хаким Молдабекович — кандидат технических наук, доцент, заведующий кафедрой информатики и информационной безопасности Евразийского национального университета им. Л. Н. Гумилева, o.ademi111@gmail.com

САЕНКО
Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, сотрудник Международной лаборатории безопасности киберфизических систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, ibsaen@mail.ru

САЗОНОВ
Антон Олегович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, ant-sazon@yandex.ru

САУАНОВ
Багдат — магистрант кафедры информатики и информационной безопасности Евразийского национального университета им. Л. Н. Гумилева, o.ademi111@gmail.com

СЕВОСТЬЯНОВА
Анастасия Сергеевна — магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, SevostianovaAS@yandex.ru

СЕЛЕЗНЕВ
Владислав Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minakov09@mail.ru

СЕРГЕЕВА
Инна Юрьевна — аспирант защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergeeva501@yandex.ru

СКЛЯРОВА
Екатерина Анатольевна — магистрант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, magnoliy6@yandex.ru

СКОРОПАД
Александр Витальевич — ведущий инженер-электроник НИЛ №4231, НИО №423, НТЦ №42 Санкт-Петербургского филиала «Ленинградское отделение научно-исследовательского института радио» (Филиал ФГУП НИИР-ЛОНИИР), sav01236@yandex.ru

СЛИВКОВ
Владимир Юрьевич — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slivkov.vova@gmail.com

СМОРОДИН
Геннадий Николаевич — кандидат технических наук, старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsmorodin@gmail.com

СОКОЛОВА
Ксения Вадимовна — студентка группы ИСТ-611м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sokolova.bonch@gmail.com

СОЛОВЬЕВ
Дмитрий Владимирович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, laos-82@yandex.ru

СОСНОВСКИХ
Александр Михайлович — аспирант, ассистент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sosnovskikh.am@yandex.ru

СТАРОСТИН
Владимир Сергеевич — кандидат физико-математических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, star_vs_47@mail.ru

СТЕПАНОВ
Антон Андреевич — магистрант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stepanovff.antoha@gmail.com

СТЕПАНОВ
Александр Петрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, stepetal94@mail.ru

СТРЕЛКОВ
Олег Валерьевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, mega.strelkov@mail.ru

СТРОКОВ
Артем Андреевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого, adimuciya7@gmail.com

СУВОРОВ
Антон Михайлович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tony-s-m@yandex.ru

СУЕТИН
Артём Игоревич — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, asuetin5@yandex.ru

СУРЖИКОВ
Илья Геннадьевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, sigrus09@gmail.com

ТАРАБАРОВ
Андрей Викторович — студент группы ИСМ-61з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antar94@bk.ru

ТАРАНОВ
Сергей Владимирович — ассистент, аспирант кафедры безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, serg.tvc@gmail.com

ТИРИДАТОВ
Сергей Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого, tiridatovsergei@bk.ru

ТКАЧЕНКО
Сергей Андреевич — инженер-исследователь лаборатории факультета безопасные информационные Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, i_krov@mail.ru

ТОПКАСОВ
Михаил Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, mr.topka@yandex.ru

ТРИФАНОВ
Максим Алексеевич — инженер-исследователь НОЦ «Технологии информационных и образовательных систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leimaxs@gmail.com

ТУЛЕУОВ
Берик Игликович — старший преподаватель кафедры математического и компьютерного моделирования Евразийского национального университета им. Л. Н. Гумилева, berik_t@yahoo.com

УСС
Владимир Станиславович — кандидат технических наук, начальник НОЦ «Технологии информационных и образовательных систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uss_w@mail.ru

УШАКОВ
Игорь Александрович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФЁДОРОВ
Никита Сергеевич — студент группы ИСТ-541 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nik1609@yandex.ru

ФЕДОРЧЕНКО
Андрей Владимирович — аспирант, младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, fedorchenko@comsec.spb.ru

ФЕДОСЕЕВ
Денис Олегович — заместитель начальника научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, 4s.bezdna@gmail.com

ФИАЛКИН
Илья Александрович — магистр Военной академии связи им. Маршала Советского Союза С. М. Буденного, nina_vlasova_79@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 — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frolkris988@gmail.com

ХАЙБРАХМАНОВА
Екатерина Сергеевна — студентка группы ИСТ-612м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, katusha.1994.10@mail.ru

ХВОСТОВ
Максим Алексеевич — студент группы ИСТ-541 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makshvostov@mail.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

ХОХЛАЧЕВА
Екатерина Андреевна
курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, vlasenko199@yandex.ru

ЦАНЯН
Артем Олегович
старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, jeArtem@ya.ru

ЦВЕТКОВ
Александр Юрьевич
старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧАУНИН
Михаил Павлович
кандидат физико-математических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikech1010@yandex.ru

ЧИСТЯКОВ
Андрей Сергеевич
магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chistgg@mail.ru

ЧИСТЯКОВ
Павел Николаевич
магистр кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, lightbringer1701@gmail.com

ШАДРИН
Дмитрий Михайлович
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, dm.shadrin@mail.ru

ШАЙСУЛТАНОВ
Максим Хамзеевич
старший оператор научной роты в Военной академии связи им. Маршала Советского Союза С. М. Буденного, maxim.shaysultanov@gmail.com

ШАМРОВ
Никита Владимирович
старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, nikitashamrov@gmail.com

ШЕРШНЁВ
Александр Сергеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, a.s.shershnev@yandex.ru

ШЕСТАКОВ
Александр Викторович — кандидат технических наук, старший научный сотрудник, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, alexandr.shestakov01@yandex.ru

ШИРЯЕВ
Василий Евгеньевич — капитан, начальник научно-исследовательской лаборатории Военной академии связи им. Маршала Советского Союза С. М. Будённого, vasily.s.e@yandex.ru

ШИРЯЕВ
Максим Евгеньевич — капитан, младший научный сотрудник НИО-5 НИЦ Военной академии связи им. Маршала Советского Союза С. М. Будённого, maksim.s.e@mail.ru

ШИРЯЕВ
Сергей Леонидович — студент Санкт-Петербургского государственного университета телекоммуникация им. проф. М.А. Бонч-Бруевича, shiryaev.sut@gmail.com

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

ШЛЯХОВ
Игорь Алексеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого, i-shlyakhov@mail.ru

ШУРАКОВА
Дарья Геннадьевна — курсант Санкт-Петербургского университета государственной противопожарной службы МЧС России, shurakova.darya@bk.ru

ЭЛЬ САБАЯР ШЕВЧЕНКО
Нидал — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nzs.vus@gmail.com

ЮРКИН
Дмитрий Валерьевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvyurkin@yandex.ru

ЯКОВЛЕВ
Сергей Викторович — магистраут кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, segaathlon@mail.ru

ЯКОВЛЕВА
Дарья Алексеевна — аспирант кафедры математики и моделирования Владивостокского государственного университета экономики и сервиса, darya.yakovleva15@vvsu.ru

ЯКУБОВА
Наиля Равильевна — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nel123@yandex.ru

АВТОРСКИЙ УКАЗАТЕЛЬ