

СПбГУТ)))

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

13th INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2023
Международная научно-техническая и научно-методическая конференция
«Актуальные проблемы инфотелекоммуникаций в науке и образовании»



АПИНО
ICAIT



2024

**СБОРНИК
НАУЧНЫХ СТАТЕЙ**

APINO.SUT.RU



ПАРТНЕРЫ



ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ



ИНФОРМАЦИОННАЯ ПОДДЕРЖКА



Научный журнал
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
И ТЕЛЕКОММУНИКАЦИИ
ijitt.ru

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. А. Брусиловского; сост. А. А. Нестеров. СПб. : СПбГУТ, 2024. Т. 2. 636 с.

ПРОГРАММНЫЙ КОМИТЕТ

Председатель

Киричек Р. В., доктор технических наук, доцент, ректор СПбГУТ (Россия)

Заместитель председателя

Брусиловский С. А., кандидат технических наук, проректор по научной работе СПбГУТ (Россия)

Ответственный секретарь

Нестеров А. А., начальник управления организации научной работы и подготовки научных кадров СПбГУТ (Россия)

Члены программного комитета

Yevgeni Koucheryavy, professor, Ph. D., Senior member IEEE, Department of Electronics and Communication Engineering Tampere University of Technology (Finland)

Ahmed A. Abd El-Latif, Ph. D., Prince Sultan University, head of "MEGANETLAB 6G", SPbSUT (Saudi Arabia)

Jong-Ho Lee, Ph. D. in Electrical Engineering, Vice President of Institute of Electronics Engineers of Korea (IEEK), ETRI (Korea)

Сеилов Ш. Ж., доктор экономических наук, академик Международной Академии Связи, декан факультета информационных технологий Евразийского национального университета имени Л.Н. Гумилева (Казахстан)

Каримов Б. Т., кандидат технических наук, доцент, директор Института электроники и телекоммуникаций, профессор кафедры инфокоммуникационных технологий Кыргызского государственного технического университета И. Разакова (Кыргызстан)

Фёдоров С. Л., кандидат технических наук, доцент, декан факультета радиотехнологий связи СПбГУТ (Россия)

Окунева Д. В., кандидат технических наук, Проректор по проектной деятельности, доцент кафедры программной инженерии и вычислительной техники (Россия)

Зикратов И. А., доктор технических наук, профессор, декан факультета информационных систем и технологий СПбГУТ (Россия)

Владыко А. Г., кандидат технических наук, доцент, декан факультета фундаментальной подготовки СПбГУТ (Россия)

Сотников А. Д., доктор технических наук, доцент, декан факультета цифровой экономики, управления и бизнес-информатики СПбГУТ (Россия)

Шутман Д. В., кандидат политических наук, доцент, декан гуманитарного факультета СПбГУТ (Россия)

Гири В. А., полковник, начальник военного учебного центра СПбГУТ (Россия)

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ СПбГУТ, Россия

Председатель

Абилов А. В., первый проректор – проректор по учебной работе

Заместитель председателя

Журавлева Н. Н., проректор по молодежной политике и международному сотрудничеству

Ответственный секретарь

Аникевич Е. А., кандидат технических наук, начальник отдела организации научно-исследовательской работы и интеллектуальной собственности

Члены организационного комитета

Ивасишин С. И., директор департамента организации и качества образовательной деятельности

Эмексузян А. Р., директор департамента экономики и финансов

Григорян Г. Т., начальник управления маркетинга и рекламы

Зыкова Н. В., начальник управления информационно-образовательных ресурсов

Казаков Д. Б., начальник управления информатизации

Гаврилова А. Н., главный специалист группы планирования научных исследований и аналитики

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

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

Научное издание

Литературное редактирование,
корректурa И. М. Татарникова

Оформление Г. И. Юрьев

Верстка М. О. Мотыгина, А. А. Шер, Д. Н. Яшугин

Подписано в печать 14.06.2024.

Вышло в свет 28.06.2024. Формат 60×90 1/8.

Усл. печ. л. 39,75. Заказ № 111-ИТТ-2024.

пр. Большевиков, д. 22, корп. 1.

Россия, Санкт-Петербург, 193232

СОДЕРЖАНИЕ

Информационные системы и технологии	5	Information Technology and Telecommunications
Аннотации	592	Annotations
Авторы статей	621	Authors of Articles
Авторский указатель	633	The Author's Index

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.418
ГРНТИ 50.43.19

ЦЕНТРАЛИЗОВАННЫЙ КЛАССИФИКАТОР ДАННЫХ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ НОРМАТИВНО- СПРАВОЧНОЙ ИНФОРМАЦИИ ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

**Г. Н. Абсагтаров, М. Д. Абылхасенов, А. А. Бурлаков,
Д. М. Шакербеков**

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

В статье рассматриваются вопросы построения и ведения централизованного классификатора данных как инструмента централизованного обеспечения нормативно-справочной информации прикладных информационных систем. Применение технологии на существующей автоматизированной системе управления позволит сократить затраты на техническую эксплуатацию за счет использования потенциала, централизованного ведения нормативно-справочной информации информационных систем.

централизованный классификатор, информационные системы, эксплуатационные данные

В силу территориальной удалённости подразделений Вооруженных Сил Республики Казахстан и прикладных информационных систем этих подразделений необходимо обеспечить обновления таблиц нормативно справочной информации (НСИ), которые в дальнейшем подлежат передаче в централизованное управление.

Автоматизированная система управления данными (АСУД) представляется, как распределённая система, имеющая центральный и периферийный уровни [1]. Центральный уровень представлен ядром системы (сервер АСУД, сервером приложений, автоматизированными рабочими местами Административного персонала АСУД), устанавливаемыми в ведомствах

Республики Казахстан. Периферийный уровень – автоматизированными рабочими местами пользователей – администраторов прикладных информационных систем, как центрального аппарата, так и периферийных подразделений.

Структура построения АСУД обуславливает реализацию следующих решений по организационной структуре управления объектами автоматизации:

- основной объем работ по актуализации НСИ выполняется на центральном уровне системы;

- распределение работ на центральном уровне (по централизованному ведению таблиц НСИ) между административным персоналом выполняется по предложенным вариантам:

- 1) модификацию данных таблиц НСИ, переданных в централизованное ведение, в БД АСУД выполняет только административный персонал центрального уровня [2]. Персонал периферийного уровня, обеспечивает и отслеживает репликацию данных рабочих таблиц НСИ прикладных информационных систем соответствующих периферийных подразделений;

- 2) модификацию данных таблиц НСИ совместно выполняет персонал центрального и периферийного уровней в соответствии с заданной схемой распределения групп подведомственных таблиц. Персонал периферийного уровня также обеспечивает и отслеживает репликацию данных рабочих таблиц НСИ прикладных информационных систем соответствующих периферийных подразделений;

- 3) модификацию данных таблиц НСИ выполняет персонал только периферийного уровня в соответствии с заданной схемой распределения групп подведомственных таблиц. Персонал периферийного уровня также обеспечивает и отслеживает репликацию данных рабочих таблиц НСИ прикладных информационных систем соответствующих периферийных подразделений. Персонал центрального уровня обеспечивает ведение и модификацию сопутствующей информации (ввод подразделений, пользователей и распределение прав доступа пользователей к АСУД, ввод прикладных информационных систем, сущностей, таблиц НСИ прикладных информационных систем, маппировка таблиц на сущности, первичный ввод данных таблиц НСИ и пр.)

Любой из указанных вариантов может быть реализован с использованием механизма назначения администратором Системы (администратором безопасности АСУД) полномочий группам пользователей к операциям с программно-информационными компонентами АСУД.

Под объектами, при управлении которыми используется комплекс задач АСУД, понимаются прикладные информационные системы ведомств

РК и его подразделений, справочники НСИ которых (хранящиеся в промышленных БД реляционного типа) целесообразно передать в централизованное ведение ЦКД АСУД.

Целесообразность передачи того или иного справочника (таблицы НСИ) прикладной информационной системы в централизованное управление определяется:

- фактом использования аналогичного справочника, информационные компоненты которого имеют идентичный технологический смысл, в другой информационной системе;

- фактом автономного использования и ведения справочника данной информационной системы различными подразделениями предприятия.

В настоящее время в РК эксплуатируются или находятся на стадии внедрения разнообразные информационные системы, имеющие автономные базы данных и самостоятельные системы ведения и обновления НСИ

Локальная централизация ведения НСИ в различных информационных системах не может в полной мере обеспечить решение задачи глобального централизованного ведения НСИ на уровне ведомств РК и его подразделений в целом, поскольку не обеспечивает централизацию для разноименных прикладных информационных систем.

В рамках АСУД предусмотрена возможность наращивания списка обслуживаемых АСУД внешних информационных систем[2], появление которых возможно в будущем, и таблиц НСИ этих систем, передаваемых в централизованное ведение.

АСУД обеспечит: хранение централизованной НСИ в единой базе данных; доставку измененных данных этих таблиц прикладным информационным системам, передавшим свои таблицы НСИ для централизованного их ведения. Под «централизованной» НСИ понимают ту часть совокупной НСИ, которую составляют базовые классификаторы, а также совместно используемую НСИ для прикладных информационных систем, таблицы НСИ которых ведутся в АСУД.

На рисунке 1 приведена принятая в АСУД схема установления соответствия между объектами НСИ (таблицами и полями таблиц) прикладных информационных систем и объектами НСИ (таблицами и полями таблиц) АСИД.

Информационное наполнение АСУД предназначено для использования во всех внешних информационных системах, передавших свои таблицы НСИ в централизованное ведение, работающих в корпоративной сети на новых и существующих программно-технических комплексах.

Система обеспечит поддержание целостности информации справочников за счет использования следующих мер:

- для поддержания ссылочной целостности данных использован механизм создания внешних ключей на уровне таблиц базы данных;

- для поддержания согласованного набора операций над несколькими таблицами (записями) использован механизм транзакций и все изменения в базе, выполняемые в рамках одной бизнес-процедуры, выполняются в рамках одной транзакции;
- для исключения дублирования применяется механизм уникальных индексов по соответствующим полям.

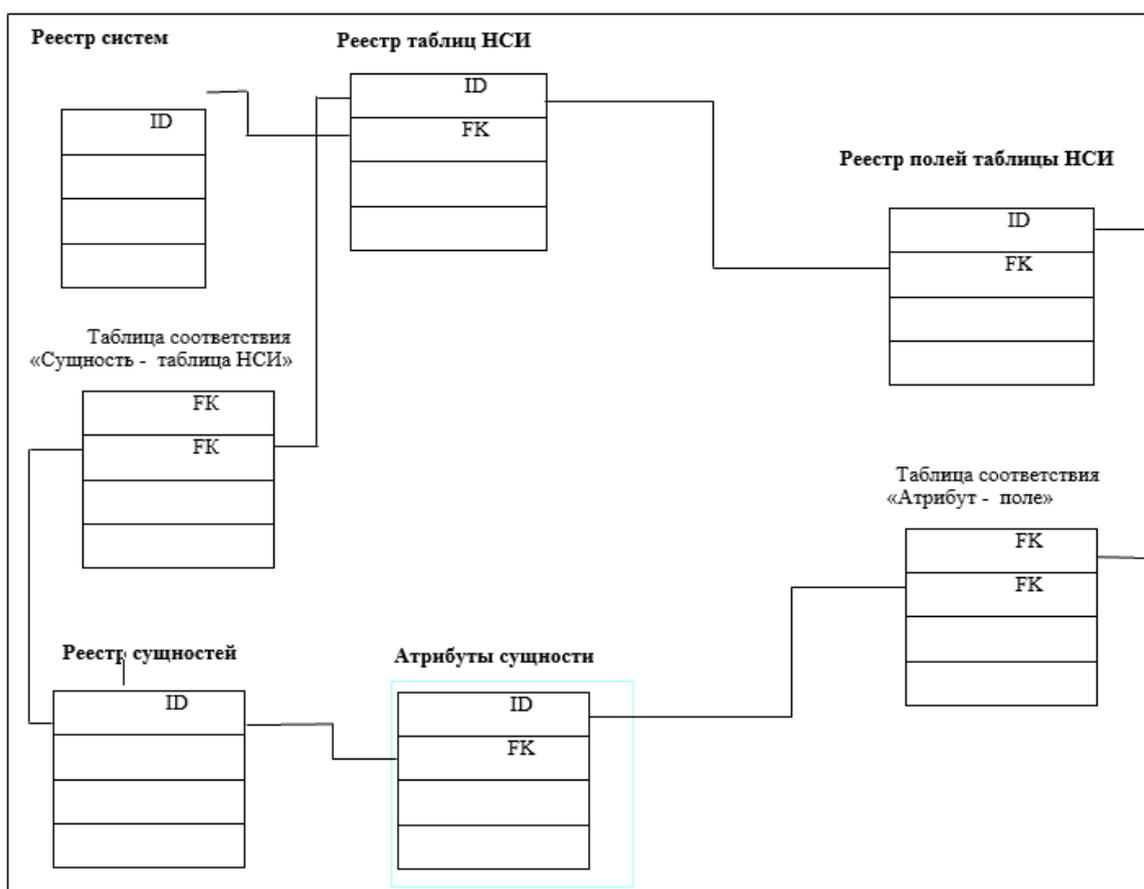


Рис. 1. Схема установления соответствия между объектами НСИ

Используемая платформа должна иметь встроенные средства проверки собственной целостности. Система обнаруживает факт отсутствия, повреждения или злонамеренной модификации собственных файлов. В случае обнаружения подобного случая Система не запускается, при этом в лог записывается причина неудачного запуска, позволяющая определить причину сбоя. Во время процедуры выборочного обновления текущая версия обновляемого модуля архивируется средствами платформы для того, чтобы при установке сбойного модуля имелась возможность отката на работоспособную версию.

Любая модификация компонент любого справочника (таблицы НСИ АСУД), исключая процедуры автоматической первичной загрузки данных справочника из электронного источника, предваряется формированием в БД

АСУД документа – основания модификации и заканчивается закрытием и утверждением пакета исходящих изменений, выполненных в соответствие с документом – основанием. Процедуру закрытия сессии изменений производит администратор, открывший данную сессию (т. е. осуществивший ввод документа – основания). Процедуру подписания пакета произведенных изменений осуществляет администратор, наделенный соответствующим правом.

Формирование информационных компонент для репликации изменений в таблицах НСИ внешних информационных систем, формирование таблиц истории изменений записей модифицируемых таблиц НСИ АСУД производится после утверждения пакета изменений. Процедура репликации данных в таблицах НСИ внешних информационных систем производится с учетом регламента репликаций для каждой из этих таблиц.

Запуск программных компонент, обеспечивающих выполнение вышеуказанных требований при работе с таблицами НСИ АСУД, осуществляется как из главного меню приложения (АРМ) пользователя – администратора АСУД, права которого позволяют работать с указанными программными компонентами, так и из интерфейсных форм, обеспечивающих реализацию процедур ведения таблиц НСИ.

Целостность данных справочников АСУД обеспечена поддержкой процедур создания внешних ключей на уровне таблиц БД, уникальных индексов по соответствующим полям, применением механизма транзакций, обеспечивающего выполнение бизнес – процедуры по изменению данных справочника закрытой и утвержденной сессии изменений в рамках одной транзакции.

Обмен с прикладными информационными системами, передавшими свои справочники в централизованное ведение АСУД, осуществляется с использованием строго регламентированных форматов. Экспорт данных в том или ином формате (XML, XLS и пр.) [3] определяется возможностью прикладной информационной системы вести прием данных в одном из этих форматов.

Список используемых источников

1. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
2. Михайличенко Н. В. Сравнительный анализ технологий построения региональных центров обработки данных // Юбилейная XV-ая Санкт-Петербургская международная конференция «Региональная информатика 2016». СПб.: СПОИСУ, 2016. С. 102–103.
3. Теория и практика построения автоматизированных систем информационной и вычислительной поддержки процессов планирования связи на основе новых информационных технологий. СПб., 1998.

УДК 004.021
ГРНТИ 81.93.29

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА АВТОМАТИЗИРОВАННОГО АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

А. В. Аверьянов, Е. П. Долгов

Академия Федеральной Службы Охрпны России

В современном мире защита информации становится все более актуальной. С развитием цифровых технологий увеличивается количество угроз, связанных с нарушением конфиденциальности, целостности и доступности данных. Особое внимание уделяется защите информационных систем государственных учреждений, так как они являются объектами повышенного интереса для злоумышленников, способных нанести серьезный ущерб национальной безопасности. В статье рассматривается актуальность создания программного комплекса для всестороннего анализа защищенности сетевой инфраструктуры, выявления возможных уязвимостей и разработки рекомендаций по их устранению, повышая тем самым общий уровень ИБ.

тестирование на проникновение, анализ защищенности, информационная безопасность

В настоящее время необходимо постоянно поддерживать следующие свойства информации: доступность, целостность и конфиденциальность. Однако с каждым годом обезопасить их становится все труднее, поскольку растет число кибератак на государственные и частные организации, что подтверждается отчетом компании «Positive Technologies». На рис. 1 представлена сравнительная статистика кибератак по кварталам за 2022 и 2023 года [1].

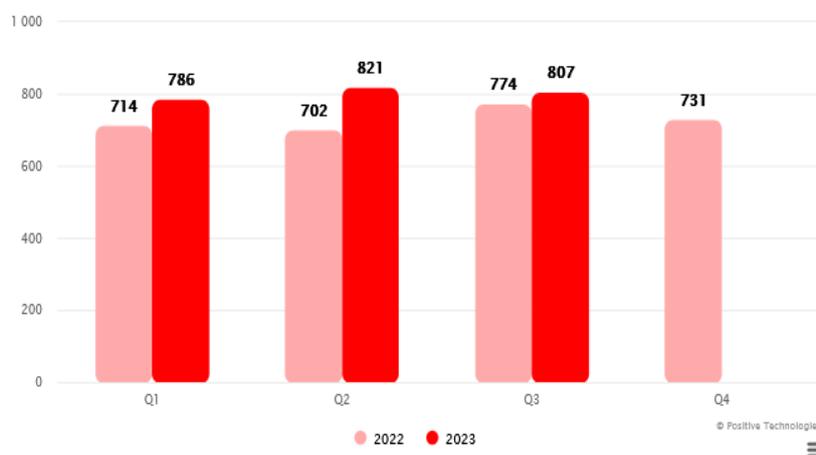


Рис. 1. Количество инцидентов в 2022 и 2023 годах (по кварталам)

На рис. 2 представлена статистика по категориям субъектов атак. Как можно заметить, кибератакам наиболее подвержены государственные и медицинские учреждения, финансовые организации и промышленность.

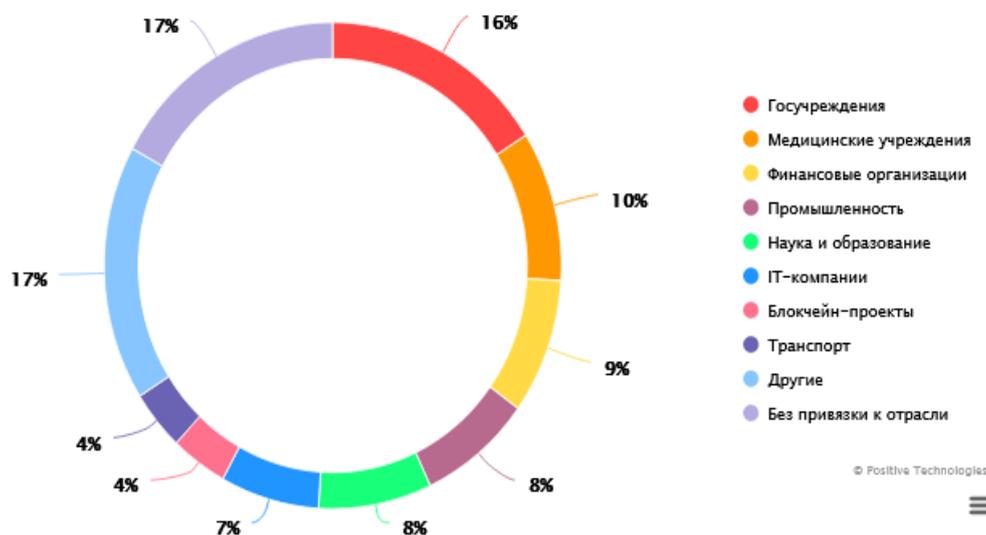


Рисунок 10. Категории жертв среди организаций

Рис. 2. Статистика по категории субъектов атак

Существует два основных типа тестирования информационных систем (ИС) на проникновение [2].

Первый – внутреннее тестирование (представлено на рис. 3). Оно проводится от лица сотрудника организации, имеющего стандартные права. При таком методе тестирования предполагается, что у специалиста есть знания о системе. Эти данные он может получить от организации, для которой проводит тестирование. Тестирование проводится с учетом этих знаний. Помогает имитировать атаки от людей, которые смогли получить часть информации о продукте.

Второй тип – внешнее тестирование (представлено на рис. 3). Оно позволяет определить, можно ли получить доступ к системе «со стороны», то есть от лица человека, никак не связанного с организацией. В данном случае у специалиста нет данных о тестируемой системе, он ведет себя как злоумышленник, который впервые столкнулся с системой. У него имеются лишь данные, которые находятся в открытом доступе. Данная методика используется большей частью реальными злоумышленниками.

В международной практике проведение тестов на проникновение регламентируется стандартами и методиками, которые регламентируют этапы тестирования, порядок испытаний тестируемых объектов, порядок взаимодействия аудитора с заказчиком и т. д.

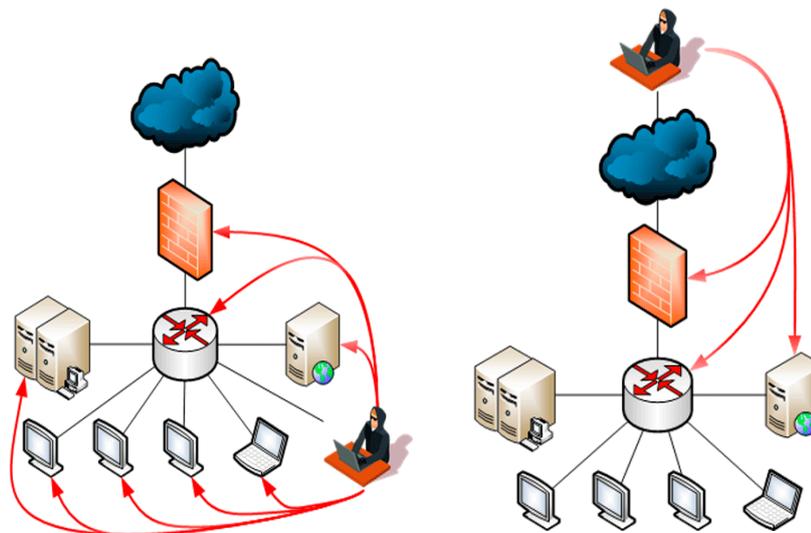


Рис. 3. Схемы реализации внутреннего (слева) и внешнего (справа) тестирования

К широко распространенным зарубежным стандартам и методикам относятся:

– методика OSSTMM – The Open Source Security Testing Methodology Manual. Разработана институтом Institute for Security and open Methodologies, который является открытым сообществом ученых и практиков в области информационной безопасности (ИБ). Данная методика является хорошо структурированным документом, который регламентирует практически все особенности и этапы тестирования на проникновение, ориентирована в большей степени на тестирование компьютерных сетей;

– методика ISSAF – Information System Security Assessment Framework. Разработана консорциумом Open Information Systems Security Group в качестве стандарта внутреннего аудита организаций этого консорциума. С помощью данной методики имеется возможность оценки политик и процедур ИБ организации, а также степень их соответствия ИТ-стандартам и требованиям нормативных документов в области ИБ;

– методика OWASP – Open Web Application Security Project. Создана сообществом OWASP в 2004 г. и развивается по настоящее время международной группой независимых экспертов-энтузиастов. Методика ориентирована на тестирование веб-приложений;

– стандарт NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment. Разработан и поддерживается в актуальном состоянии одним из подразделений национального института стандартизации США National Institute of Standards and Technology (NIST). Данный стандарт в отличие от предыдущих методик также можно использовать как шаблон для разработки – какие стандартные функции обеспечения ИБ должны присутствовать в разрабатываемом объекте;

– методика PTF – Penetration Testing Framework. Является детальным техническим руководством по проведению тестирования на проникновение в технической части. Данное руководство не содержит общетеоретической информации, подобно методикам OSSTMM или ISSAF, однако предоставляет практически исчерпывающий перечень уязвимостей объекта подлежащих проверке, в некоторых случаях, с указанием рекомендуемой порядка проведения тестирования и инструментария для него.

К наиболее проработанным, среди оригинальных отечественных методик тестирования на проникновение, относится методика от Positive Technologies. Данная методика разработана одной из ведущих российских компаний в области ИБ. Компания специализируется на комплексном аудите ИБ, оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга ИБ.

Средства тестирования на проникновение – это программное обеспечение (ПО), позволяющее проводить анализ защищенности информационных систем, заключающийся в выполнении имитации атаки на систему с целью оценки ее безопасности. Средства тестирования на проникновение используются для поиска слабых мест в ИС, которые позволяют злоумышленнику получить доступ к информационным ресурсам и техническим средствам.

Выделяют следующие виды ПО, используемые для тестирования: [3].

– Kali Linux является лидером среди инструментов тестирования систем на проникновение, имеющим в себе множество различных дистрибутивов для этой цели;

– BackTrack Linux – это дистрибутив Linux, который включает в себя множество инструментов для анализа и тестирования ИБ компании;

– Metasploit – фреймворк для проведения тестирования на проникновение, содержащий в себе как эксплойты, так и специализированные модули;

– Nmap – программа для сканирования сетей с любым количеством пользователей. Она показывает, в каком состоянии находятся объекты сети, дает о них информацию и облегчает дальнейшую атаку. Можно встретить название zenmap – так называется графический интерфейс для Nmap;

– Nessus – программа, которая автоматически ищет уязвимости в системах и сетях. Нужна для поиска распространенных слабых мест. Имеет базу, которая обновляется каждую неделю, поэтому программа почти всегда актуальна;

– Wireshark – программа, которая анализирует трафик в сети. Она знает, как устроены пакеты, которые передаются по разным сетевым протоколам, может «разобрать» их на составляющие и прочитать из них информацию;

- Aircrack-ng – набор утилит для тестирования безопасности беспроводных сетей;
- MaxPtrof. Позволяет получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений;
- Core Impact – продукт для тестирования несанкционированных проникновений в систему, с ее помощью можно оценить ИБ компании таким же образом, как и злоумышленник.

Для более качественного анализа защищенности ИС необходимо разработать многофункциональный инструментарий, позволяющий осуществлять поиск и обнаружение уязвимостей. Учитывая сложность и особенности функционирования ИС, предлагается разработать модульное программное средство, позволяющее проводить анализ защищенности системы.

Структурная схема разрабатываемого средства представлена на рис. 4.

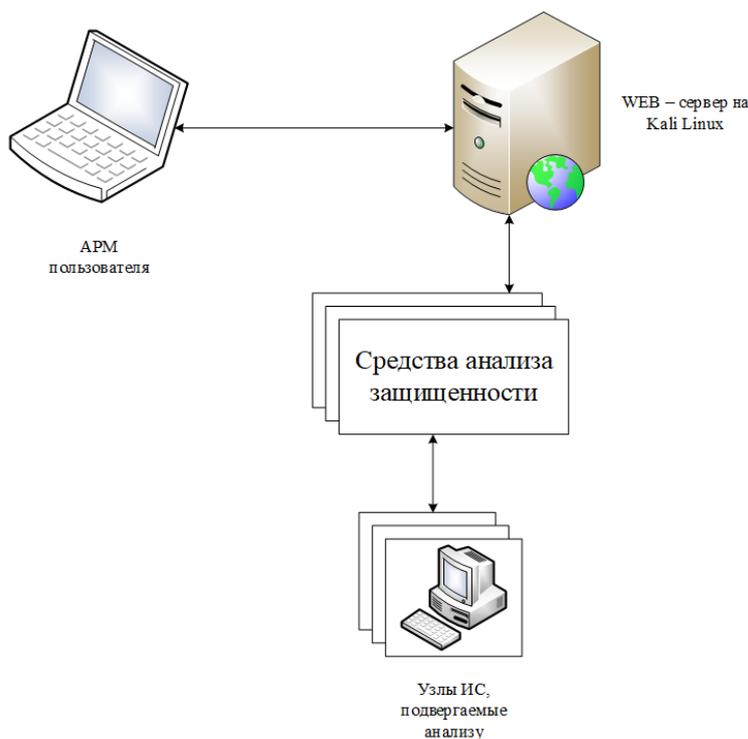


Рис. 4. Схема стенда программного комплекса автоматизированного анализа защищенности

В данный программный комплекс автоматизированного анализа защищенности включены следующие средства тестирования: операционная система Kali Linux, средства тестирования NMap, Wariti, OpenVas, Nessus, так как данные средства позволяют получить наиболее подробную информацию при проведении соответствующих мероприятий по анализу защищенности.

В заключении отмечается, что при проведении испытаний были достигнуты конкретный результаты. Была повышена оперативность проведения анализа защищенности путем автоматической выработки отчета по результатам тестирования. Также отмечается удобство использования данного программного комплекса.

Список используемых источников

1. Актуальные киберугрозы: III квартал 2023 года / Positive Technologies. Электрон. текстовые дан. <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3> (дата обращения: 21.03.2024)
2. Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с англ. В.С. Яценкова. М.: ДМК Пресс, 2021. 310 с.: ил.
3. Макаренко С. И., Смирнов Г. Е Анализ стандартов и методик тестирования на проникновение // Научно-техническая информация. 2020. 29 с.

УДК 004.414.23
ГРНТИ 50.41.25

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ НЕЙРОННЫХ СЕТЕЙ

В. С. Авраменко, Е. С. Чичков

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

Предложен способ экспериментальной оценки эффективности вариантов реализации различных архитектур нейронных сетей на основе программного комплекса, обеспечивающего одинаковые исходные данные и условия для тестирования оцениваемых нейросетей. Представлены структура и описание работы программного комплекса, показатели эффективности нейронных сетей.

нейронная сеть, программный комплекс, показатель, оценка, эффективность точность, ресурсоемкость, оперативность

В настоящее время существенно ускорился прогресс в области технологий искусственного интеллекта (ИИ). Особенно активно в различных сферах деятельности внедряются технологии машинного обучения, в том числе и на основе искусственных нейронных сетей. Самостоятельная разработка и производство различного рода систем на основе нейронных сетей является приоритетным направлением развития в ведущих странах. В связи с этим актуализировалась задача оценки эффективности систем искусственного интеллекта (СИИ) на основе нейросетей.

В общем случае в зависимости от исходных данных и реализуемых СИИ функций возможно несколько типовых вариантов постановок задач на создание (выбор) средств математического, программного и аппаратного обеспечения СИИ на основе методов машинного обучения, в том числе и на основе нейронных сетей.

Первый вариант постановки задачи возникает в случае необходимости разработки СИИ «с нуля», то есть когда целью является разработка (выбор) математического, программного и аппаратного обеспечения СИИ при заданных требованиях по точности, оперативности и ресурсоемкости.

Также может быть поставлена задача разработки (выбора) математического и программного обеспечения для заданных или уже имеющихся в составе системы аппаратных средств. Решением задачи является программная реализация разработанной или выбранной оптимальной или рациональной нейросети.

Третий вариант обусловлен необходимостью выбора оптимальных или рациональных аппаратных средств (процессоры общего назначения, графи-

ческие карты, нейропроцессоры и т.д.) при заданном (уже имеющемся) математическом обеспечении (заданной структуре и параметрах нейросети) и программном обеспечении.

Для решения этих задач необходимо оценивать эффективность различных вариантов реализации СИИ на всех этапах ее создания. Но в настоящее время еще не до конца сформировался общепринятый подход к оценке СИИ на основе нейросетей [1]. Поэтому приходится доверять оценкам нейросетей, заявленными их разработчиками, или самостоятельно проводить оценивание отдельных показателей по собственным методикам [2]. При этом не всегда учитываются требования к оценке СИИ, как программного средства [3].

Вышеуказанные факторы в первую очередь негативно влияют на точность оценивания, что может привести к неправильным решениям по программно-аппаратной архитектуре СИИ. Также в настоящее время актуальна проблема оперативности оценивания, обусловленная необходимостью разработки СИИ специального назначения в условиях ограниченного временного ресурса на детальное теоретическое и экспериментальное исследование качества или эффективности.

Таким образом, сложилась проблемная ситуация, обусловленная несоответствием сложившихся на практике подходов к оцениванию эффективности нейросетей (СИИ на их основе) современным требованиям по точности и оперативности. Особенно остро она проявляется при решении задачи сравнительной оценки эффективности различных реализаций нейросетей для решения конкретной задачи.

Одним из путей решения данной проблемы является создание единой технологической среды для экспериментального оценивания эффективности нейросетей на основе программного комплекса, обеспечивающего автоматизацию трудоемких и сложных этапов оценивания.

Под единой технологической средой оценивания понимается единая система показателей эффективности и процедур измерения, расчета и оценивания, одинаковые наборы данных (датасеты) для обучения нейросетей, одинаковые наборы реальных данных для тестирования.

Структура программного комплекса представлен на рис.1. Основные элементы программного комплекса следующие: виртуальные машины (ВМ) для имитации определенной программно-аппаратной платформы для нейронной сети (НС); генератор датасетов (ДС) – наборов данных, предназначенных для обучения НС; датасеты; набор неразмеченных реальных данных (ДСрд), предназначенных для испытания НС; база данных результатов работы НС (БДрез); программный модуль оценки эффективности (ПМОЭ), предназначенный для расчета значений и оценки частных и обобщенных показателей эффективности НС ($Y_{рез}$ – показатель результативности, $Y_{рес}$ – показатель ресурсоемкости, $Y_{оп}$ – показатель оперативности).

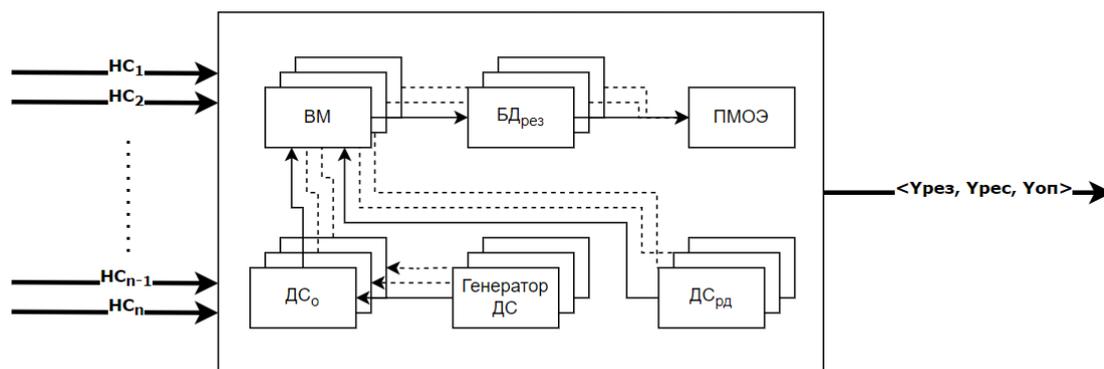


Рис.1. Структура программного комплекса для экспериментальной оценки эффективности нейронных сетей

На вход программного комплекса подаются исследуемые нейронные сети различной архитектуры и конфигурации. При необходимости осуществляется генерация датасетов и обучение НС. Далее для измерения характеристик сети, необходимых для расчета значений показателей результативности, ресурсоемкости и оперативности, на вход исследуемых НС подаются наборы реальных данных. Все результаты испытаний фиксируются в базе данных результатов, на их основе в модуле оценки эффективности рассчитываются значения частных и обобщённых показателей эффективности.

Основные свойства и некоторые частные показатели эффективности НС (СИИ на основе НС) приведены в таблице 1.

ТАБЛИЦА 1. Свойства и показатели эффективности нейронных сетей

Эффективность НС		
Результативность	Оперативность	Ресурсоемкость
Accuracy («Точность») – доля правильных ответов НС. Loss – точность нейронной сети по показателям отклонения. Precision – доля правильных ответов модели в пределах класса. Recall («Полнота») – доля истинно положительных классификаций.	Время получения результата. Время обучения. Время генерации датасета.	Количество вычислительных операций. Загрузка процессора. Объем занимаемой оперативной памяти. Объем занимаемой постоянной памяти.

В некоторых случаях для оценки НС может быть использован комплексный показатель эффективности $Y_{эф}$ НС, определяемый как отношение результата к затратам на его получение:

$$Y_{эф} = \frac{Y_{рез}}{Y_{рес}}$$

Особенно актуальна задача сравнительного анализа эффективности НС при разработке малогабаритных мобильных систем, самостоятельно обрабатывающих данные [4]. В частности, многие беспилотные летательные аппараты (БПЛА) используют компьютерное зрение для обнаружения и распознавания объектов различного рода. Вместе с тем реализация обработки данных на борту БПЛА во многих задачах требует вычислительного устройства достаточно высокой производительности. Для малогабаритных БПЛА эта задача является проблемной, так как ее решение путем использования мощных высокопроизводительных процессоров с соответствующим энергоснабжением влечет за собой увеличение массогабаритных характеристик, при этом для сохранения требуемых полетных характеристик (скорость, высота, продолжительность полета) может потребоваться модернизация или замена двигателей и других конструктивных элементов. Соответственно, возникает необходимость использования в малогабаритных БПЛА компактных вычислителей и соответствующих средств математического, информационного и программного обеспечения, обеспечивающих обработку данных с требуемыми значениями показателей результативности и оперативности и минимальными вычислительными затратами, что, в свою очередь, требует оценивания эффективности вариантов решения данной задачи.

Таким образом, применение единой технологической среды оценивания на основе предлагаемого программного комплекса позволит существенно повысить точность и оперативность оценивания эффективности программных и программно-аппаратных реализаций нейросетей различных архитектур за счет автоматизации процесса оценивания, обеспечения одинаковых условий, исходных данных и процедур измерения и оценивания.

Список используемых источников

1. Щербин А. С. Проблемы оценки качества архитектур нейронных сетей и алгоритмов поиска архитектур // Вестник НГУ. Серия: Информационные технологии. 2023. № 21(2). С. 51–62.
2. Маликов А. В., Авраменко В. С. Оценка достоверности диагностирования компьютерных инцидентов в инфокоммуникационных системах // Труды V межвузовской научно-практической конференции: Проблемы технического обеспечения войск в современных условиях. 2020. С. 189–193.
3. Ковалев И. С., Паращук И. Б., Смирнов А. А. Анализ основных характеристик качества программного обеспечения для управления современными инфокоммуникационными сетями // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. С. 645–649.
4. Авраменко В. С., Чичков Е. С. Применение сверточных нейронных сетей для распознавания объектов беспилотными летательными аппаратами // Региональная информатика и информационная безопасность. Сборник трудов. СПб.: СПОИСУ, 2023. Выпуск 12. С. 94–98.

УДК 681.5:681.586
ГРНТИ 55.30.31

РАЗРАБОТКА ПО СБОРУ МОБИЛЬНЫМ РОБОТОМ ROBO-RICA ИНФОРМАЦИИ ОБ ОБЪЕКТАХ НА ОГРАНИЧЕННОЙ ПЛОЩАДИ

Н. Р. Агафонов, Г. В. Возгрин, П. А. Волынкин

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

Представлено программное обеспечение для робототехнической платформы ROBO-RICA, позволяющее мобильному роботу сканировать площадку ограниченных размеров на предмет обнаружения на ней объектов 5x5 см. Робот движется по заданной контрастной линии траектории. При обнаружении объекта при помощи датчика расстояния робот сигнализирует об этом звуковым сигналом, объезжает препятствие и сохраняет в памяти местоположение обнаруженного объекта. После завершения сканирования поверхности робот повторно проходит дистанцию, но уже при отсутствии объектов. В местах бывшего расположения объектов робот звуковым сигналом дает понять, что ранее на этом месте находился объект.

мобильные роботы, алгоритмы сканирования площади, решение аппаратных проблем

Использование мобильных робототехнических устройств имеет довольно широкий спектр применений. Одной из задач, которые могут решаться подобными роботами является задача по сбору информации о наличии на определенной площади тех или иных объектов. Для тестирования алгоритма решения этой задачи был использован мобильный робот из комплекта ROBO-RICA [1]. Предполагается поручить роботу просканировать всю площадку заданных размеров, запомнить расположение обнаруженных объектов и при повторном прохождении по площадке сигнализировать звуком в тех местах, где ранее были обнаружены объекты и на мониторе отображать номер объекта.

Набор мобильного робота ROBO-RICA включает в себя: монтажную плату с набором винтов и гаек, а также крепежных пластин; пару гусениц, блок двигателя с редуктором и плату управления (рис. 1). Для программирования робота используется отдельная плата USB-программатора. Роль микроконтроллера выполняет микросхема PIC16F887 с перепрограммируемым запоминающим устройством с объемом памяти 14 Кбайт. Одним из главных достоинств данного набора является наличие 8 программируемых портов ввода/вывода с возможностью передачи как аналогового (только вход), так и цифрового (вход и выход) сигналов. Это позволяет использовать довольно обширный набор датчиков для выполнения различных задач. Для данной задачи были использованы датчики: инфракрасный измеритель расстояния GP2D120, инфракрасный отражатель ZX-03 (для измерения уровня

освещенности/восприятия яркости поверхности), инфракрасный пульт ДУ ER-4 и приемник ZX-IRM. Данные датчики идут в наборе с роботом.

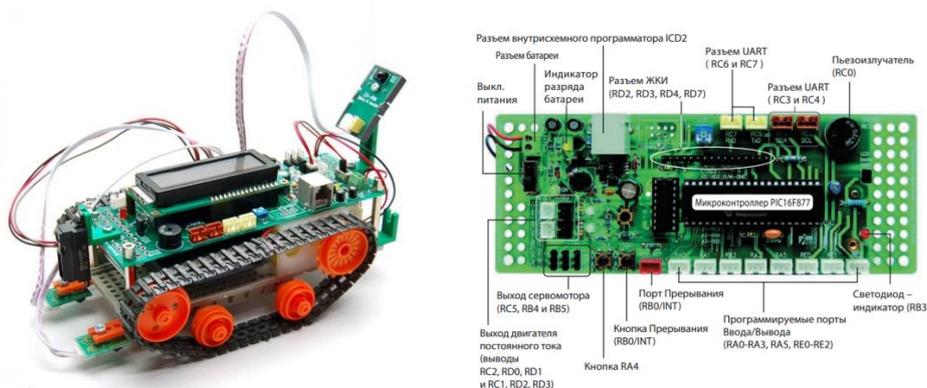


Рис. 1. Мобильный робот ROBO-PICA и плата управления роботом

Управляющая программа может быть написана на языках Ассемблер, BASIC или C. Для программ на последних двух языках необходимо использование компилятора. Программа в данной работе была написана на языке C, с использованием компилятора mikroC. Достоинствами среды разработки mikroC является удобная графическая оболочка с обширным инструментарием для отладки: отслеживание структуры программы, переменных и функций, «бесшовное» встраивание ассемблерного кода, а также получение графиков статистики программного кода и дерева вызовов процедур [2].

Основой решения задачи является выбор оптимального маршрута прохождения и, соответственно, способа сканирования обозначенной площади. Его выбор определяет скорость и точность выполнения, а также сложность написания программы.

Для решения задачи были рассмотрены 2 варианта прохождения и сканирования площадки, которые на этапе анализа были названы соответственно: «поиск сканированием» и «поиск прохождением» (рис. 2).

Первый из них предполагает сканирование всей площади круговыми движениями робота с «опорных точек». После сканирования робот должен напрямую двигаться к прошлым местам расположения объектов. Этот способ обеспечивает полноценное сканирование площадки и быстрое воспроизведение положения объектов, при втором запуске.

Недостатки первого метода:

- более высокая сложность масштабирования;
- требуется большой объем памяти (программных слов) для математических операций и вычислений;
- требуются более точные движения робота;
- сложное программное исполнение;
- не проверено на практике: возможно требует большего времени выполнения, из-за большого количества остановок на этапе «сканирования».

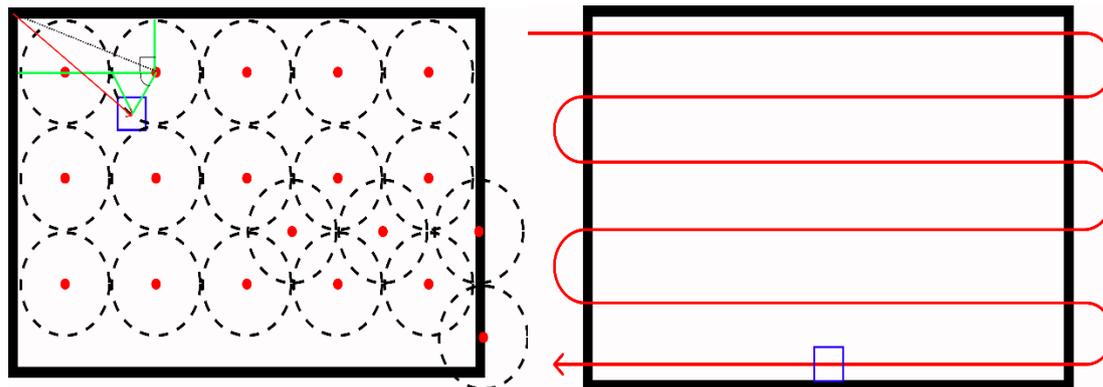


Рис. 2. Два варианта решения задачи

Суть второго варианта состоит в проезде площадки по прямым линиям и обнаружению объектов, при практически непосредственном контакте с ними. При повторном запуске робот проезжает по тому же пути, воспроизводя предыдущее местоположение препятствий. Данный способ намного легче в программном исполнении, однако он имеет более долгий этап “воспроизведения”. Также оба алгоритма обладают своими проблемами, вызванными аппаратными недостатками.

По итогам сравнения, для реализации был выбран второй способ. Главной проблемой, при написании программы, оказался поиск способа “запоминания” расположения объектов.

Решение было найдено, в виде создания условной системы координат [линия; время]. Робот проходит по полю какое-то количество линий n (в зависимости от масштаба площадки), что является аналогом координаты по оси ординат. При прохождении площадки происходит отсчёт времени движения по каждой n -ой линии t – аналог координаты по оси абсцисс (Рис.3).

При обнаружении объекта происходит остановка робота и запись в два массива текущего номера и времени. Во время повторного проезда происходит постоянное сравнение текущих значений номера линии и времени, при их совпадении с записанными в массивах значениями, робот останавливается и выводит на экран порядковый номер обнаруженного объекта.

Во время выполнения задания был обнаружен ряд аппаратных проблем, потребовавший внесения корректировок в программу и значительно увеличивший время решения.

Необходимость корректировки работы датчиков

При изменении внешних условий работы робота (уровень освещенности, смена покрытия) возникает необходимость корректировать пороги срабатывания датчиков. Так, при проведении эксперимента в помещении с освещенностью, отличной от той, в которой происходила его настройка, датчики освещенности могут среагировать на светлом покрытии, что приведёт к развороту робота раньше, чем это необходимо, либо же, в некоторых

случаях, заикливанию его работы на процедуре разворота (она происходит при обнаружении датчиком освещенности черной линии – границы площади).

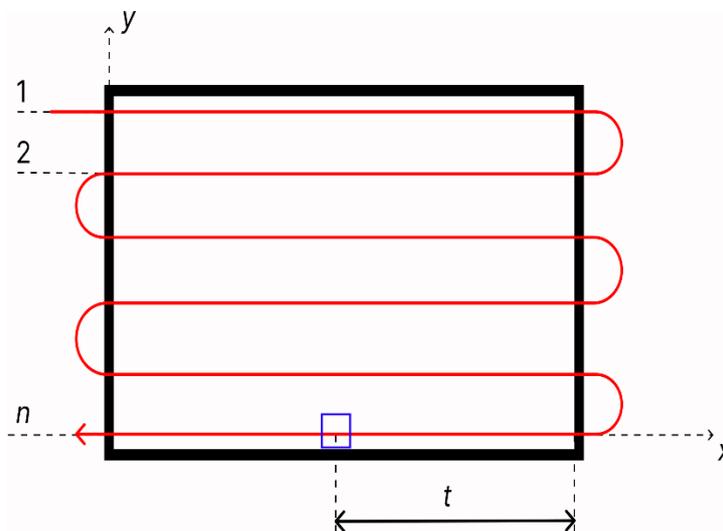


Рис. 3. Итоговый алгоритм сканирования

Аналогичная ситуация складывается с инфракрасным датчиком расстояния. Изменение условий освещенности может привести к ошибочному определению расстояния до объекта, что вызывает необходимость корректировки расстояния, на которое роботу нужно дополнительно проехать при воспроизведении положений объектов, чтобы встать на место, где находился объект.

Конструктивные особенности робота

Из-за нахождения в задней части робота двух моторов и блока аккумуляторных батарей, возникает проблема неправильной «развесовки», что крайне негативно сказывается на ходовых качествах. Так, при начале движения после остановки, или при наезде на небольшую неровность, «нос» робота может задрасться, что приведёт к тому, что датчики освещенности подадут низкий сигнал, вызвав процедуру разворота. Это происходит из-за крайне низкой дальности работы датчиков линии: 3–8 мм. Для решения этой проблемы было введено ограничение по времени на реагирование данных, получаемых с датчиков освещенности (проверка нахождения черной линии начинается только спустя определенный промежуток времени).

Невозможность движения робота по прямой

Из-за изношенностей деталей, а также конструктивных особенностей, робот не может поддерживать прямолинейное движение на дальней дистанции. Это привело к необходимости добавить возможность корректировки

движения робота с помощью пульта ДУ, поскольку прямолинейное движение является важнейшей частью в обоих, представленных ранее, алгоритмах.

Возможные пути решения аппаратных проблем

Ошибку инфракрасного датчика расстояния возможно уменьшить, путём замены его на лазерный, который имеет большую точность и меньшую подверженность влиянию помех.

Ошибочные срабатывания датчиков освещенности можно уменьшить, используя датчики с большей точностью или дистанцией работы. Либо же, путём установления на верх робота дополнительного элемента измерения уровня освещенности (фоторезистор, фотодиод или фототранзистор). Получая с такого датчика данные об уровне освещенности в помещении, можно корректировать чувствительность инфракрасных отражателей. Однако же это приведёт к необходимости дополнительно программировать это взаимодействие.

Проблему «развесовки» можно решить путём переноса блока аккумуляторных батарей ближе к передней части робота. Это предотвратит случайные «вскакивания» робота на неровностях. Данная проблема является наиболее сложной в решении, поскольку движение робота зависит от большого количества параметров. Вот несколько возможных путей решения:

- установка более мягкого гусеничного полотна, что увеличит сцепление с покрытием;
- описанная ранее нормализация «развесовки», также частично может решить эту проблему;
- замена моторов или же изменение конструкции их соединения с ведущей звездой гусеничного трака, что предотвратит засор штифта, передающего крутящее усилие. Соответственно, это уменьшит разницу усилий, приходящих на гусеницы.

В итоге была разработана программа на языке С по поиску объектов на неразмеченной ограниченной площади. Выявлены недостатки устройства робота ROBO-PICA, часть которых была решена программно, а также предложены варианты их исправлений на физическом уровне.

Написанная программа может быть легко адаптирована на различном размерах площадки и количеству объектов, которые могут быть на ней расположены, в пределах памяти микроконтроллера.

Список используемых источников

1. Robot experiment with PIC microcontroller based-on Robo-PICA robot kit // Innovative Experiment Co. Ltd., 2006. 88 с.
2. Заец Н. И. Радиолюбительские конструкции на PIC-микроконтроллерах. М.: Солон-Пресс, 2006. 191с.

УДК 004.05
ГРНТИ 81.93.29

ПРОГРАММНОЕ СРЕДСТВО УПРАВЛЕНИЯ ТЕСТИРОВАНИЕМ НА ПРОНИКНОВЕНИЕ НА ОСНОВЕ РАНЖИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ

Д. А. Агеносов, В. И. Байсарин, Н. В. Погодин, Д. А. Свечников

Академия Федеральной Службы Охраны Российской Федерации

В статье рассматриваются предложения по построению программного средства управления тестированием на проникновение на основе ранжирования угроз безопасности. Программное средство позволяет получать данные для сканирования, собирать информацию с тестируемых хостов, находить уязвимости и формировать эксплоиты, а также генерировать отчеты. Разработанные предложения обеспечивают получение объективных данных по результатам исследований защищенности объекта.

угрозы безопасности, поиск уязвимостей, программное средство тестирования на проникновение

Согласно отчета компании «Positive Technologies» об актуальных киберугрозах за 4-й квартал 2023 года каждая третья успешная атака на организации была связана с эксплуатацией уязвимостей, не выявленных в системе защиты информации [1]. Для повышения полноты учитываемых актуальных угроз при тестировании на проникновение необходимо производить поиск дополнительной информации об возможных уязвимостях. Существующие обособленные средства тестирования не позволяют сформировать объективные данные по результатам исследований защищенности объекта. Учитывая данные недостатки, авторами предложен подход по созданию универсального программного средства тестирования на проникновение, обеспечивающего:

- получение данных для сканирования с веб-интерфейса;
- сбор данных с хоста активным или пассивным методом сканирования;
- поиск уязвимостей программного обеспечения;
- поиск информации о каждой обнаруженной уязвимости;
- поиск опубликованных эксплоитов для каждой уязвимости;
- создание отчета по тестированию.

Программное средство автоматизированного тестирования на проникновение состоит из следующих компонентов: веб-интерфейс; веб-сервер; модуль сканирования уязвимостей; СУБД и обеспечивает взаимодействие с администратором через веб-интерфейс. Функциональная модель работы

средства автоматизированного тестирования на проникновение показана на рис. 1.

Исходные данные, полученные через веб-интерфейс, передаются на сервер и далее в модуль сканирования уязвимостей, который осуществляет поиск уязвимостей на целевом хосте.

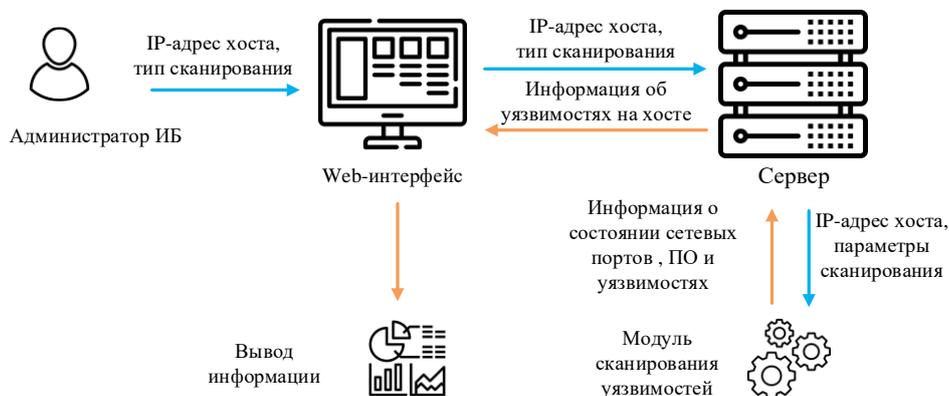


Рис. 1. Функциональная модель программного средства управления тестированием на проникновение

Модуль сканирования уязвимостей включает следующие компоненты: сетевой сканер; анализатор; интерфейс взаимодействия. Функциональная схема модуля сканирования уязвимостей представлена на рис. 2.

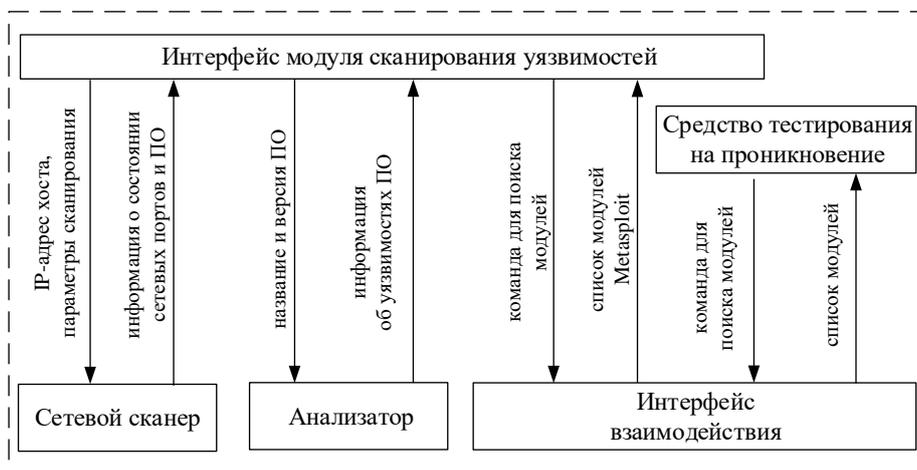


Рис. 2. Функциональная схема модуля сканирования уязвимостей

Сетевой сканер уязвимостей является главным компонентом и выполняет как активное, так и пассивное сканирование объекта. Активное сканирование позволяет выполнить сбор подробной информации об операционной системе, состояниях портов и версиях служб на исследуемом хосте [2]. Используемый в программе сканер Nmap (Network Mapper) поддерживает

различные режимы сканирования TCP, UDP, SYN, ACK, FIN, Xmas, Null, и Idle и позволяет администратору безопасности настраивать объекты и параметры сканирования.

Кроме перечисленных, Nmap предоставляет возможность использования скриптов NSE (Nmap Scripting Engine), что расширяет его функциональность и позволяет автоматизировать задачи, связанные с сканированием и анализом уязвимостей. Например, с помощью NSE возможно автоматически проверить наличие уязвимостей, провести анализ сервисов и выполнить эксплуатацию уязвимости.

Пассивное сканирование выполняется с использованием поисковых систем Shodan и Censys, что позволяет обнаруживать серверы, веб-камеры, маршрутизаторы, подключенные к сети, с использованием различных фильтров. Поисковые системы также используются для выявления сервисных баннеров, предоставляющих метаданные о программном обеспечении [3].

Модуль анализа обеспечивает поиск уязвимостей программного обеспечения, установленного на хосте и дополнительной информации о обнаруженных уязвимостях и эксплоитах.

Модуль интерфейса взаимодействия обеспечивает взаимодействие с эксплойтами и плагинами тестирующей платформы. Используемый в программе Metasploit является одним из универсальных инструментов в области тестирования на проникновение и обеспечивает широкий набор эксплойтов для выявления уязвимостей в сетевых и прикладных программах. Он также предоставляет возможность создания собственных эксплойтов и модулей, что позволяет адаптировать его под конкретные задачи и сценарии тестирования. Кроме того, Metasploit обладает автоматизированными функциями сканирования сети на наличие уязвимых узлов, выбора необходимых эксплойтов и проведение тестирования системы защиты информации.

Таким образом, разработанное программное средство по сравнению с аналогами представляет широкие возможности по сканированию и обнаружению уязвимостей, обеспечивает возможность проведения тестов на проникновение, формирует подробные отчеты исследований на основе ранжирования угроз безопасности.

Список используемых источников

1. Актуальные киберугрозы: IV квартал 2023 года // Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4> (дата обращения: 13.01.2024).
2. Маркин Д. О., Горбачев П. Н., Юркин А. А., Шугуров Д. Е. Программно-аппаратные средства обеспечения информационной безопасности: пособие. Орёл: Академия ФСО России, 2019. 340 с.
3. Средства тестирования на проникновение 2022 // Anti-malware. URL: <https://www.anti-malware.ru/security/penetration-testing> (дата обращения: 13.01.2024).

УДК 537.87
ГРНТИ 60.33.09

ИССЛЕДОВАНИЕ И СРАВНЕНИЕ ФОТОРЕДАКТОРОВ

Б. А. Аль-Нами, Э. Э. Бабаева

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

В 2024 году фотографы по-прежнему горячо обсуждают преимущества Lightroom по сравнению с Photoshop. Каждая платформа предоставляет мощные функции и инструменты для редактирования, но важно понимать их различия, чтобы принять обоснованное решение. В этой статье мы сравним Adobe Photoshop и Lightroom, поговорим о различиях и сходствах программного обеспечения.

качество, надежность, контроль процессов и продукции, радиофотоника, фотодетектор, радиофотонная линия передачи, Adobe Photoshop, Adobe lightroom

Adobe Photoshop – графический редактор растровых изображений. Он предназначен для профессиональных фотографов, графических дизайнеров и художников, которым требуются расширенные инструменты и функции для сложного редактирования и манипулирования изображениями. Одна из немногих вещей, которые не делает Photoshop, – систематизация изображений. Photoshop может очень легко выполнять базовое редактирование фотографий, но его самая сильная сторона – сложные манипуляции с изображениями и расширенное локальное редактирование. Хотите объединить несколько фотографий в одну композицию? Или избавиться от некоторых нежелательных особенностей на фотографии?

Adobe lightroom – программа Adobe для разработки и систематизации изображений Raw с цифровых камер. Он также имеет хорошие возможности редактирования, но они больше связаны с глобальным редактированием и простым локальным редактированием, а не с полноценными манипуляциями с изображениями, такими как Photoshop. Лайтрум имеет большое количество инструментов для организации и последующего поиска информации. Можно сортировать изображения по разным параметрам, например, по марке и модели камеры, дате/времени съемки, диафрагме, выдержке, ISO и т. д. Lightroom также сохраняет все изменения, проведенные с фотографией, так что можно вернуться и доработать в любой момент [1, 2].

Возможности Lightroom:

Основное преимущество данного приложения – его доступность на телефонах и планшетах, обработка изображений в любом месте в любое время, а также возможность скопировать обработку и вставить ее в другие фотографии, что позволяет быстро редактировать репортажные съемки или

серии снимков, это существенно облегчает процесс работы фотографа. А также сортировка и хранение фотографий в облаке Лайтрум без потери качества и настроек.

Функционал:

– Подмодули гистограммы и инструментов: гистограмма, обрезка и выпрямление, удаление пятен, коррекция эффекта «красных глаз», градуированный фильтр, радиальный фильтр, корректирующая кисть.

– Базовый субмодуль: Обработка: цветная и черно-белая; Профили камеры; Баланс белого: температура и оттенок; Тон: Экспозиция, Контраст, Светлые участки, Тени, Белый и Черный; Присутствие: Текстура, Четкость, Удаление дымки, Яркость и Насыщенность.

– Субмодуль «Тоновая кривая»: Регион: Светлые участки, Светлые участки, Темные участки, Тени; Точечная кривая.

– Субмодуль HSL / Цвет / Ч/Б: оттенок, насыщенность, яркость.

– Подмодуль разделенного тонирования: основные моменты: оттенок, насыщенность и баланс; Тени: оттенок и насыщенность.

– Подмодуль «Детализация»: резкость: величина, радиус, детализация и маскировка; Шумоподавление: яркость, детализация, контрастность, цвет, детализация и плавность.

– Подмодуль коррекции объектива: Профиль объектива: удаление хроматической аберрации, включение коррекции профиля; Руководство: Дисторсия, Удаление границ и Виньетирование.

– Субмодуль преобразования: автоматическое преобразование, преобразование: вертикальное, горизонтальное, поворот, соотношение сторон, масштаб, смещение по оси X, смещение по оси Y.

– Субмодуль эффектов: Виньетирование после кадрирования: стиль, количество, средняя точка, округлость, растушевка, блики; Зерно: количество, размер, шероховатость.

– Подмодуль калибровки камеры: версия процесса, тени: оттенок, основной красный: оттенок и насыщенность, основной зеленый: оттенок и насыщенность, основной синий: оттенок и насыщенность.

Возможности и функционал программы Adobe Photoshop практически безграничны: сложные склейки, ретушь, множество наложений, работа со слоями, возможность многослойной цветокоррекции и регулировка прозрачности слоев [3].

В Photoshop есть раздел под названием «Camera Raw», который полностью имитирует параметры настройки Lightroom (хотя интерфейс выглядит немного иначе). Вы можете применить Camera Raw к любому изображению, выбрав «Фильтр > Фильтр Camera Raw» в верхнем меню Photoshop [4].

Так что же удобнее для обработки фото? Для этого нужно провести сравнение, я выбрала одно фото для обработки с нуля в Adobe Photoshop и Lightroom (рис. 1, 2).



Рис. 1. Сравнение в adobe photoshop и lightroom

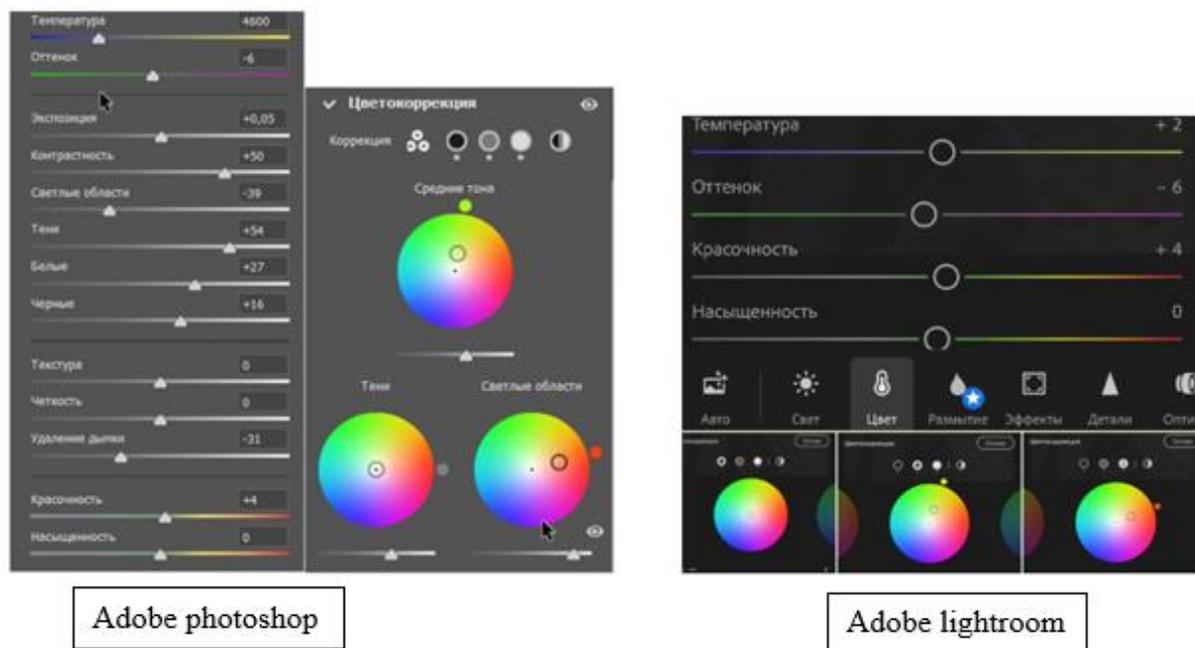


Рис. 2. Сравнение в Adobe Photoshop и Lightroom

Оба кадра обработаны с одинаковой настройкой, при этом выглядят абсолютно иначе: приложения воспринимают цвет и работают с ним по-разному [5].

Кроме того, можно видеть небольшие различия в функционале программ: некоторые настройки выставляются иначе и имеют разные значения. Например, температура.

Из собственного опыта, Лайтрум более удобен для быстрой или мобильной обработки, но если нужно работать с фото детально: ретушь, исправление неровностей, текстуры, инструмент «штамп», то удобно сразу использовать Adobe Photoshop. Adobe lightroom применим для фото дальнего плана и поэтому незаменим для фотографов [6]. Lightroom более прост в освоении для начинающих, содержит большое количество инструментов для обработки, можно скопировать настройки с одного фото на остальные, нет необходимости открывать несколько файлов и легко вернуться, и исправить фото, так как они все хранятся в приложении по настроенному пользователю формату.

Список используемых источников

1. Al-Nami B. A., Musaeva T. Modern methods to solve the problems of adapting images in web pages and the possibility of using artificial intelligence to do so in the future // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 180-185.
2. Al-nami B. A. Converting images from one extension to another without losing its quality, problems and solutions // big data и анализ высокого уровня: IX международная научно-практическая конференция: в 2х частях. Минск, 2023. С. 51-61.
3. Кокошкин А. В., Коротков В. А., Коротков К. В., Новичихин Е. П. Слепое восстановление изображений, искажённых смазом и дефокусировкой, при неизвестной форме и параметрах АФ // Радиоэлектроника. 2014. № 9.
4. Адамчик М. В. Дизайн и основы композиции в дизайнерском творчестве и фотографии. Харвест. 2010. 192 с.
5. Al-Nami B. A. The impact of artificial intelligence on the profession of designers and programmers // Вопросы исторического и современного развития: международная научно-практическая конференция и научно-образовательная студенческая конференция по архитектуре и дизайну. В 2-х томах. Тюмень, 2023. С. 274-276.
6. Фриман М. Школа фотографии Майкла Фримана. Композиция. М.: Добрая книга, 2012. 160 с.

УДК 004.514,415.2
ГРНТИ 81.95.33

ПРОЕКТИРОВАНИЕ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ЦВЕТОЧНОГО МАГАЗИНА

Б. А. Аль-Нами, Н. А. Беляева

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

В данной работе проводится исследование касательно использования людьми мобильных приложений по доставке цветов, анализ визуального и функционального представления дизайна такого приложения, а также оценка его аналогов, представленных на рынке в данный момент.

UI-design, графический пользовательский интерфейс, мобильное приложение, средства разработки, интерфейс, design, mobile applications, внедрение, проектирование

Так как большая часть людей при нынешнем темпе жизни выполняет все повседневные дела с мобильного, и заказ цветов с подарками будет удобнее именно с телефона. Для этого требуется мобильное приложение, позволяющее найти, выбрать, заказать и отследить доставку подарка и букета до нужного адреса [1].

Многие приложения по доставке цветов имеют кричащий, непривлекательный дизайн интерфейса, мало ассоциирующийся с нежными красивыми букетами.

Целью работы было разработать удобное приложение флористического магазина для выбора и доставки и подарков с визуально приятным интерфейсом и востребованным среди пользователей функционалом [2, 3].

Для подтверждения актуальности темы, а также выявления требований к мобильному приложению, был проведен опрос.

По результатам опроса 92 % интервьюируемых сказали, что любят дарить цветы, 72 % из которых делают это регулярно. Однако большая часть опрошенных отметила, что опыт использования онлайн-сервисов для заказа был негативным. Это подтверждает необходимость доработки подобных систем.

Также было выявлено, что большинство пользователей (64 %) в первую очередь ориентируются на цветовую гамму при выборе букета. Данный параметр удобно отразить в виде фильтра в будущем мобильном приложении.

88 % опрошенных хотели бы иметь возможность самостоятельно выбирать состав подарка при заказе. Данный факт также должен быть учтен в дальнейшей разработке [4].

После проведения опроса были выявлены основные требования и критерии к мобильному приложению, на основании которых был проведен конкурентный анализ. (рис.1).

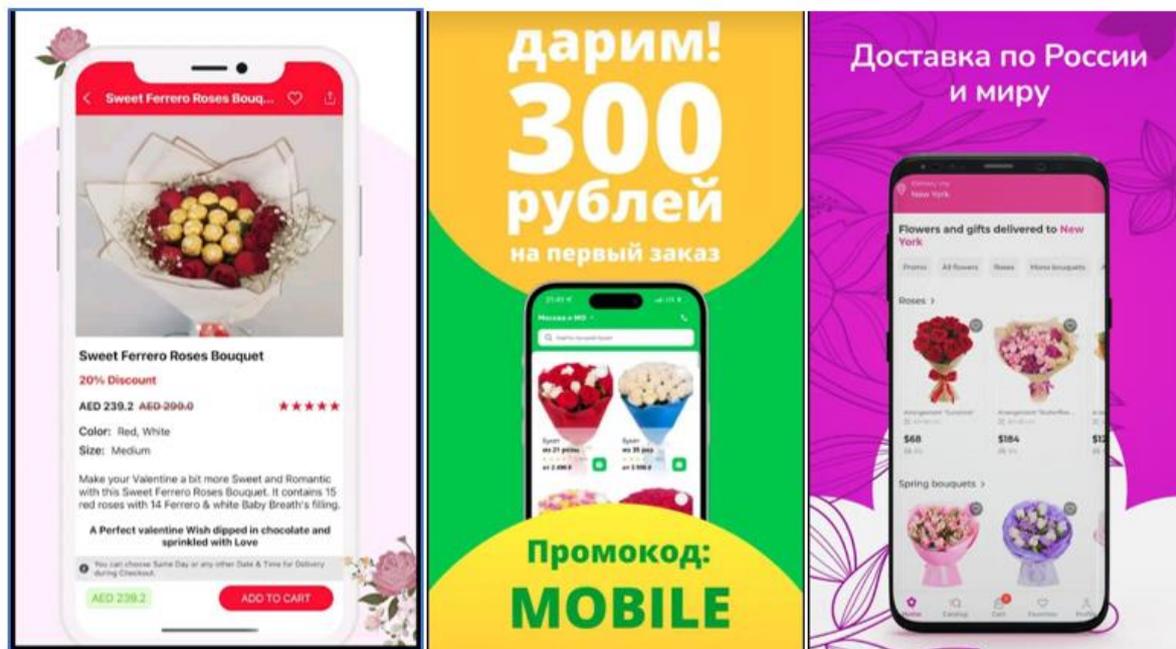


Рис. 1. Скриншоты приложений по доставке цветов

Критерии сравнения:

Визуальные требования:

- 1. Минималистичность
- 2. Отсутствие визуального шума
- 3. Спокойная цветовая гамма
- 4. Интуитивно понятный интерфейс

Функциональные требования:

- 1. Фильтры и категории
- 2. Согласование времени и адреса доставки
- 3. Конструктор подарка
- 4. Подборки к праздникам

Удобные фильтры и категории для быстрого поиска:

преимущественно в таких приложениях (если брать российские) предлагаются уже собранные букеты, поиск по цветам предоставляется лишь на самые известные – розы [5].

Однако найдены и удачные примеры, с выборкой по стоимости (до определенной суммы), настроению, по конкретным цветам и праздникам (см. рис. 2).

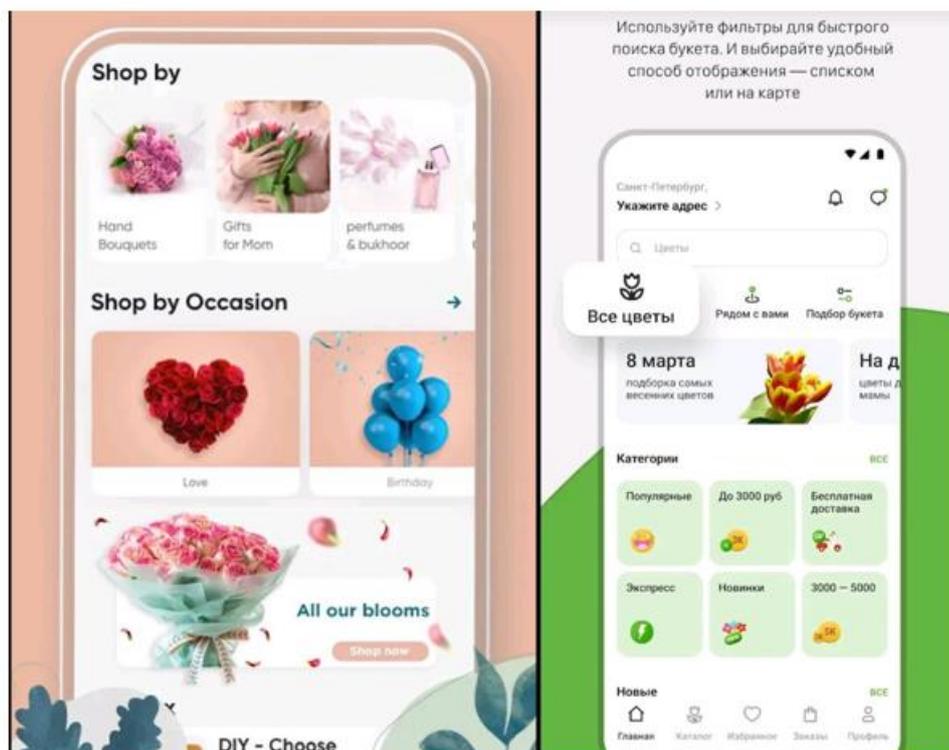


Рис. 2. Скриншоты приложений с выборками

Функция согласования времени и адреса доставки: она актуальна, когда хочется сделать приятно не слишком знакомому человеку или если проконтролировать и согласовать доставку самому нет возможности. Поэтому решено добавить данную функцию в разработку.

Аналоги оценивались по балльной системе в соответствии с вышеперечисленными критериями. Максимальный балл – 8 (по 4 балла за визуальную и функциональную составляющую). Чем выше балл, тем лучше оценен конкретный аналог [6].

Подробный анализ конкурентов на конкретных примерах существующих приложений представлен в таблицах 1–3 ниже.

Из таблицы 1 видно, что большинство приложений обладают слабым визуальным представлением (0–1 балл из 4). Часто встречается слишком яркая гамма и визуальный шум.

Требованию минималистичности большая часть приложений конкурентов также не удовлетворяет.

Особенно низкий балл за визуальную составляющую у приложения Flor2U (0 баллов из 4).

По таблице 2 можно видеть, что ни в одном из проанализированных приложений конкурентов нет функции конструктора подарков. Что подтверждает новизну и актуальность данной разработки.

На основании полученных баллов в таблицах 1 и 2 можно составить общий рейтинг для приложений конкурентов (см. табл. 3).

ТАБЛИЦА 1. Оценка визуальной составляющей приложений конкурентов

Визуальная составляющая					
Название приложения / Критерий	Минимализм	Отсутствие визуального шума	Спокойная цветовая гамма	Интуитивно понятный интерфейс	Суммарный балл
Flor2U	0	0	0	0	0
Flawery	1	1	1	1	4
Aroma Flowers UAE	0	0	0	1	1
Русский букет	0	0	0	1	1
Floward online	1	1	1	1	4

ТАБЛИЦА 2. Оценка функций приложений конкурентов

Функциональная составляющая					
Название приложения / Критерий	Согласование времени и адреса	Фильтры и категории	Конструктор подарка	Подборки к праздникам	Суммарный балл
Flor2U	0	0	0	0	0
Flawery	0	1	0	1	2
Aroma Flowers UAE	1	1	0	0	2
Русский букет	0	1	0	0	1
Floward online	1	1	0	1	3

Как видно из таблицы 3, ни одно из приложений конкурентов не набрало максимального балла (8 баллов) за обе составляющие [7]. Таким образом, данная разработка актуальна и требует создания собственного приложения по доставке цветов с учетом недостатков и ошибок в приложениях конкурентов.

Особое внимание будет уделено визуальной части приложения, так как большинство приложений конкурентов получили максимально низкий балл за оформление.

ТАБЛИЦА 3. Итоговый рейтинг приложений конкурентов

Итоговый рейтинг		
Место	Название приложения	Итоговая оценка
1	Floward online	7/8
2	Flawery	6/8
3	Aroma Flowers UAE	3/8
4	Русский букет	2/8
5	Flor2U	0/8

В качестве хорошего примера реализации приложения по доставке цветов был выбран Floward online, так как он удовлетворяет большинству поставленных требований (7 баллов из 8) и имеет понятный интерфейс при сохранении нужных функций.

Список используемых источников

1. Прасолова Е. А., Курзаева Л. В. Проектирование интерфейса мобильного приложения для центра дополнительного образования // Международный студенческий научный вестник. 2018. № 5.
2. Седлецкий К. В. Анализ технологий разработки мобильных приложений // Молодежный вестник Уфимского государственного авиационного технического университета. 2020. № 1 (22). С. 136–138.
3. Семенчук В. Мобильное приложение как инструмент бизнеса. Альпина Диджитал, 2016. 270 с.
4. Голошапов А. Л. Google Android. Создание приложений для смартфонов и планшетных ПК. БХВ-Петербург, 2013. 832 с.
5. Дерюгин С. В. Методы и средства проектирования информационных систем // Молодой ученый. 2017. № 17. С. 51–56.
6. Майер Р. Android 2: Программирование приложений для планшетных компьютеров и смартфонов. М.: Эксмо, 2011. 672 с.
7. Ремаренко С. А., Фролов Д. А. Анализ возможностей использования технологий мобильных приложений в деятельности предприятия // Молодой ученый. 2015. Т. 22. № 5 (102). С. 32–34.

УДК 004.8: 004.032.26
ГРНТИ 28.23.00:37

РОЛЬ НЕЙРОСЕТЕЙ В РАЗВИТИИ МАШИННОГО ПЕРЕВОДА

Б. А. Аль-Нами, И. Г. Боков

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

Главной целью следующей статьи является введение в принципы работы нейросетей в ходе машинного перевода текста. Помимо этого, в статье приводится мировая история машинного перевода, его актуальные проблемы и перспективы развития, а также общая информация касательно принципов работы нейросетей.

нейросети, автоматизация, машинный перевод, естественный язык, искусственный интеллект, технологии машинного перевода

Машинный перевод как понятие призван минимизировать вовлечённость человека в непосредственный процесс перевода. Полное исключение переводчика в процедуре перевода крупных текстов опрометчиво, поскольку даже для рукотворных переводов необходима редактура, но даже буквальный перевод отдельных слов является в этом плане существенным прорывом относительно использования словаря.

С этой точки зрения переводная машина Петра Троянского, концептуально созданная ещё в 1933 году, не кажется большим прорывом, поскольку требует активного использования человеческих ресурсов, но уже она определяет алгоритм из трёх этапов работы. Сама машина представляла из себя сопоставленный перевод конкретного слова на несколько языков в виде таблицы, фотокамеру и печатную машинку [1]. На первом этапе перевода оператор машины фотографирует слово и его переводы на несколько языков и обозначает грамматические пояснения с помощью печатной машинки, на втором проверяющие раздельно составляют из полученной информации текст, и на третьем этапе знающие оба языка редакторы совместно приводят текст в литературный вид. В то же время, качественный машинный перевод позволяет сократить этапы перевода слов и составления из них предложений, что приводит к значительной экономии человеческих и временных ресурсов, рис.1.



Рис. 1. Проект переводной машины Троянского

Машинный перевод текста, а не отдельных слов, имеет ряд серьёзных проблем, связанных с невозможностью «понимания» контекста программой. Это приводит к наличию ряда уязвимых мест, связанных с использованием:

- • многозначительных слов и омонимов;
- • устойчивых выражений и сочетаний слов;
- • нестандартных аббревиатур и терминов.

Кроме того, проблемы в процессе перевода возникают по причине различий в построении предложений между разными языками, что не только приводит к очевидной неестественности итогового перевода, но и может вызвать ошибки в согласовании слов в итоговом результате, из чего могут последовать проблемы из обозначенного выше перечня [2].

Если проблема сочетаний слов всё же может быть решена с большим трудом с помощью т.н. основанных на правилах системах (rule-based), то само по себе определение контекста является извечной проблемой подобных систем, и наиболее вероятным ключом к её решению может быть именно использование нейросетей [3]. В то время, как большая часть усилий по совершенствованию машинного перевода была сосредоточена на составлении правил, в девяностых годах исследовательский центр ИВМ имени Ти Джея Уотсона подошёл к проблеме машинного перевода со статистической точки зрения. Принцип работы системы машинного перевода «Кандид» заключался в следующем: поданный на вход текст на первом языке обозначался как искажённый в процессе перевода текст на втором языке, и поэтому поставленной для системы задачей была дешифровка «изначальной версии» ввода. Таким образом, наиболее вероятный перевод на английский (e) изначальной французской фразы (f) может быть представлен в следующем виде (1):

$$e^* = \arg \max p(f | e) \times p(e), e \in E, \quad (1)$$

где E – перечень всех фраз на английском в заданной языковой модели.

Для составления языковой пары использовалась документация канадского парламента в США, ведомая на английском и французском языке, что позволило получить большой первоначальный объем текста для обучения системы. Несмотря на то, что в команде исследовательского центра практически не было людей, знакомых с французским языком, получившаяся модель работала исправно и сравнительно хорошо, что демонстрирует эффективность подобного подхода [4].

В обозначенной выше системе заметны элементы, свойственные обучению нейросетей: первоначальное обозначение пар «ввод-вывод», построение ассоциаций и кластеризация по выведенным признакам. Для подобного процесса у IBM имелся большой набор изначальных данных (упомянутая документация посольства). Но в отличие от современных нейросетей, машинное обучение системы Candid не представляло из себя т.н. глубокое обучение, т.е. способное выводить вычисленный самостоятельно результат на основе введенных данных: Candid была способна сопоставлять ввод с уже имеющимся данными. Для следующего шага – генерации новых данных на основе имеющихся – в девяностые годы не хватало вычислительных мощностей.

Появление этих самых вычислительных мощностей привело к появлению архитектуре нейросетей под названием трансформер. В ходе его работы поступающий текст разбивается на последовательности текста (N-граммы) и преобразуется в токены, в то время как каждый токен затем преобразуется в вектор на основании таблицы векторного представления слов и контекстуализируется на каждом уровне обучения, уменьшаясь или увеличиваясь в весе в ходе обработки [5]. В подобной таблице похожие по значению слова имеют схожий вектор, и в зависимости от небольших изменений контекста нейросетью и выбирается наиболее подходящее в данном случае слово (или его элемент). В свою очередь, архитектура трансформера позволяет сформировать т.н. Большие Языковые Модели – языковые модели, способные к пониманию и генерации базового языка и обученные без учителя, т.е. без определённых заранее кластеров. В свою очередь, подобные языковые модели, способные оперировать первоначальным «смыслом» отдельных элементов речи, не ограничивающихся только словами, являются при использовании достаточных объёмов текста по-настоящему эффективными средствами перевода текста с одного языка на другой [6].

Таким образом, методы статистического перевода, впервые рассмотренным IBM и применяемые в наше время при создании нейросетей, на данный момент являются наиболее перспективным методом развития машинного перевода в противовес правило-ориентированным. На данном этапе развития нейросетей важную роль играют особенности архитектуры, что демонстрирует, например, компания OpenAI со своей нейронной моделью Генеративного предобученного трансформера (GPT): за последние пять лет

всего было выпущено четыре поколения архитектуры данной модели, каждая из которых по эффективности значительно превышает предыдущую. С ростом имеющихся у IT-компаний данных и ресурсов, возможно, разработки в области нейросетей уже в ближайшие годы позволят получить машинный перевод, предельно близкий к возможному человеческому. Доступность подобных инструментов для широкой общественности находится под вопросом – однако в крупных кампаниях развитие нейросетей почти наверняка приведёт к сокращению штатов и переводчиков, по аналогии с подобными процессами в других сферах работы.

Список используемых источников

1. Аль-Нами Б. А., Сидорова С. М., Чупрова А. Ю. Области применения искусственного интеллекта // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 236–239.

2. Нейронные сети в машинном переводе: статус-кво // Системный Блок. URL: <https://sysblok.ru/nlp/nejronnye-seti-v-mashinnom-perevode-status-kvo> (дата обращения: 14.12.2023)

3. Аль-Нами Б. А., Бондаренко Д. С., Кривошеев Д. В. Различные виды предварительного обучения (Pre-Training) в качестве способов решения основных проблем NLP // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 85–88.

4. Аль-Нами Б. А., Вильготский Е. П. Нейросети – ключ к будущему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 63–67.

5. Аль-Нами Б. А., Васильев В. В., Мелехов О. С. Искусственный интеллект: от теории к практике // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 85–88.

6. Аль-Нами Б. А., Сугако С. А. Технологии чат-ботов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 253–256.

УДК 004.514
ГРНТИ 81.95.33

РАЗРАБОТКА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ВЕБ-САЙТА ЛОГИСТИЧЕСКОЙ КОМПАНИИ

Б. А. Аль-Нами, Ю. Р. Пигарева

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

Данная научная статья посвящена разработке пользовательского интерфейса веб-сайта логистической компании для решения существующей проблемы - разрозненного хранения фирменных продуктов и документов. В статье рассматривается процесс создания специализированного раздела на веб-платформе, предназначенного для удобного доступа сотрудников к актуальным версиям шаблонов документов, презентаций, логотипов и других брендовых материалов.

веб-сайт, интерфейс, карусель, айдентика, дизайн, пользователь, плоский дизайн, пользовательский интерфейс, визуальный дизайн интерфейсов, пользовательский опыт, проектирование интерфейса, интерфейсы сайтов

На сегодняшний день многие компании сталкиваются с проблемой разрозненного хранения фирменных продуктов таких как шаблоны документов, презентаций, логотипы и другие элементы бренда. Отсутствие централизованного доступа к этим ресурсам приводит к неэффективному использованию времени сотрудников и возможным ошибкам в работе из-за использования устаревших или несогласованных материалов [1].

Для решения данной проблемы необходима разработка пользовательского интерфейса веб-сайта компании, включающего в себя отдельный раздел, предназначенный для сотрудников. Этот раздел будет функциональным пространством, где сотрудники смогут легко получать доступ к актуальным версиям всех фирменных продуктов и документов, не прибегая к поиску помощи у коллег и без риска использования устаревших материалов [2].

Предмет исследования - раздел сайта, содержащий информацию необходимую сотрудникам.

На основании технического задания заказчика было принято решение о создании отдельного раздела на сайте с шаблонами различных документов [3]. Чтобы попасть в данный раздел, каждому сотруднику нужно пройти авторизацию (рис.1). После чего сотрудник переходит в новую категорию с образцами документов (рис.2), необходимых для дальнейшей работы:

Для удобства пользователя были разработаны следующие страницы:

- • Образцы презентаций

- • Образцы необходимых для работы документов
- • Образцы с айдентикой

В разделе с презентациями можно просмотреть ранее разработанные презентации [4] и выбрать необходимые для работы. В данном разделе предусмотрен просмотр конкретного образца, а также фильтрация по: теме, языку и так далее (рис. 3). Также по каждой презентации можно посмотреть сведения о: теме, авторе, основных цвета. Затем выбранные файлы в личном кабинете можно скачать (рис. 4).

Остальные страницы имеют аналогичный дизайн.

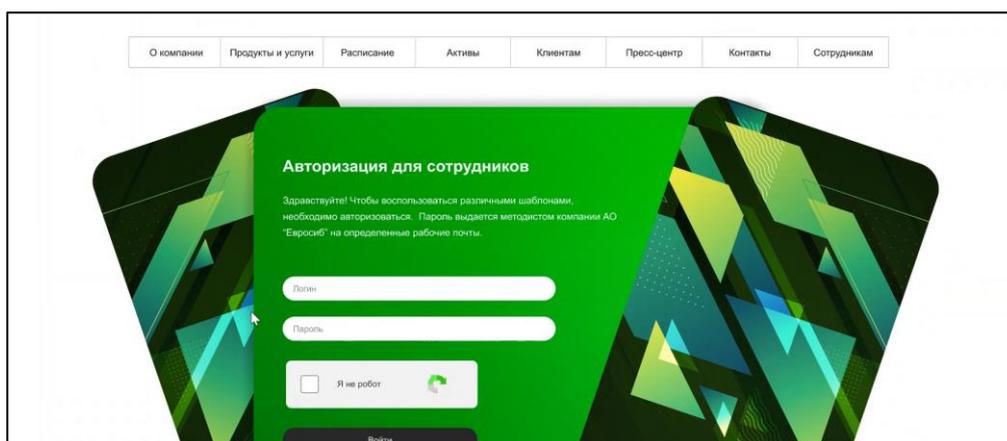


Рис. 1. Авторизация

На данной картинке (рис. 1) показан процесс авторизации. При переходе на данную страницу сотрудник видит текст о том, что он увидит далее, после входа в систему. Чтобы пройти авторизацию, сотруднику необходимо ввести логин и пароль, который им предварительно выдали, и нажать кнопку «Войти».

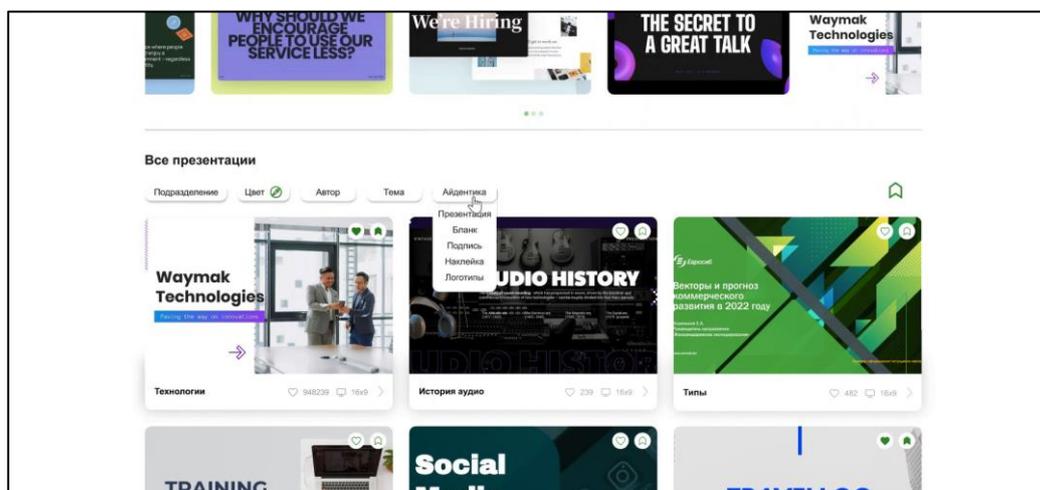


Рис. 2. Образцы документов

На рис. 2 можно просмотреть перечень шаблонов. В верхней части находится карусель с лучшими образцами документов. Для выделения какого-то конкретного шаблона только в своем личном кабинете, необходимо нажать на кнопку «Флажок». А чтобы отметить у всех понравившийся образец – «Сердце». Также здесь присутствует фильтрация по нескольким категориям: подразделения, цвета, авторы, темы и айдентика.

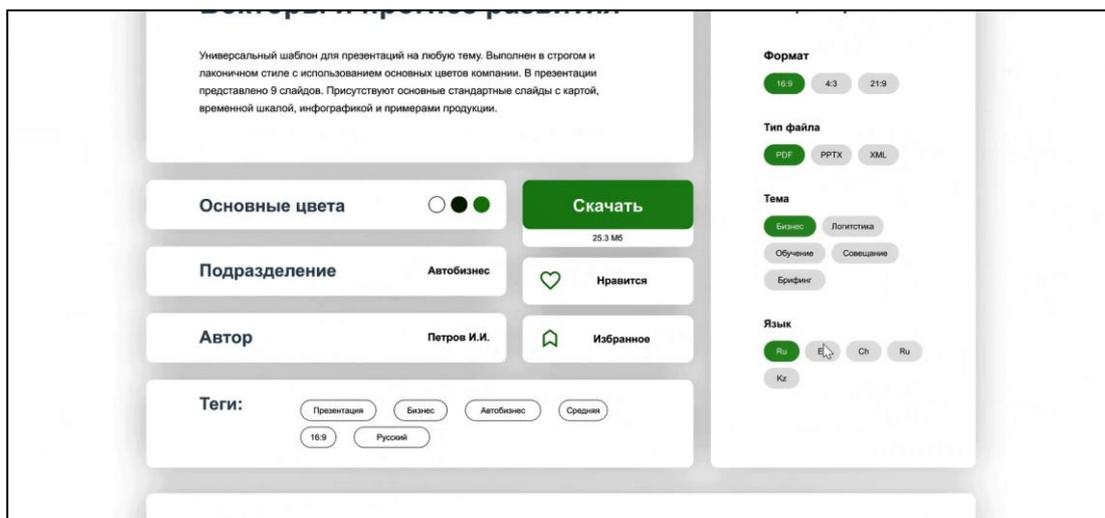


Рис. 3. Просмотр конкретного образца

Здесь (рис. 3) подробно показан конкретный образец документа, выбор документа по определенным категориям, которые были ранее перечислены.

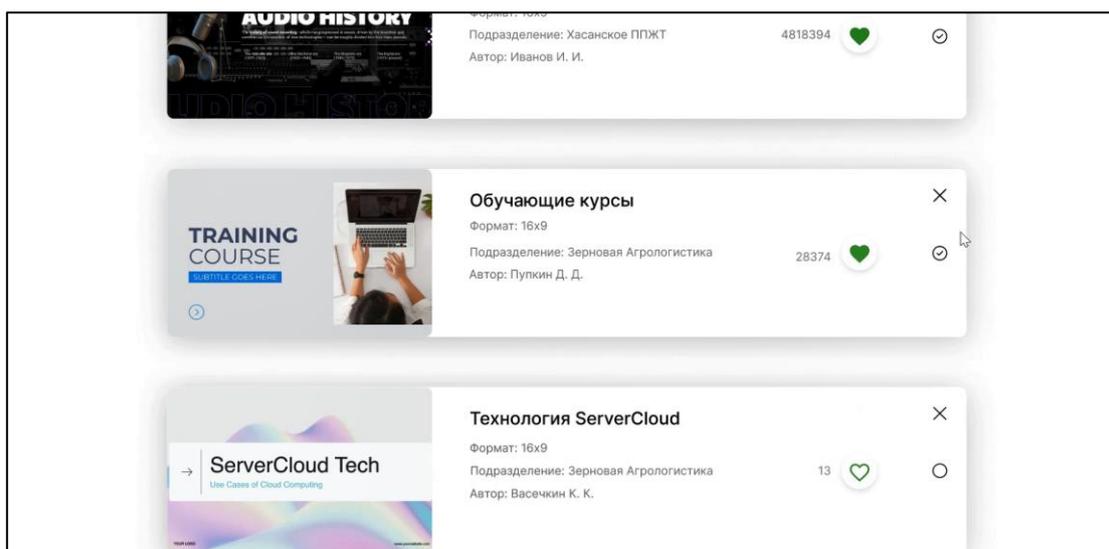


Рис. 4. Скачивание файлов

Тут (рис. 4) можно увидеть выбранные презентации, которые в дальнейшем будут скачены. Об этих документах есть краткая информация об авторе, подразделении и формате [5]. Если выбранный документ разонравился, то его легко удалить, нажав на «Крестик».

Результаты исследования

Перед разработкой личного кабинета были просмотрены варианты на различных сайтах, изучена литература по данной тематике и был разработан вариант, максимально соответствующий требованиям заказчика.

Разработка нового дизайна личного кабинета позволяет сэкономить время сотрудников на поиске необходимых для работы файлов. Наличие различных вариантов презентаций дает возможность создавать новые презентации в необходимом корпоративном стиле. Удаленный доступ в личный кабинет позволяет сотруднику найти все необходимое для работы в любой точке мира.

Список используемых источников

1. Михеев С. И., Рукавишников В. А. Разработка структуры пользовательского интерфейса, поисковой оптимизации сайтов на базе языка «Java Script» // Современные наукоемкие технологии. 2013. № 8-2. С. 361–362.
2. Айрапетян Г. М. Дизайн мобильного приложения // Молодой ученый. 2018. № 48 (234). С. 12–15.
3. Печников В. Н. Создание Web-страниц и Web-сайтов. М.: Триумф, 2010. 370 с.
4. Смирнова И. Е. Начала web-дизайна. СПб., 2010. 491 с.
5. Миронов А. С. Пользовательский интерфейс // Молодой ученый. 2016. № 15 (119). С. 145–147.

УДК 004.424
ГРНТИ 81.93.29

ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ ИНФОРМАЦИИ

Б. А. Аль-Нами, В. В. Селина

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

В данной статье рассмотрена проблема утечки и подделки информации. Целью работы является изучение криптографии и выявление метода защиты передаваемой информации. В ходе работы была выявлена необходимость защиты информации. В результате была написана программа «encoder», с помощью которой происходит шифрование информации с дальнейшим ее дешифрованием, чтобы предотвратить возможность ее прочтения и подделки.

шифрование, дешифрование, защита информации, информационная среда, симметричное шифрование, программа, криптография, криптографические ключи, общий закрытый ключ, аутентификация

Проблема: при передаче информации в текстовом формате может произойти утечка передаваемой информации.

Шифрование и, соответственно, дешифрование, одна из важнейших тем нашего общества на данный момент истории человечества. Сейчас информация стала, по сути, основным товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит воруют и подделывают и, следовательно, ее необходимо защищать. Современное общество все в большей степени становится информационно-обусловленным, успех любого вида деятельности все сильнее зависит от обладания определенными сведениями и от отсутствия их у конкурентов [1]. И чем сильнее проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации с железной необходимостью привело к возникновению индустрии средств защиты информации. Среди всего спектра методов защиты данных я выбрала метод шифрования с помощью общего закрытого ключа [2].

Итоговая цель – написать программу, так или иначе связанную с темой работы. Был выбран вариант с симметричным шифрованием, в связи с тем, что изначально в планах была программа с ручным шифрованием, а другие варианты подразумевают под собой автоматическое шифрование и заморочки с несколькими криптографическими ключами шифрования [3].

Вашему вниманию предоставляю программу под названием «encoder», которой может пользоваться каждый, по мере необходимости.

Метод шифрования, используемый в программе простыми словами:

Берется определенная фраза для шифрования, от неё забирается первая буква, находится её позиция в определённом алфавите, потом она заменяется на букву с той же позиции, но в другом алфавите [4].

В нашей программе:

- • Симметричное шифрование
- • Общий закрытый ключ
- • Аутентификация каждого пользователя
- • Темная и светлая тема для удобства

Используемые языки программирования: Python, HTML, CSS.

Если вы используете программу впервые, необходимо пройти регистрацию для более удобного использования программы [5].

Для этого в левом нижнем углу есть кнопка «Регистрация». После открытия меню нужно ввести идентификатор (он же логин), создать собственный ключ, который будет прикреплен к вашему идентификатору, затем ввести пароль.

После регистрации Вам нужно совершить вход под своим личным идентификатором (рис. 1).

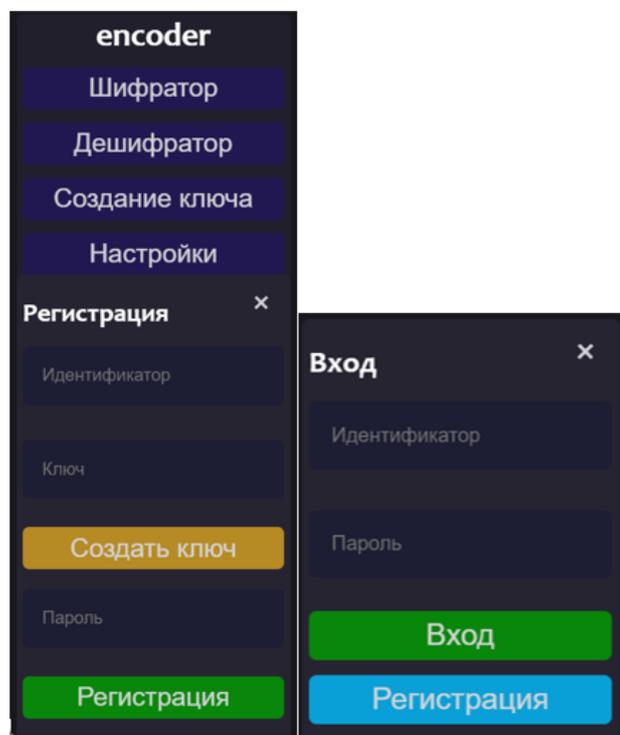


Рис. 1. Идентификация пользователя

Чтобы зашифровать сообщение, надо перейти во вкладку «Шифратор». Ввести текст в специальное поле, вставить ключ и преобразовать информацию. Наоборот, чтобы расшифровать полученный преобразованный текст, нужно перейти во вкладку «Дешифратор» и сделать то же самое (рис. 2).

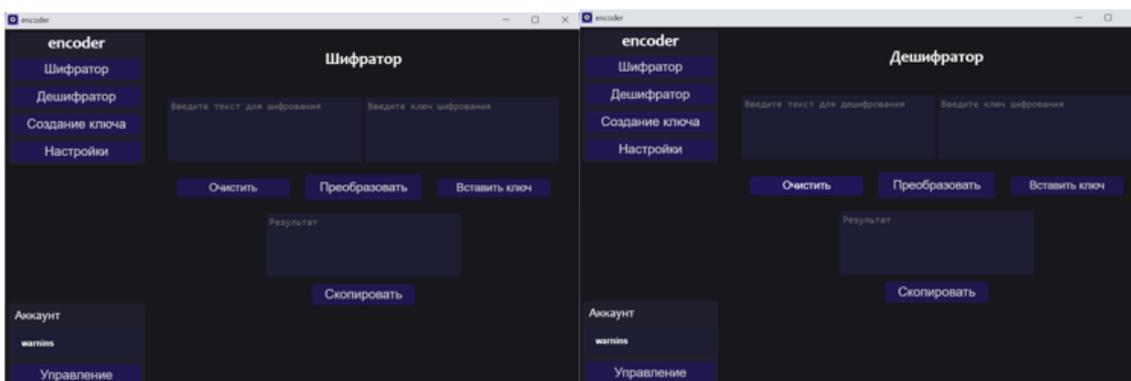


Рис. 2. Шифрование и дешифрование

Если вдруг у вас не вставляется ключ, тогда необходимо создать новый ключ во вкладке «Создание ключа» и работать с помощью нового ключа, предварительно его куда-то записав (рис. 3).

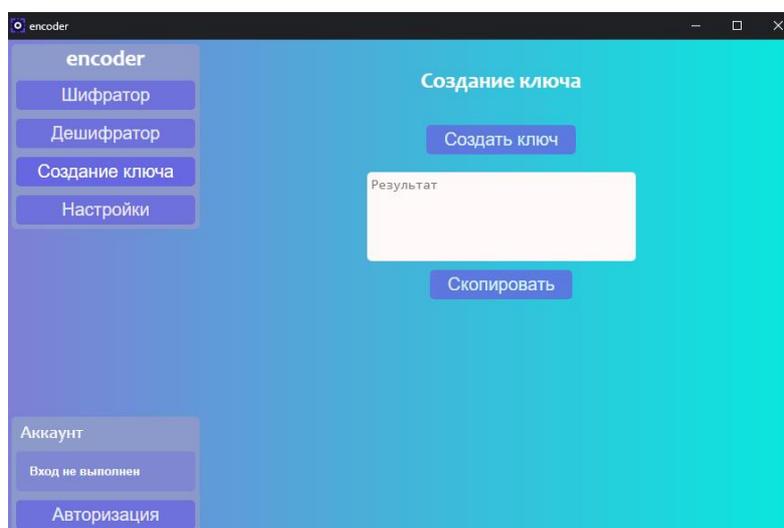


Рис.3. Создание ключа

Для индивидуального удобства можно включить темную тему программы (или же оставить светлую). Для этого нужно перейти во вкладку «Настройки» и выбрать предпочитаемый интерфейс (рис. 4).

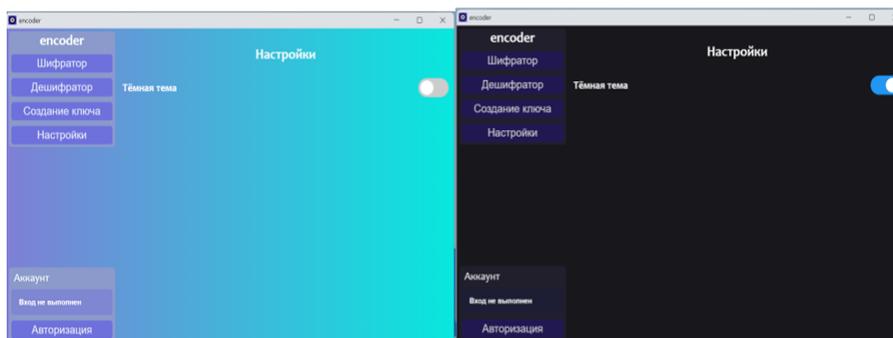


Рис. 4. Интерфейс

Также в программе можно как выйти с аккаунта, так и удалить его по личным причинам. В случае, если Вы планируете выйти из аккаунта – нужно нажать кнопку «Выйти». А для того, чтобы удалить аккаунт – нажать кнопку «Удалить аккаунт», которая находится ниже (рис. 5).

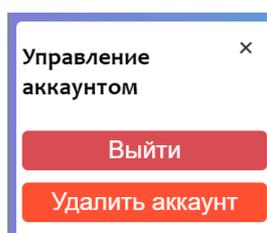


Рис. 5. Выйти или удалить аккаунт

Наглядный пример работы программы:
Сначала зашифруем текст, вставив в поле для ключа, личный ключ (рис. 6).

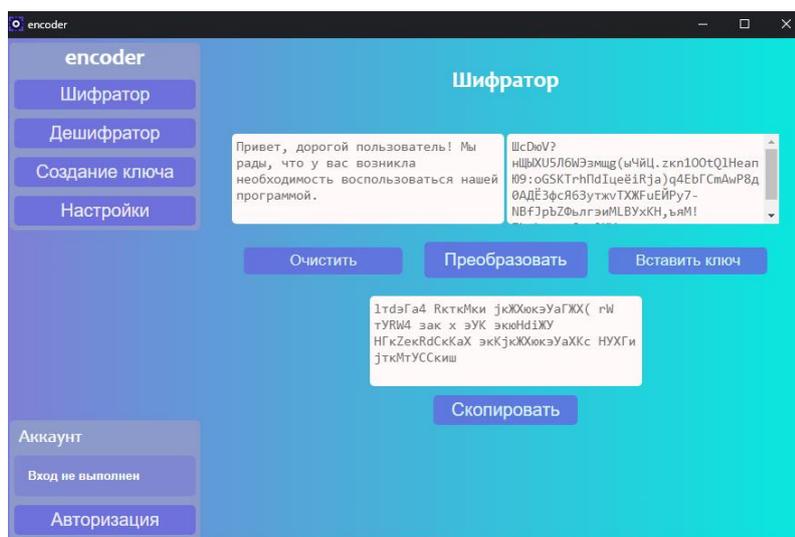


Рис. 6. Пример шифрования.

Далее расшифруем текст с помощью того же ключа, что и зашифровали текст (рис. 7).

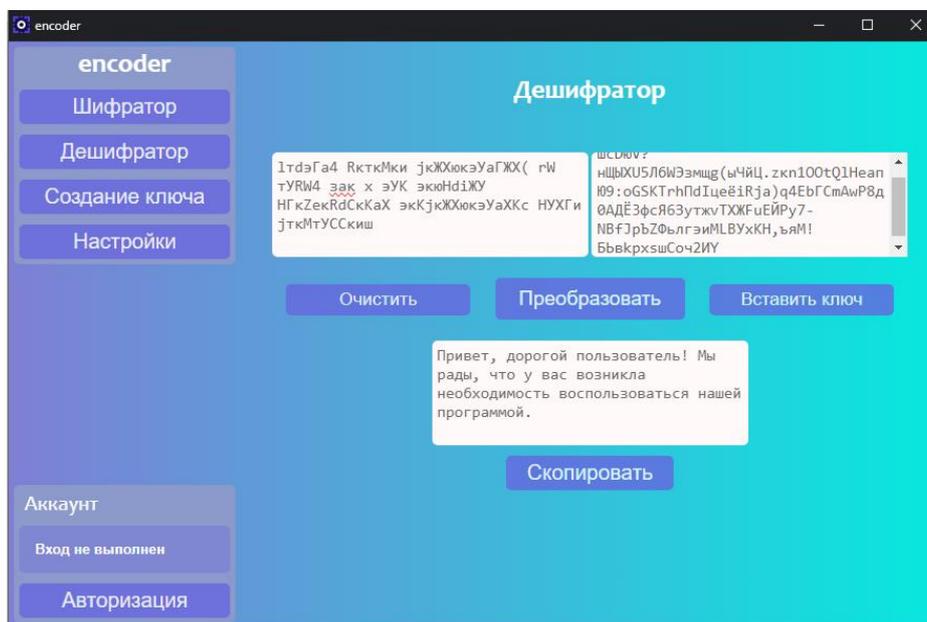


Рис. 7. Пример дешифрования.

Вывод: в ходе работы была исследована тема защиты информации при передаче в текстовом виде и, как следствие, была написана программа на разных языках программирования, с помощью которой можно шифровать и дешифровать информацию, тем самым не переживать за то, что ее может кто-то подделать или прочитать.

Список используемых источников

1. Аль-Нами Б. А., Загретдинов А. Э. Анализ методов шифрования // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 133–135.
2. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. М.: Машиностроение, 2014. 256 с.
3. Аль-Нами Б. А., Губин Ю. М. Вредоносное программное обеспечение // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 117–120.
4. Бабенко Л. К. Современные интеллектуальные пластиковые карты. М.: Гелиос АРВ, 2015. 416 с.
5. Аль-Нами Б. А., Омаров Э. Г. Защита персональных данных и законодательство о защите информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 192–195.

УДК 004.42
ГРНТИ 50.05.09

ИССЛЕДОВАНИЕ РАЗНИЦЫ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛЬНОГО И ОБЪЕКТНО- ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ В ЯЗЫКЕ PYTHON

Б. А. Аль-Нами, К. Е. Симкин

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

В современной IT индустрии существует огромное количество различных языков программирования, в основном в них применяются два вида программирования: объектно-ориентированное и функциональное. В этой статье будет разбираться применение этих видов программирования в языке Python, как одного из самых простых и востребованных в индустрии.

Python, язык программирования, web-разработка, библиотеки Python, синтаксис языка, Объектно-ориентированное программирование

Объектно-ориентированное программирование (ООП) - метод разработки ПО, работающий с объектами, которые включают в себя данные и функции для работы с этими данными. В ООП программа состоит из объектов, которые взаимодействуют между собой с помощью методов, являющихся функциями внутри класса. Объекты обладают свойством наследования, таким образом один и тот же метод может быть использован в любом дочернем классе, наследуемом от родительского, таким образом изменение кода программы происходит достаточно быстро. ООП позволяет создавать модульные программы, которые легко поддаются модификации [1].

Функциональное программирование (ФП) – стиль программирования, который в первую очередь основан на вычислении функций. В этом стиле программирования программы представляются как набор функций, в которые в качестве аргументов передаются определенные данные, которые обрабатываются внутри функции, после чего функция либо возвращает результат обработки, либо не возвращает ничего. В функциональном программировании используются такие понятия, как чистые функции, каррирование и рекурсия.

Отличительные черты ООП и ФП в Python, их сравнение

Объектно-ориентированное программирование (ООП) и функции в Python имеют разные цели и способы применения [2].

ООП используется для создания модульных и легко изменяемых программ, основанных на классах и объектах. Оно позволяет инкапсулировать данные и методы внутри класса, что обеспечивает их защиту и возможность повторного использования. С помощью ООП создаются Дочерние и Родительские классы, которые могут использовать одни и те же методы, описанные в классе с более высокой иерархией. Кроме того, для обращения к родительским методам используются методы суперклассов [3].

В таблице 1 Функции в Python используются для разделения логики программы на более мелкие и управляемые части. Функции могут принимать аргументы, выполнять операции над ними и возвращать результат. Функции могут быть вложенными, рекурсивными или вызываться из других функций.

ТАБЛИЦА 1. Различие ООП и ФП

ООП	ФП
Работает с данными и классами	Работает с функциями и алгоритмами
Имеет свойство наследования, что упрощает написание однотипных несложных алгоритмов	Не имеет свойства наследования, в результате чего каждая функция прописывается отдельно и вызывается в случае необходимости
Быстро выполняет задачи с минимальным количеством кода	Выполняет задачи медленнее, требуется больше кода
Используется для работы с большими системами с несложными задачами	Используется для специализированных сложных задач и алгоритмов
В силу наследственности гораздо проще поддерживать и изменять нужные алгоритмы	Из-за большого количества кода сложнее поддерживать и изменять алгоритмы

В первую очередь, очевидно, выбор того или иного вида программирования зависит от задач, которые стоят перед кодером.

Благодаря своим отличительным чертам, ООП по большей части подходит для написания сложных и комплексных систем, в которых многие задачи похожи и для того, чтобы не усложнять код большим количеством функций, которые будут постоянно вызывать друг друга в случае надобности, гораздо быстрее, проще и функциональнее будет использовать ООП, в силу возможности Инкапсуляции и наследования [4].

С другой стороны, функциональное программирование, в силу более тонкой настройки и возможности написания сложных алгоритмов, зачастую используется для проверки навыков программистов, кроме того этот вид

программирования по большей части используется для научно-технических вычислений и веб разработки. Также функциональное программирование подходит для обработки больших данных, а благодаря открытости кода функциональное программирование гораздо проще тестировать, так как весь код находится перед человеком.

Несмотря на то, что каждое из этих направлений имеет свои преимущества и используется в разных сферах, зачастую они пересекаются. По сути, каждый тип объекта в Python принадлежит своему классу, таким образом для каждого из них существуют определенные методы, которые применяются в функциональном программировании и наоборот, метод класса, который создает кодер, представляет собой функцию [5].

И все же если рассматривать конкретный код, то сразу понятно, ООП это или функциональное программирование.

Разработчику следует знать и уметь применять оба метода программирования, ООП используется для написания больших систем с не сложными алгоритмами, а ФП для небольших систем с сложными алгоритмами. Для большинства задач подойдут оба способа, но в силу простоты и быстроты в современном мире по большей части при программировании на Python используется именно ООП, который в случае крайней необходимости дополняется небольшим количеством алгоритмов, прописанных внутри класса.

Список используемых источников

1. Аль-Нами Б. А., Губин Ю. М. Вредоносное программное обеспечение // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-технической и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 117–120.

2. Аль-Нами Б. А., Волков И. Р. Использование информационных технологий в автоматизации процессов производства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 97–99.

3. Аль-Нами Б. А., Сидорова С. М., Чупрова А. Ю. Перспективы применения искусственного интеллекта в разработке программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 231–235.

4. Лутц М. Программирование на Python. СПб.: Символ-Плюс, 2015. 1131 с.

5. Саммерфилд М. Программирование на Python 3. Подробное руководство. СПб.: Символ-Плюс, 2017. 604 с.

УДК 004.945.5
ГРНТИ 50.13.15

ОСНОВЫ СОВРЕМЕННОЙ КОНТЕЙНЕРИЗАЦИИ

Б. А. Аль-Нами, М. А. Тужикова

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

С развитием информационных технологий и разработки программного обеспечения, ростом числа программ и их объёма возникла потребность в некотором инструменте, который позволил бы быстро и легко развертывать программы на различных устройствах и операционных системах. Нужен помощник, который упростил бы процесс создания среды, в которой будут учтены все зависимости приложения, и в которой оно сможет без проблем запуститься, что конечно же очень сильно облегчит жизнь программистам.

контейнеризация, разработка, данные, приложений, управление, ресурс, мониторинг, показатели

Контейнеризация стала ключевым инструментом для разработки и развёртывания приложений. Её суть – упаковывания приложения вместе с его зависимостями в так называемые контейнеры, обеспечивая изоляцию и стандартизацию окружения. Контейнеризация - методология упаковки, переноса и запуска приложений с их зависимостями в изолированном контейнере. В современной разработке ПО контейнеризация играет ключевую роль [1].

Ключевые особенности контейнеризации:

– •Полное отделение

При контейнеризации используются функции операционной системы для создания изолированной среды, в которой функционируют контейнеры. Изоляция гарантирует, что контейнер имеет доступ только к своим собственным локальным ресурсам и не имеет возможности взаимодействовать с другими контейнерами или с самой хост-системой.

– •Docker-образы

Контейнер создается из Docker-образа, содержащего в себе:

– 1. Сам код приложения

– 2. Зависимости приложения

Образы строятся на основе Docker-файла, который определяет структуру и зависимости приложения.

– •Управление ресурсами:

Контейнеризация предоставляет средства для управления ресурсами, такими как время и память, что способствует стабильной и оптимизированной работе приложения.

– •Управление множеством контейнеров:

Существуют специальные системы для управления размещением, масштабированием и контролем состояния сразу нескольких контейнеров, например Kubernetes.

– •Пример использования:

Простым примером контейнеризации является работа с Docker для создания и запуска веб-серверов, десктопных приложений, баз данных. Контейнер содержит в себе всю необходимую информацию для настройки окружения приложения, необходимого для его корректной работы, так что приложение может успешно развёртываться на любой хост-системе.

Преимущества контейнеризации:

– •Портируемость: Контейнеры способны запускаться на различных платформах, где установлен соответствующий контейнерный движок.

– •Изолированность: Каждый контейнер обладает своим отдельным изолированным окружением, что предотвращает возможные конфликты между зависимостями различных приложений.

– •Эффективное использование ресурсов: Использование контейнеров позволяет оптимизировать использование ресурсов хост-системы и избегать трудностей при масштабировании приложения.

Технологии контейнеризации:

– •Docker – одна из самых популярных платформ для контейнеризации, позволяющая упаковывать приложения и их зависимости в контейнеры.

– •Kubernetes – инструмент для оркестрации контейнеризированных приложений – автоматизации их развертывания, масштабирования и координации в условиях кластера [2].

– •OpenShift – это надстройка над Kubernetes, предлагающая дополнительные функции.

В Таблице 1. краткое сравнение показывает общие различия между Docker, Kubernetes и Openshift. Каждый из них обладает своими оригинальными характеристиками, и подходит для разных сценариев использования (рис. 1).

ТАБЛИЦА 1. Сравнение Docker, Kubernetes и Openshift

Критерий	Docker	Kubernetes	Openshift
Оркестрация	Ограниченная встроенная оркестрация.	Полнофункциональная оркестрация контейнеров	Интегрированная платформа управления
Масштабирование	Предоставляет базовые средства масштабирования	Официально поддерживает масштабирование	Встроенные средства автомасштабирования
Управление приложениями	Поддерживает управление приложениями	Официально поддерживает управление приложениями	Обширные возможности управления приложениями
Инструменты разработки	Обширный набор инструментов для разработки и развертывания контейнеров	Ориентирован на оркестрацию контейнеров, без покрытия разработки	Интегрированный набор инструментов для разработки, оркестрации и управления
Обучение и поддержка	Широкие ресурсы обучения и поддержки	Официальные курсы и консультационные услуги	Интегрированные ресурсы обучения и поддержки
Уровень абстракции	Низкий уровень абстракции, предназначен для инструментов разработчика	Высокий уровень абстракции, предназначен для DevOps	Золотая середина, охватывает обе данные области
Применение	Инструмент разработчика и системного администратора	Основной акцент на инструментах DevOps	Комбинирует разработчика, DevOps и администратора систем

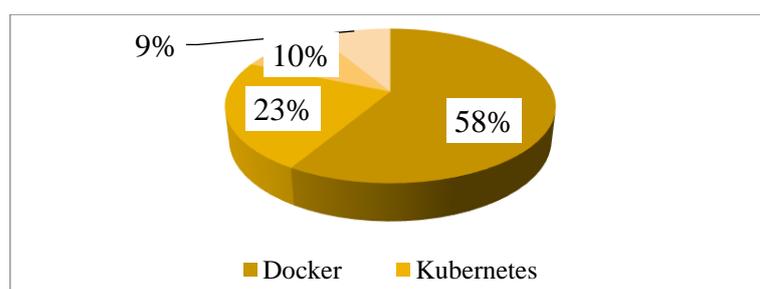


Рис. 1. Сравнение Docker, Kubernetes, Openshift и других по использованию

Мониторинг контейнеров:

- •Инструменты мониторинга

Существует множество инструментов мониторинга, специально разработанных для отслеживания контейнерных сред. Некоторые популярные инструменты включают:

– 1. Prometheus – система мониторинга и уведомлений с открытым исходным кодом, специально разработанная для отслеживания показателей и сбора данных в распределенных системах.

– 2. Grafana – платформа визуализации данных с открытым исходным кодом, которая предоставляет возможности мониторинга, визуализации и предупреждения.

– 3. Datadog – облачная платформа мониторинга и аналитики, специализирующаяся на мониторинге показателей, просмотре журналов и сборе следов запросов.

4. ELK Stack (Elasticsearch, Logstash, Kibana) – предоставляет набор инструментов для сбора, обработки, хранения и визуализации данных. Elasticsearch используется для хранения и анализа данных, Logstash – для сбора и обработки данных, а Kibana – для визуализации данных [3].

• Отслеживание производительности:

1. Мониторинг ресурсов контейнера:

– Отслеживание использования ресурсов процессора, памяти и сети контейнеров.

– Выявление узких мест в производительности и неэффективных процессов.

2. Отслеживание изображений и контейнеров:

– Мониторинг использования изображений и рабочих контейнеров.

– Оценка структуры и распределения контейнеров для оптимизации.

3. Сбор метрик и логов:

– Сбор данных о работе приложений и систем с использованием логов и метрик.

– Оптимизация производительности на основе собранных данных и тенденций.

• Проектное управление:

1. Оповещения и аварийные сигналы

Настройка оповещений для реагирования на проблемы с производительностью или нештатные ситуации.

Интеграция с системами уведомлений для быстрого реагирования на проблемы.

2. Анализ производительности

Использование показателей для анализа производительности и выявления тенденций.

Принятие решений на основе данных о производительности для повышения производительности системы.

• Безопасность контейнеров:

1. Мониторинг безопасности

– Отслеживание недостатков безопасности, взломов, аномального поведения и других безопасностных аспектов в контейнерах.

2. Обнаружение и реакция на инциденты

– Обнаружение и реагирование на угрозы, в том числе автоматизированные реакции на безопасность.

Чрезвычайно важно правильно настроить мониторинг контейнеров, чтобы иметь всестороннее представление о их производительности, безопасности и сбоев в реальном времени [4,5].

Заключение

Контейнеризация является мощным средством для создания, развертывания и управления приложениями. С ее помощью облегчается разработка и управление приложениями в различных средах. Контейнеризация представляет собой метод виртуализации операционной системы, который позволяет упаковывать и развертывать приложения, включая все их зависимости (такие как библиотеки и прочие нужные компоненты), в контейнер. Контейнер включает в себя все необходимое для запуска приложения: код, среду выполнения, системные инструменты, библиотеки и настройки.

Вышеприведенная информация максимально раскрыла основы контейнеризации и ее важность в современной разработке программного обеспечения.

Список используемых источников

1. Аль-Нами Б. А., Сайтчина А. В. Использование виртуальных собеседников для автоматизации и оптимизации работы с клиентами // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 218–223.

2. Аль-Нами Б. А., Баскова А. А., Васенькова А. А. Автоматизированные информационные технологии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 50–52.

3. Погодин В. А., Кузнецов А. Л., Серова И. В. Контейнеризация: история и тенденции // Контейнерный Бизнес. 2005. № 2 (2).

4. Аль-Нами Б. А., Бурков А. Д., Слепцов А. К. Современные информационные технологии и безопасность информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 79–84.

5. Аль-Нами Б. А., Рябинина С. А. Обеспечения компьютерной безопасности в коммерческой организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 214–218.

УДК 721.012
ГРНТИ 67.23.03

**ВЫБОР ПРОГРАММЫ ДЛЯ ВЫПУСКНИКОВ
ПРОГРАММЫ БАКАЛАВРИАТА ПО ПРОФЕССИИ
ИНЖЕНЕР – ПРОЕКТИРОВЩИК.
РУКОВОДСТВО ПО ИСПОЛЬЗОВАНИЮ
GEORECOUNTER**

Б. А. Аль-Нами, Д. Д. Цыганова

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

Многие выпускники программы бакалавриата сталкиваются с проблемой освоения новых программ, которые могут упростить их работу в сфере инженерии и проектирования. Данная статья поможет им ознакомиться с программой для будущих инженеров – проектировщиков и продемонстрирует ее функционал, а также мы рассмотрим пример ее работы на одной из самых популярных систем автоматизированного проектирования и черчения – Automated Computer Aided Drafting and Design - проектирование с помощью компьютерных технологий.

проектирование, Automated Computer Aided Drafting and Design, AutoCAD, инженер, черчение

Работая инженером или в любой другой сфере, человеку важно использовать программы, которые значительно упростят выполнение повторных действий (оформление, вставка таблиц, подписей или условных обозначений). Одной из таких программ является GeoRecounter. Данная программа предназначена для облегчения работы с чертежами, обработки результатов информации [1]. Она позволяет работать с геоданными, растровыми файлами, помогает работать с базой данных Росреестра (рис.1). Также любой пользователь имеет возможность пополнять библиотеку чертежей как своими чертежами, которые используются для его работы, так и использовать уже встроенную в программу [2].

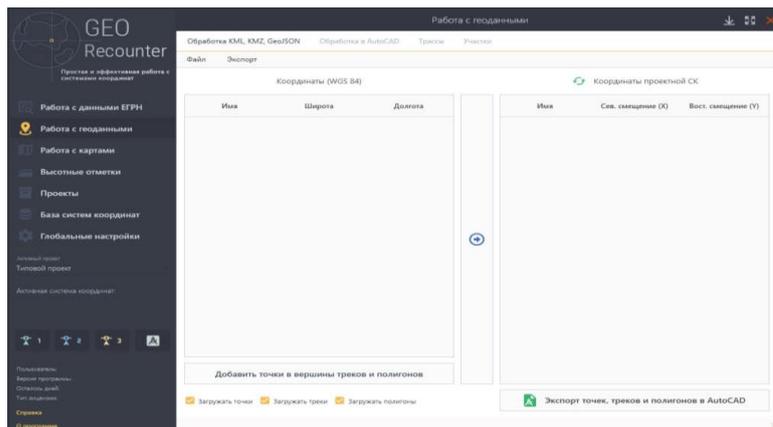


Рис. 1. Пользовательский интерфейс GeoRecounter

Сегодня мы рассмотрим функционал такой библиотеке и попробуем создать свои чертежи, протестируем их привязку к AutoCAD.

Для начала нам нужно иметь саму программу AutoCAD, у нас версия 2021 года, и GeoRecounter, ее можно скачать на пробный период на официальном сайте (<https://georecounter.ru/>)

Один из самых повторяющихся символов при создании документации или других документов – это подпись. Сейчас мы покажем, как ее добавить в библиотеку чертежей [3].

1. Воспроизведите свою подпись на бумаге и конвертируйте ее в файл формата Portable Document Format (PDF).

2. С помощью верхней панели AutoCAD в разделе вставка найдете «импорт PDF», рис. 2.

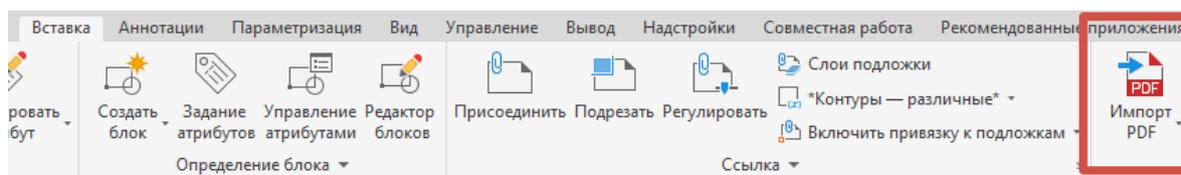


Рис. 2. Верхняя панель AutoCAD в разделе Вставка

3. Используя инструмент «полилиния» в верхней панели раздела «Главная», нарисуйте контур (рис. 3, 4).

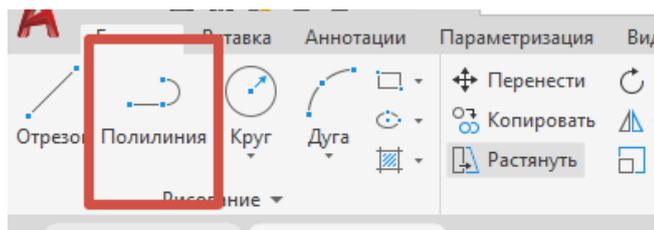


Рис. 3. Главная панель AutoCAD

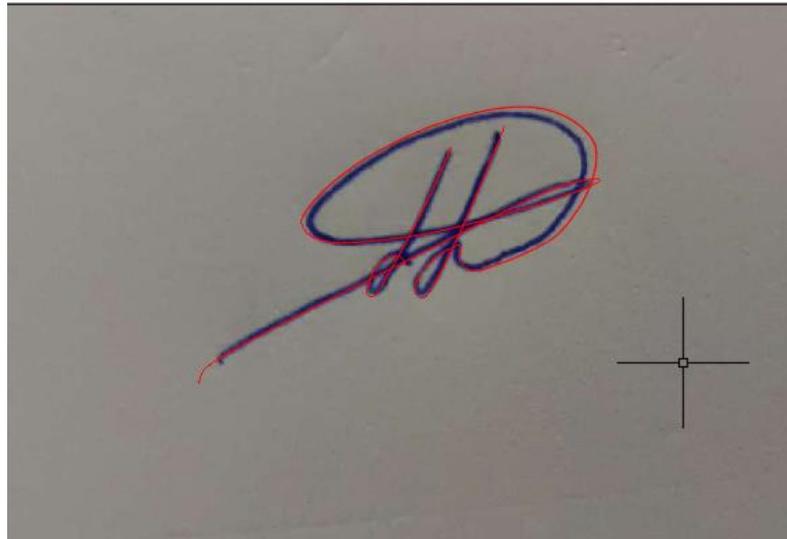


Рис. 4. Воспроизведение подписи

4. Сохраните свой чертеж в отдельной папке, которую в дальнейшем будете использовать для библиотеки (рис. 5).

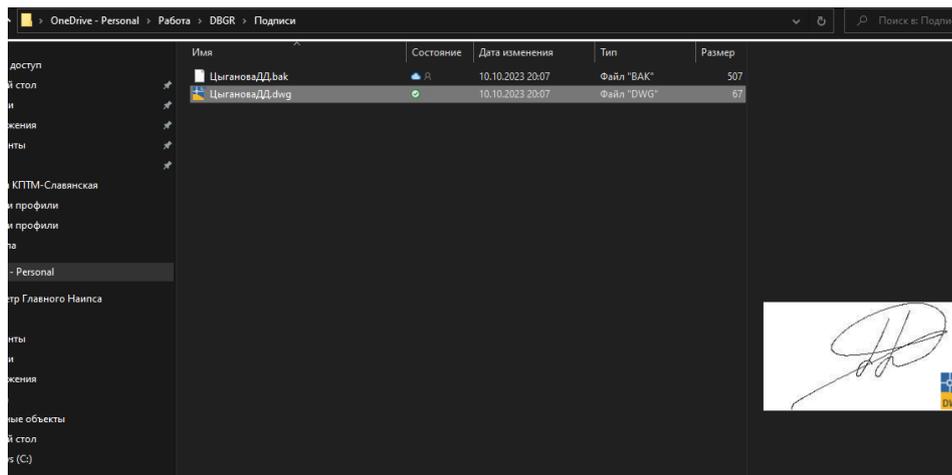


Рис. 5. Интерфейс папки сохранения

5. В GeoRecounter заходим в раздел «библиотека чертежей», внизу находим строку «путь к папке» и вставляем путь, где находится наша подпись (рис. 6).

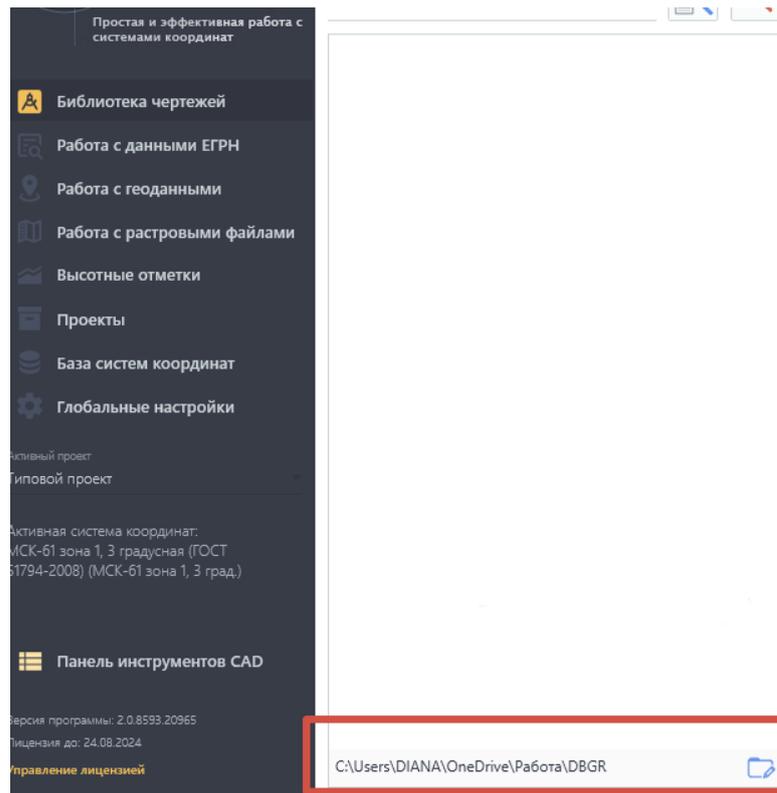


Рис. 6. Интерфейс программы Georecounter, установка пути сохранения

6. Выполняем проверку работоспособности (рис.7-9).

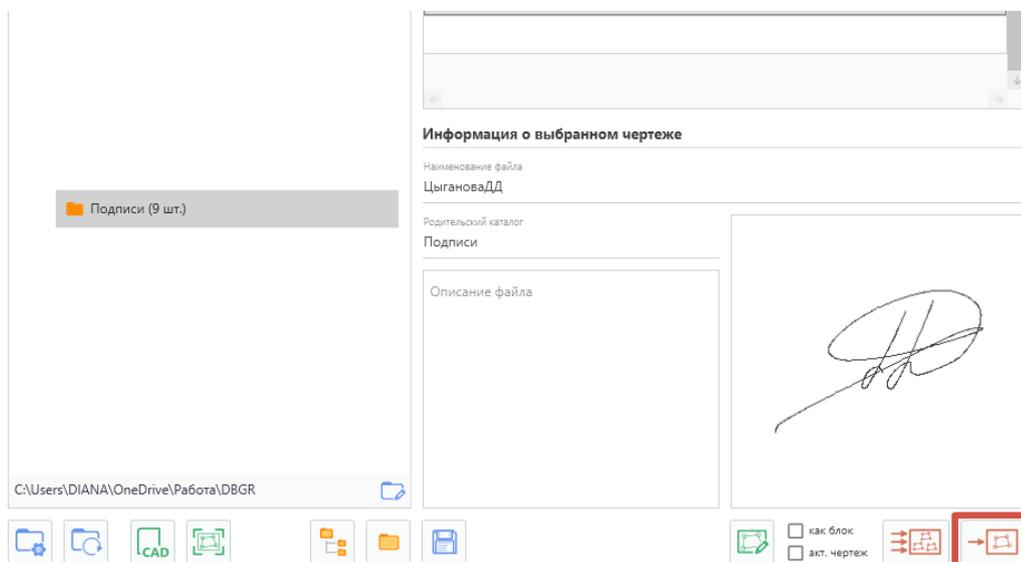


Рис. 7. Интерфейс программы Georecounter – выбор созданного объекта

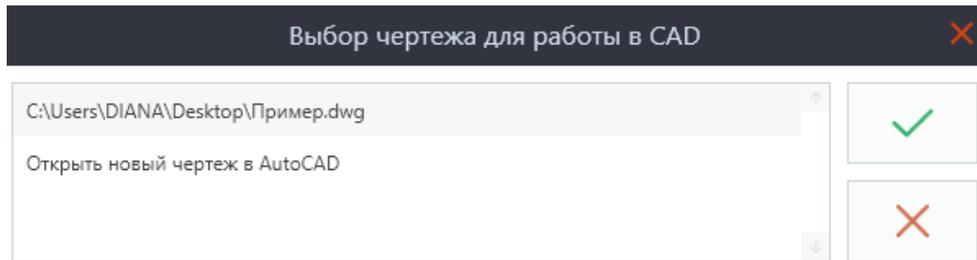


Рис. 8. Интерфейс программы Georecounter – выбор чертежа в AutoCAD

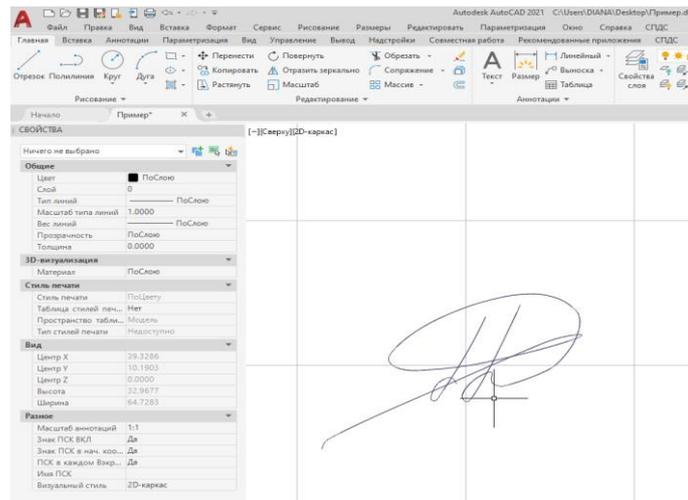


Рис. 9. Интерфейс программы AutoCAD – вставка созданного объекта

Моя библиотека чертежей в GeoRecounter (рис. 10).

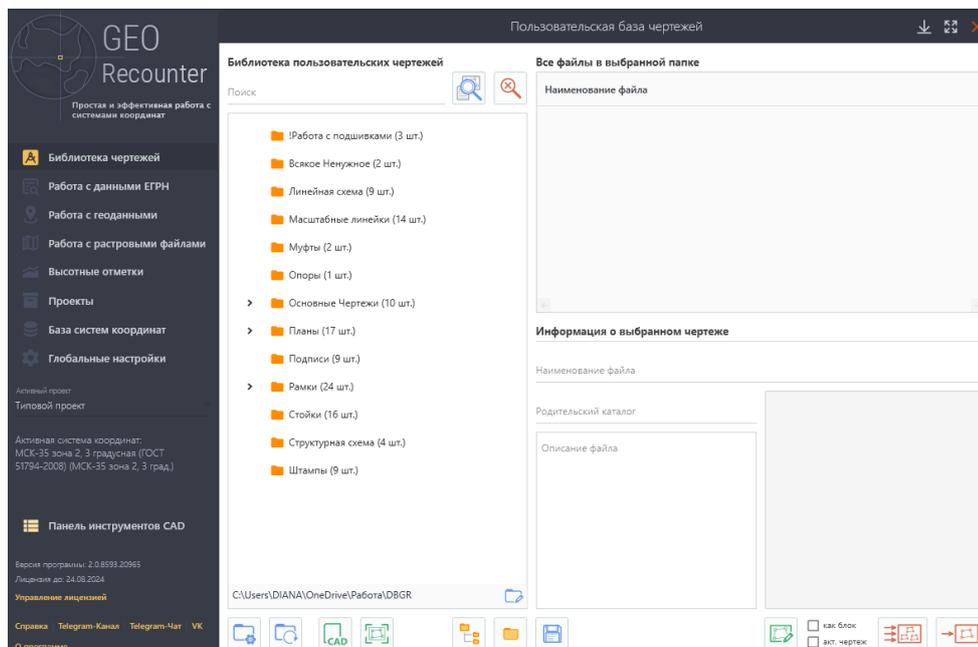


Рис. 10. Пользовательский интерфейс программы GeoRecounter

Следуя такому алгоритму, вы можете создать свои собственные чертежи, пополнять библиотеку и значительно сократить свою работу во время создания проектов [4].

GeoRecounter очень полезная программа как для начинающих инженеров, так и для людей, которые уже преуспели в данной профессии. Она подойдет не только для AutoCAD, но и для NanoCad, ZWCAD, BricsCAD.

Все, что вам нужно для пользования, это:

- • наличие персонального компьютера с установленной операционной системой Windows;
- • постоянный доступ к сети Интернет.
- • практические навыки оформления документации в среде AutoCAD, NanoCAD, ZWCAD, BricsCAD.

Используя данную программу, Вы значительно сокращаете время работы с чертежами, с геоданными и многим другим. С ней вы сможете показать свои навыки в работе инженера и добиться успеха!

Список используемых источников

1. Официальный сайт. URL: <https://georecounter.ru> (дата обращения: 03.01.2024)
2. Правила устройства электроустановок 7-е и 6-е издание. Нормативно-технический документ. 2022. С. 462
3. Гушул М. М. Справочник инженера производственно-технического отдела. 1985.
4. Руководящий документ отрасли. Состав исполнительной документации на законченные строительством линейные сооружения магистральных и внутризоновых ВОЛП. РД.45.156-2000. 2000 г.

УДК 004.056
ГРНТИ 81.93.29

КОНФИДЕНЦИАЛЬНОСТЬ ЛИЧНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Д. К. Апостолевский, А. Климов

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

Интернет стал неотъемлемой частью нашей жизни. Он предоставляет нам доступ к информации, помогает в учебе и работе, позволяет общаться с друзьями и близкими. Однако, помимо множества преимуществ, цифровой ландшафт представляет собой неизбежный риск для личной безопасности и защищенности.

В данной статье будут рассмотрены виды интернет-опасностей и методы борьбы с ними.

информационная безопасность, защита персональных данных, правовое регулирование, безопасный интернет, кибербуллинг, груминг, социальные сети

Защита себя в Интернете имеет первостепенное значение, учитывая распространенность киберугроз, утечек данных, онлайн-мошенничества и вторжений в частную жизнь. Защита личной информации и разумное использование онлайн-практик необходимы для обеспечения безопасного цифрового опыта.

Интернет-безопасность - защищенность от различных угроз, которые могут возникнуть при осуществлении деятельности и совершении операций в интернете. Она является составной частью более общих понятий, таких как кибербезопасность и компьютерная безопасность. Сюда входят вопросы безопасности браузера и интернет-соединения, а также правила поведения в Интернете. В процессе длительного пребывания в сети можно столкнуться с рядом угроз интернет-безопасности. Например, это несанкционированный доступ к компьютерным системам, электронным почтовым ящикам и веб-ресурсам (взлом), а также вирусы и вредоносный софт, способные привести к потере данных и сделать систему уязвимой для других угроз. Кроме того, существует риск кражи личных данных, включая личную и финансовую информацию, злоумышленниками [1].

Ключевые стратегии личной безопасности:

– 1. Конфиденциальность и защита личных данных.

Первое и самое важное правило – сохранение конфиденциальности Ваших личных данных. Никогда не публикуйте в Интернете личную информацию, такую как адрес, номер телефона, дату рождения, пароли и т.д. Если

вы используете социальные сети, установите настройки конфиденциальности так, чтобы ваши данные были видны только друзьям.

– 2. Безопасность электронной почты.

Соблюдайте осторожность при обнаружении нежелательных электронных писем, сообщений или всплывающих окон с запросом личной или финансовой информации. Попытки фишинга часто имитируют законные источники, стремясь обманом заставить пользователей раскрыть конфиденциальную информацию. Крайне важно проверять подлинность запросов и воздерживаться от перехода по подозрительным ссылкам или вложениям. Используйте двухфакторную аутентификацию для защиты вашего почтового ящика [2].

– 3. Укрепление паролей и аутентификации.

Надежные и уникальные пароли – первая линия защиты от несанкционированного доступа к личным учетным записям. Внедрение многофакторной аутентификации (MFA) еще больше повышает безопасность, требуя дополнительного этапа проверки, что значительно снижает риск несанкционированного доступа, даже если пароли скомпрометированы. Используйте сложные пароли, состоящие из букв, цифр и символов. Не используйте один и тот же пароль для разных аккаунтов. Регулярно меняйте пароли и делайте их уникальными для каждого аккаунта. Используйте менеджеры паролей для хранения и генерации паролей.

– 4. Настройки конфиденциальности и защита данных.

Просматривайте и настраивайте параметры конфиденциальности на платформах социальных сетей, в приложениях и онлайн-сервисах. Ограничьте объем личной информации, публикуемой публично, и регулярно проверяйте разрешения, предоставленные приложениям. Будьте осторожны при передаче конфиденциальных данных, таких как адреса, номера телефонов или финансовая информация, и раскрывайте эту информацию только на безопасных, авторитетных веб-сайтах. Помните о потенциальных последствиях публикации личной информации, сведений о местоположении или фотографий, поскольку эти данные могут быть использованы киберпреступниками или использованы для кражи личных данных.

– 5. Регулярные обновления программного обеспечения и меры безопасности.

Поддерживайте актуальность программного обеспечения, операционных систем и антивирусных программ. Обновления программного обеспечения часто включают исправления безопасности, устраняющие уязвимости, снижающие риск использования злоумышленниками.

– 6. Установите антивирусные программы.

Вирус – ПО, которое направлено на кражу ваших личных данных, включая банковские. Попасть на ваше устройство такое вредоносное ПО

может с разных сайтов и приложений. Сделать безопасными свои устройства и личную информацию можно, установив тот самый антивирус [3].

Недостаточно скачать любую программу и запустить. Необходимо также регулярно обновлять антивирус, так как разработчики вредоносного софта постоянно совершенствуют свои способы кражи данных и меняют их действие.

– 7. Важно заботиться о безопасности детей.

Так как дети часто лазают необдуманно по разным сайтам и многого не понимают, важно объяснить ребенку азы пользования Интернетом и безопасности в Интернете. Если ребенок слишком маленький, то можно установить родительский контроль или сторонние приложения, настроенные на ограничения пользования мобильного или компьютерного устройства.

Сколько же таких маленьких и больших, обманутых индивидов придутся на нашу страну? Для ответа на данный вопрос был проведен опрос и на его основе была выведена статистика, каково процентное соотношение обманутых людей, распределив их по возрасту:

Было опрошено 148 человек, из них 97 были подвергнуты обману в Интернете, из которых (рис. 1):

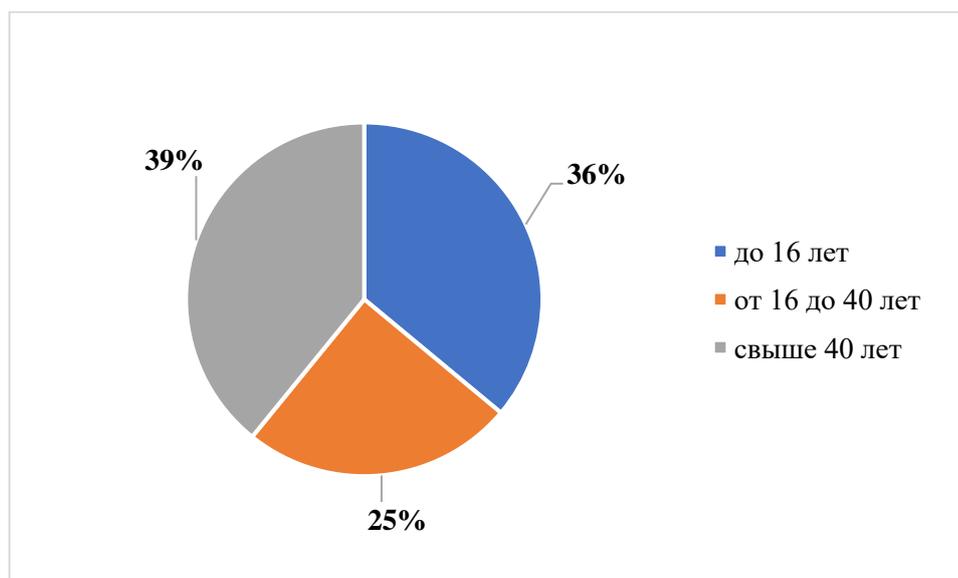


Рис. 1. Статистика мошенничества в России в 2023 году

Культивирование цифровой грамотности и расширение прав и возможностей:

Образование играет ключевую роль в повышении личной безопасности в Интернете. Продвижение цифровой грамотности дает людям возможность распознавать угрозы, принимать обоснованные решения и применять передовые методы обеспечения онлайн-безопасности. Обучение себя и других,

особенно детей и пожилых людей, которые могут быть более уязвимы к онлайн-рискам, имеет решающее значение для создания более безопасной цифровой среды [4].

Заключение

Интернет предлагает беспрецедентные возможности, но его среда требует бдительности и превентивных мер для обеспечения личной безопасности и защищенности. Применяя упреждающий подход, получая информацию о возникающих угрозах и внедряя надежные методы обеспечения безопасности, люди могут уверенно и безопасно перемещаться в цифровой сфере. Все требования невозможно выполнять, чтобы не попасть на кражу или слив своих информационных данных (и не только информации). В течение жизни можно наткнуться на множество афер или по неосторожности все же ошибиться, но выполняя базовые приемы осторожности, можно привести шанс обмана к минимуму.

Список используемых источников

1. Аль-Нами Б. А., Дубоусова Е. В. Актуальные проблемы обеспечения безопасности информационных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 124–128.

2. Аль-Нами Б. А., Ивашова М. М. Актуальность и угрозы информационной безопасности в современном мире // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 145–149.

3. Аль-Нами Б. А., Кравцов К. П., Тулин Я. А. Безопасность информационных систем: основные угрозы и методы решения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 164–168.

4. Аль-Нами Б. А., Омаров Э. Г. Защита персональных данных и законодательство о защите информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 192–195.

Статья представлена научным руководителем, кандидатом технических наук, старшим преподавателем кафедры ИКД Аль-Нами Б. А.

УДК 654.739
ГРНТИ 49.33.29

ОБЗОР АНАЛИЗОВ ДАТЧИКОВ УМНЫХ ДОМОВ

Н. М. Артамонов, Н. А. Васильев, Н. Л. Виткевич, А. С. Кустов

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

В данной статье описывается модель архитектуры Интернета вещей, а также проводится всестороннее сравнение различных систем умного дома, таких как технологии Google, Яндекса, Xiaomi и Apple, с акцентом на их функциональности, удобстве использования, интеграции с другими устройствами, а также аспектами безопасности и конфиденциальности данных. Через анализ основных характеристик и особенностей каждой системы, статья позволяет читателям получить полное представление о возможностях и ограничениях различных систем умного дома, помогая им сделать информированный выбор при планировании или модернизации своей домашней автоматизации.

машинное обучение, умный дом, технологии автоматизации, обработка информации, интеграция устройств, функциональность систем умного дома

На сегодняшний день умные дома становятся все более востребованными, предоставляя уникальные возможности для автоматизации и управления различными аспектами домашней жизни.

В таких системах ключевую роль играют датчики, собирающие информацию о состоянии окружающей среды, энергопотреблении и поведении пользователей. Однако с увеличением объема собираемых данных становится важным эффективное их обработка и анализ для принятия обоснованных и рациональных решений. Развитие технологий умного дома отражает стремление обеспечить более комфортное, эффективное и экологически устойчивое обитаемое пространство.

Сфера Интернета вещей представляет собой актуальное и стремительно растущее на данный момент направление развития информационных технологий. Согласно статистике, представленной *J'son & Partners Consulting* (рис. 1), с 2010 по 2020 год количество IoT-устройств увеличилось почти в 3 раза, а их общая стоимость почти в 4,5 раза, и эти цифры продолжают расти, что положительно сказывается на динамике развития данной сферы [1].

Согласно сектору стандартизации электросвязи Международного союза электросвязи (МСЭ), существует четырехуровневая модель архитектуры IoT, которая включает в себя следующие уровни: Уровень устройств, Уровень сети, Уровень обработки данных и Уровень приложений (рис. 2).

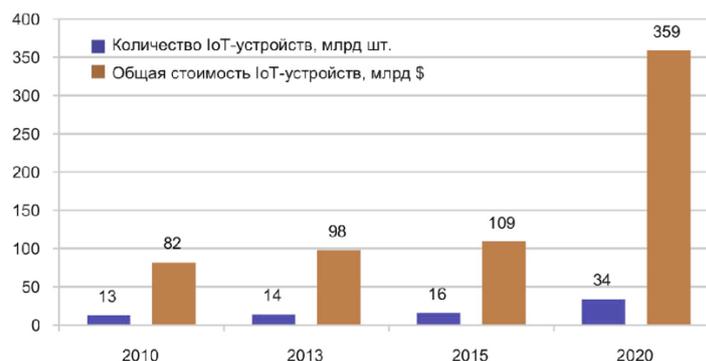


Рис. 1. График роста количества IoT-устройств в мире (по данным J'son & Partners Consulting)



Рис. 2. Четырехуровневая модель архитектуры IoT

На первом уровне находятся физические устройства IoT, такие как сенсоры, исполнительные устройства, встроенные системы и другие устройства, собирающие данные из окружающего мира. Элементы этого уровня обычно обладают собственными микропроцессорами, оперативной памятью и сетевыми интерфейсами для подключения к сети.

Второй уровень отвечает за передачу данных от устройств к облачным сервисам и обратно. Это может включать в себя различные технологии связи, включая проводные и беспроводные сети, мобильные сети, сети LPWAN (Low Power Wide Area Network), и другие.

Третий уровень представляет собой агрегирование, обработку, а также анализ входных данных. К ним относятся различные вычислительные ресурсы, которые отвечают за поддержку Интернета вещей – это различное ПО, облачные сервисы, серверные станции и так далее. На уровне приложений происходит обработка выходных данных с предыдущего уровня, благодаря которым выполняется обеспечение функциональных

механик конечного приложения. К ним относятся: системы аналитики, управления, приложения и другие различные системы и сервисы.

Также существует дополнительный пятый уровень – трансверсальный, который охватывает все вышеперечисленные уровни, а также отвечает за безопасность системы, управление и мониторинг. Трансверсальный уровень несёт в себе протоколы и методы идентификации, аутентификацию и авторизацию, защиту данных и контроль доступа [2].

Одним из крупнейших инноваторов в сфере умных домов является *Google*, который представляет возможность использовать уникальное, автоматизированное решение, позволяющее управлять домашней технологической средой. Компания *Google* представляет конечным пользователям удобный контроль интеллектуальных средств, которые улучшают комфорт пользователя, безопасность и повышение энергоэффективности повседневной жизни. Технологический гигант стремится обеспечивать инновационные решения для создания современного умного дома.

Компания *Apple* имеет свой взгляд на умный дом, который сочетает функциональность, эффективность и дизайн для достижения наилучшего комфорта в повседневной жизни. Она представляет интуитивно понятную и гармоничную интеграцию элементов умного дома в домашнюю среду. Основной фокус *Apple* состоит в сохранении приватности и безопасности конфиденциальных данных конечных пользователей. Это достигается за счет обработки данных с датчиков умных домов за счет уменьшения передачи данных через облачные сервисы, тем самым повышая защиту данных. Компания создала такие средства как *HomeKit* и *Siri*, которые оказывают помощь в обеспечении более удобного управления устройствами и сценариями. Технологический гигант ведёт активную разработку средств и систем для повышения качества управления умным домом, сохраняя при этом высокий уровень защиты персональных данных пользователей.

Яндекс – российский технологический гигант, который также взялся за сферу умных домов, компания представила передовые технологии для обеспечения удобства и автоматизации бытовых вопросов. Компанией был представлен голосовой помощник – Алиса, платформа – Яндекс.Станция и другие технологические устройства. Все представленные на рынке устройства компании повышают автоматизацию домашних процессов и создают оптимальные сценарии умного дома. Основная задача в данном направлении состоит в том, чтобы предоставлять пользователям доступные и интуитивно понятные решения для сферы умных домов. Также компания не забывает про меры обеспечения защиты и конфиденциальных данных пользователей, которые собираются с датчиков.

Свой умный дом представила также компания *Xiaomi*. Умный дом в представлении компании отображает технологичную инновационную си-

стему, которая позволяет осуществлять управление домашними устройствами при помощи мобильного программного обеспечения или голосовых команд. Домашний автоматизированный комплекс интегрирует в себя различные умные устройства, такие как освещение, отопление, безопасность, аудио-видео системы, а также датчики и умные замки.

Xiaomi использует комплексный подход при создании своих умных домов. Они предлагают широкий спектр умных устройств, которые интегрируются в одну общую экосистему, что обеспечивает полную автоматизацию и удобство в управлении домашними системами. Ключевыми подходами *Xiaomi* являются:

– 1. Интеграция: *Xiaomi* создает устройства, совместимые друг с другом и с легкостью интегрирующиеся в умный дом. Это позволяет пользователям контролировать все устройства через единую платформу или приложение с помощью смартфона.

– 2. Разнообразие: они предлагают широкий спектр умных устройств, включая умные лампы, умные датчики, умные замки, умные розетки и прочие. Это позволяет пользователям выбрать и настроить устройства под свои потребности и предпочтения.

– 3. Удобство использования: *Xiaomi* разрабатывает простые и интуитивно понятные интерфейсы для своих умных устройств, чтобы пользователи могли легко управлять ими и настраивать по своему усмотрению. Кроме того, многие устройства поддерживают голосовое управление, что делает управление домашними системами еще удобнее.

– 4. Качество и доступность: *Xiaomi* стремится предоставить высокое качество продуктов по доступной цене. Они используют передовые технологии и инновационные решения, чтобы сделать умный дом доступным для массового потребителя.

– В целом *Xiaomi* следует принципу создания умного дома, который легко управляется и настраивается пользователями, обеспечивая комфорт, безопасность и энергоэффективность в их домах.

Также помимо перечисленных компаний, существует также особый подход для умного дома, представленный в статье [3].

Подход, предлагаемый в статье, основывается на анализе данных систем умного дома. Весь анализ построен на использовании нейронных сетей *MobileNets*, которые представляют собой набор моделей компьютерного зрения.

В представленной статье, перед началом работы с датчиками, выполняется обучение с помощью репозитория *TensorFlow*. Всего проводится 10 этапов обучения. Для каждого из этапов случайным образом выбирается набор из 10 изображений, которые загружаются в конечный слой для получения прогнозов. Прогнозы впоследствии сравниваются с начальными обу-

чающими метками и, следовательно, обновляются методом обратного распространения. Идея алгоритма обратного распространения состоит в том, чтобы, основываясь на вычислении ошибки, возникшей в выходном слое нейронной сети, пересчитать значение весов последнего слоя нейронов и, таким образом, перейти к предыдущим слоям, от начала до конца, то есть обновить все веса слоев от последнего до достижения входного слоя сети, для этого выполняя обратное распространение ошибки, полученной сетью.

Однако в данном подходе представлено обучение всего по трем классам, что не позволило получить еще более высокую точность.

Вывод: умные дома представляют собой инновационную концепцию, которая все больше проникает в повседневную жизнь людей, обеспечивая комфорт, безопасность и эффективное использование ресурсов. Технологические компании, такие как *Google*, *Xiaomi*, *Apple* и *Яндекс* активно развивают и предлагают широкий спектр умных устройств, интегрируемых в единую экосистему, для создания умных домов. В умных домах пользователи могут управлять освещением, отоплением, безопасностью, развлечениями и другими системами через смартфон или голосовое управление, что делает жизнь более удобной и гибкой.

Одной из ключевых преимуществ умных домов является их способность оптимизировать использование ресурсов, таких как энергия и вода, позволяя сократить расходы и внести вклад в экологическую устойчивость. Несмотря на все преимущества, умные дома также представляют некоторые вызовы, связанные с приватностью данных и кибербезопасностью, поэтому важно обеспечить соответствующую защиту и безопасность систем.

В целом, описание умных домов демонстрирует их значимость в современном мире и перспективы использования этой технологии для создания комфортной, безопасной и эффективной домашней среды.

Список используемых источников

1. Json & Partners Consulting. Российский рынок межматематических коммуникаций и интернета вещей по итогам 2019 г. // URL: https://json.tv/ict_telecom_analytics_view/rossiyskiy-rynok-mejmashinnyh-kommunikatsiy-i-interneta-veschey-po-itogam-2019-goda-prognoz-do-2025-goda-20200717045903 (дата обращения: 17.12.2023)
2. Международный союз электросвязи. URL: <https://www.itu.int/rec/T-REC-Y.2060-201206-I> (дата обращения: 17.12.2023)
3. Саенко И. Б., Лаута О. С., Васильев Н. А., Садовников В. Е. Подход к эффективной обработке информации с датчиков системы умного дома при помощи методов машинного обучения // Международная научная конференция по проблемам управления в технических системах. 2023. Т. 1. С. 229–233.

Статья представлена начальником научно-исследовательского отдела научно-исследовательского центра Военной академии связи, кандидатом технических наук Тихоновым С. С.

УДК 004.832.28
ГРНТИ 05.35.29

СПОСОБ СЕТЕВОГО КОНТРОЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Н. М. Артамонов, В. А. Липатников, К. В. Мелехов

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

В данной статье исследуется вопрос разработки структуры средств сетевого контроля и выбора технологии нейронных сетей для построения средств сетевого контроля безопасности. Рассмотрены различные виды нейронных сетей и осуществлён выбор наиболее подходящей нейронной сети для сетевого контроля. Представленные в статье результаты исследования могут быть полезны для специалистов в области информационной безопасности и сетевых технологий.

средства сетевого контроля (ССК), информационно-телекоммуникационная сеть (ИТКС), нейронные сети

Актуальность. Назначение средств сетевого контроля (ССК) – это мониторинг, контроль безопасности компьютерных сетей и выявление кибератак (КА). ССК позволяют сетевым администраторам своевременно реагировать на угрозы безопасности и обеспечивать эффективное функционирование сетевой инфраструктуры.

Известны методы обеспечения необходимого уровня защищенности различных систем, например, способ управления безопасностью связи (БС) ИТКС путем реализации ложной сети на основе выделенного сервера с контейнерной виртуализацией [1]. Однако, в этой статье не в полной мере рассмотрены возможности автоматизации системы ССК за счет нейронных сетей.

Известен способ контроля уязвимостей при масштабировании автоматизированных систем менеджмента организации интегрированной структуры, который заключается в том, что управление БС основано на выявлении уязвимостей [2]. В данной статье рассмотренный способ не в полной мере подстраивается под текущие тенденции развития КА в современном мире. Использование этого метода не обеспечит повышение защищенности разрабатываемых систем.

В статье [3] недостаточное внимание уделено анализу динамики действий нарушителя, которые включают сценарии внешних и внутренних

вторжений. Возникает противоречие между эффективными новыми средствами информационного вторжения и существующими способами защиты ИТКС. Поэтому задача повышения защиты ИТКС путем построения средств сетевого контроля БС и защиты от вторжений со стороны нарушителей является актуальной.

При исследовании известных способов защиты ИТКС [4] не были рассмотрены способы прогнозирования вторжений на основе произошедших событий.

В статье [5] не в полной мере рассмотрены способы защиты ИТКС на основе прогнозирования вторжений.

В патенте [6] описывается способ защиты ИТКС от несанкционированных воздействий, который основывается на том, весь поток информации, обрабатываемый в сети, проходит проверку на наличие нарушений и в случае обнаружения уязвимости, администраторам сети посылается сигнал для принятия дальнейших решений. Однако, не рассматривается прогнозирование нарушений на основе нейронных сетей, что может значительно замедлить работу сетевых администраторов и ИТКС в целом.

Целью данной работы является повышение оперативности и достоверности выявления нарушений БС и обнаружений КА.

Объект исследования: ИТКС, функционирующих в условиях многоэтапных КА.

Предмет исследования: оперативность и достоверность обнаружения нарушений безопасности связи (БС) ИТКС.

Цель: Повышение оперативности и достоверности обнаружения нарушений БС и многоэтапных КА с учетом изменения состава применяемых КА повышенной сложности.

Задача: Разработка способа сетевого контроля БС путем применения нейронных сетей.

Решение: Структура ССК предлагается реализация на уровне сетевых устройств и программного обеспечения, обеспечивая контроль и управление доступом к ресурсам сети, мониторинг сетевого трафика, обнаружение и предотвращение угроз БС, а также управление сетевой инфраструктурой ССК представляют в виде комплекса аппаратно-программных устройств. Эта структура может быть реализована на уровне сетевых устройств, операционных систем, приложений и сервисов. На рис. 1 представлена схема расположения ССК в составе ИТКС.

Структурная схема ССК и прогнозирования КА представлена на рис. 2, где представлен процесс обработки цифрового потока (ЦП) через ССК, поступающего в ИТКС.

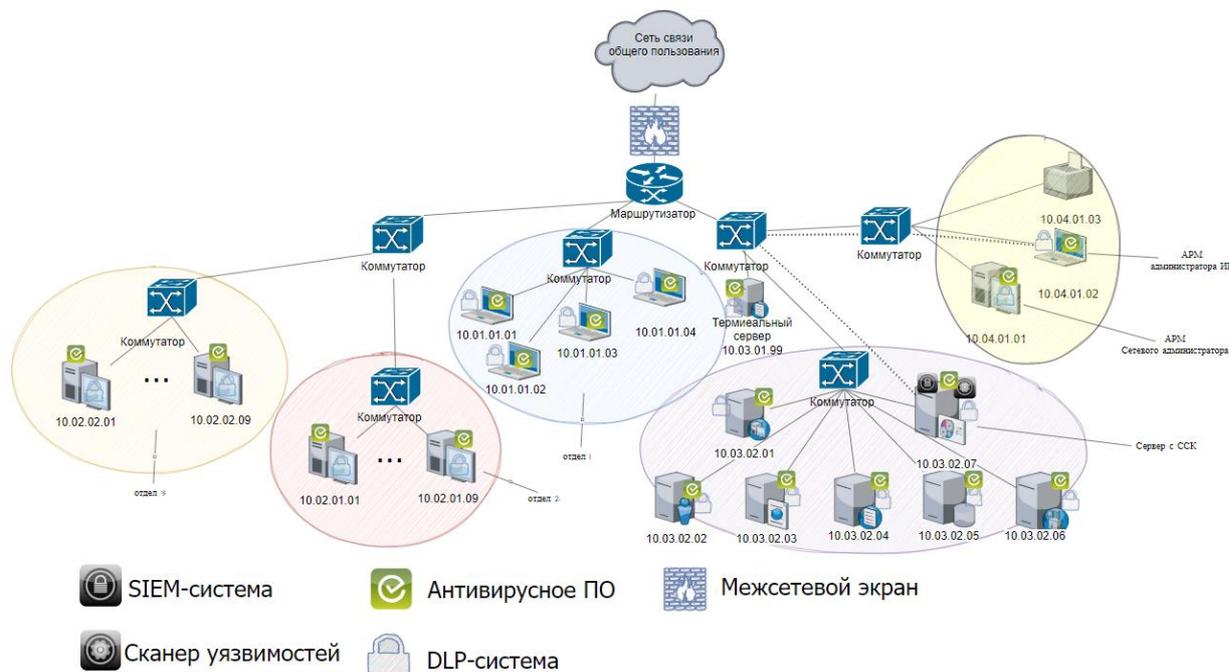


Рис. 1. ССК в составе СЗИ в ИТКС

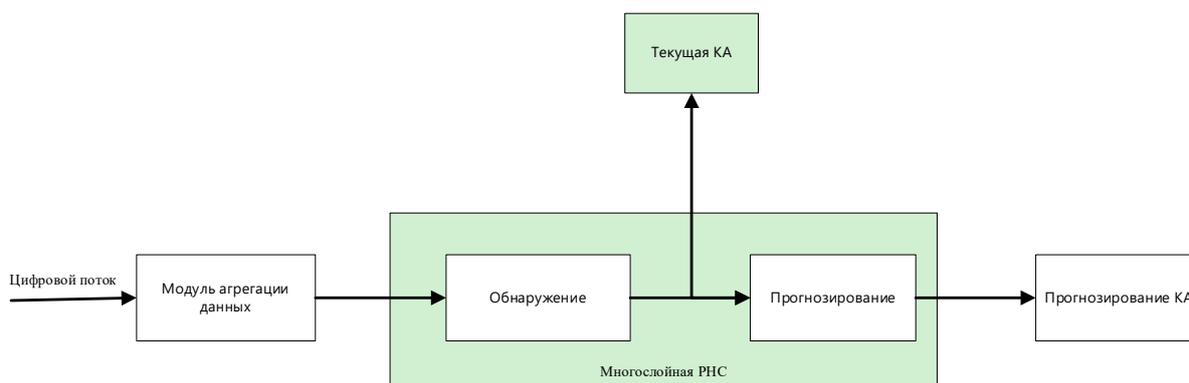


Рис. 2. Структурная схема ССК и прогнозирования КА

Алгоритм обработки ЦП (см. рис. 2):

– 1. Поступающий ЦП проходит через модуль агрегации данных, в котором выявляются общие тенденции и закономерности, а также формируется последовательность реализаций потока.

– 2. Затем агрегированные данные предоставляются многослойной РНС для обнаружения нарушений БС и многоэтапных КА.

– 3. В многослойной рекуррентной нейронной сети (РНС) на первом этапе выявляются текущие нарушения БС, если такое происходит, то выполняется оповещение администратором об угрозе КА и ожидание принятия решения администратором.

4. На втором этапе на основе истории уже обработанных ЦП, выполняется анализ и прогнозирование КА.

Структурная схема многослойной РНС представлена на рис. 3.

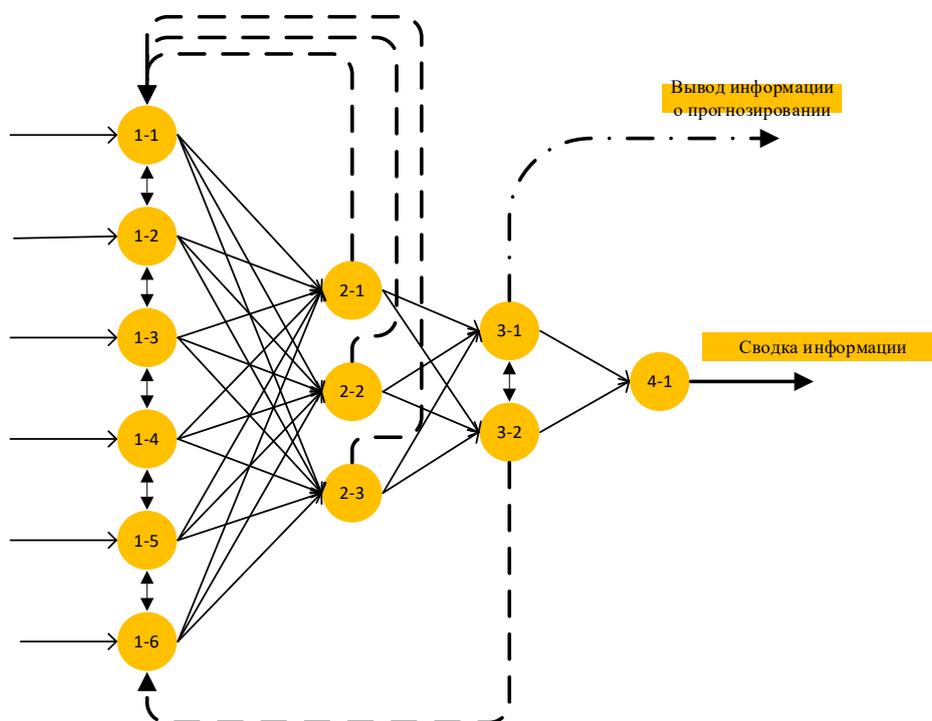


Рис. 3. Структурная схема многослойной РНС

В данной схеме представлено 3 слоя РНС.

Первый слой содержит элементы 1-1, 1-2, 1-3, 1-4, 1-5, 1-6. На вход данного слоя поступает нормированный ЦП.

Второй слой содержит элементы 2-1, 2-2, 2-3. На вход данного слоя поступает обработанная информация с первого слоя. Выходом с данного слоя является информация, передаваемая нейронам первого слоя для дальнейшего анализа и прогнозирования КА, также выходом является ЦП, в котором не обнаружены угрозы БС.

Третий слой содержит элементы 3-1 и 3-2. Он отвечает за вывод информации о прогнозировании, а также предоставляет информацию для четвертого слоя.

Четвертый слой содержит один элемент 4-1, задача которого заключается в формировании сводки информации о поступающем ЦП.

Алгоритм многослойной РНС представлен на рис. 4.

Описание алгоритма. После получения ЦП на вход многослойной РНС, он проверяется на наличие угроз информационной безопасности. Затем проверяется условие: если угроз нет, то это конец алгоритма, иначе предоставляется информация для администратора ИБ. За ним остаётся решение о том, что делать с данным цифровым потоком. После чего идёт про-

верка на устранение угрозы. Если угроза не устранена, то ЦП снова перенаправляется к администратору ИБ, если устранена, тогда происходит прогнозирование КА на основе ранее обнаруженных угроз ИБ. После прогнозирования атаки поступает вывод информации о том, что в скором времени прогнозируется атака на ИТКС. А также формируется информация о ЦП за отведённый период времени.

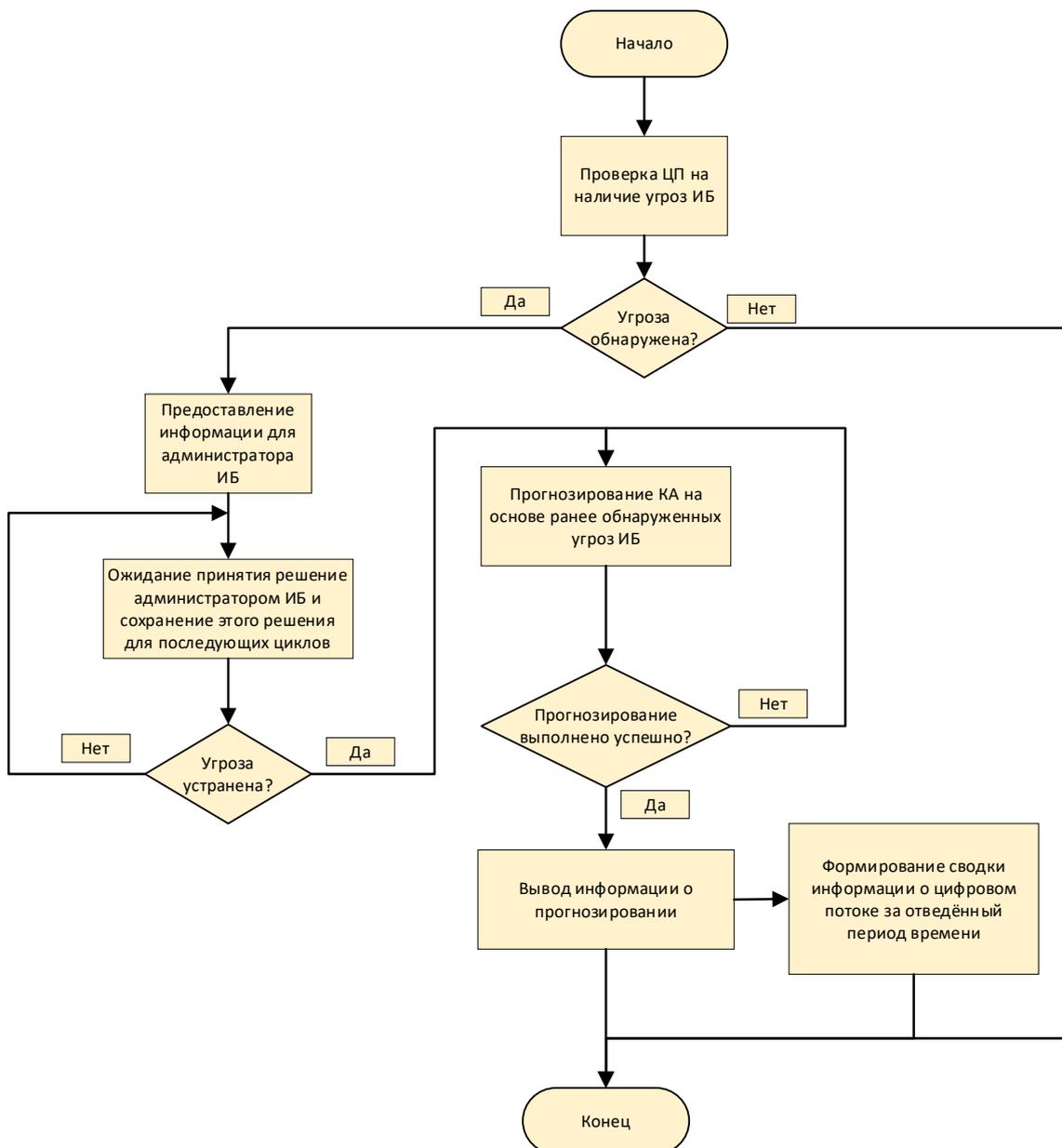


Рис. 4. Алгоритм работы многослойной РНС

Степень достижения цели обычно оценивается по уровню защиты информационных активов от угроз, уровню соответствия стандартам и законодательству, а также по уровню реагирования на инциденты безопасности.

Это может включать в себя оценку наличия и эффективности мер по предотвращению атак, защите конфиденциальной информации, а также системы обнаружения и реагирования на угрозы. Оценка степени достижения цели в БС помогает определить уровень рисков и защищенности ИТКС, а также принять меры для дальнейшего улучшения безопасности.

Новизна способа заключается в том, чтобы использовать РНС в ССК - это представляет собой новую и важную концепцию в области сетевых технологий. Использование РНС в средствах сетевого контроля открывает новые возможности для оптимизации управления сетевой инфраструктурой, обеспечивая автоматизацию процессов мониторинга, анализа и управления сетью. Применение способа может стать ключевым фактором в повышении эффективности сетевого управления и обеспечении более надежной работы ИТКС в целом.

Таким образом использование многослойной РНС для анализа и прогнозирования угроз БС в ИТКС позволит повысить оперативность и достоверность обнаружения нарушений безопасности связи и многоэтапных КА с учетом изменения состава применяемых многоэтапных КА повышенной сложности.

Список использованной литературы

1. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4. С. 67–76. DOI:10.15217/issn1684-8853.2017.4.67
2. 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.
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. Ivo Batina. Model Predictive Control for Stochastic Systems by Randomized Algorithms. Eindhoven: Technische Universiteit Eindhoven, 2004. 157 p.
5. Byres E., Lowe J. The Myths and Facts Behind Cyber Security Risk for Industrial Control Systems // ISA Process Control Conf., 2003. P. 1–6.
6. Липатников В. А., Чепелев К. В., Шевченко А. А. Способ защиты информационно-вычислительной сети от вторжений. Патент на изобретение RU 2705773 C1, 11.11.2019. Заявка № 2019100252 от 09.01.2019.

УДК 004.9
ГРНТИ 50.41.25

ПРОГРАММНОЕ ПРИЛОЖЕНИЕ ВИЗУАЛИЗАЦИИ МЕСТ ДЛЯ ПРОВЕДЕНИЯ ПЛЕНЭРОВ

А. А. Ахраменко, О. Б. Кузнецова

Мурманский арктический университет

Мероприятия пленэрной живописи демонстрируют рост заинтересованности среди населения в России. Широкий доступ к образованию и развитие творческих сообществ создают благоприятную среду для развития интереса к пленэру. Визуализация возможных мест для проведения пленэров на карте дают широчайшие возможности всем желающим запечатлеть места на открытом воздухе.

геоинформационное обеспечение, программное приложение, визуализация, пленэр, места проведения пленэров

В каждом уголке России есть чудесные и запоминающиеся своей красотой места, расположенные в городах и за их пределами. За границами помещений открывается множество зданий, памятников, мостов, смотровых площадок парков, аллей, рек и озер, богатое крупными и мелкими объектами, представляющие особую ценность для работы художника на открытом воздухе.

Художникам для совершенствования навыков необходимо постоянно заниматься практикой. Для живописцев, занимающихся пленэром, подобрать новое место тяжело, так как требуется потратить время на перемещение между местами и их оценку. Некоторые объекты для рисования могут удаляться на сотни километров, делая поиск практически невозможным [1].

Избавить от данных ограничений может сервис, предоставляющий карту мест для проведения пленэра. Такое решение даст пользователю возможность оставлять на карте метку с дополнительной информацией в виде фотографий и комментариев, формируя свой список из таких мест, которым можно поделиться с другими пользователями.

Целью работы является разработка и реализация приложения визуализации мест для проведения пленэров.

Приложение визуализации мест для проведения пленэров включает следующие задачи (рис. 1):

- обработка и хранение данных;
- картографическая визуализация информации.

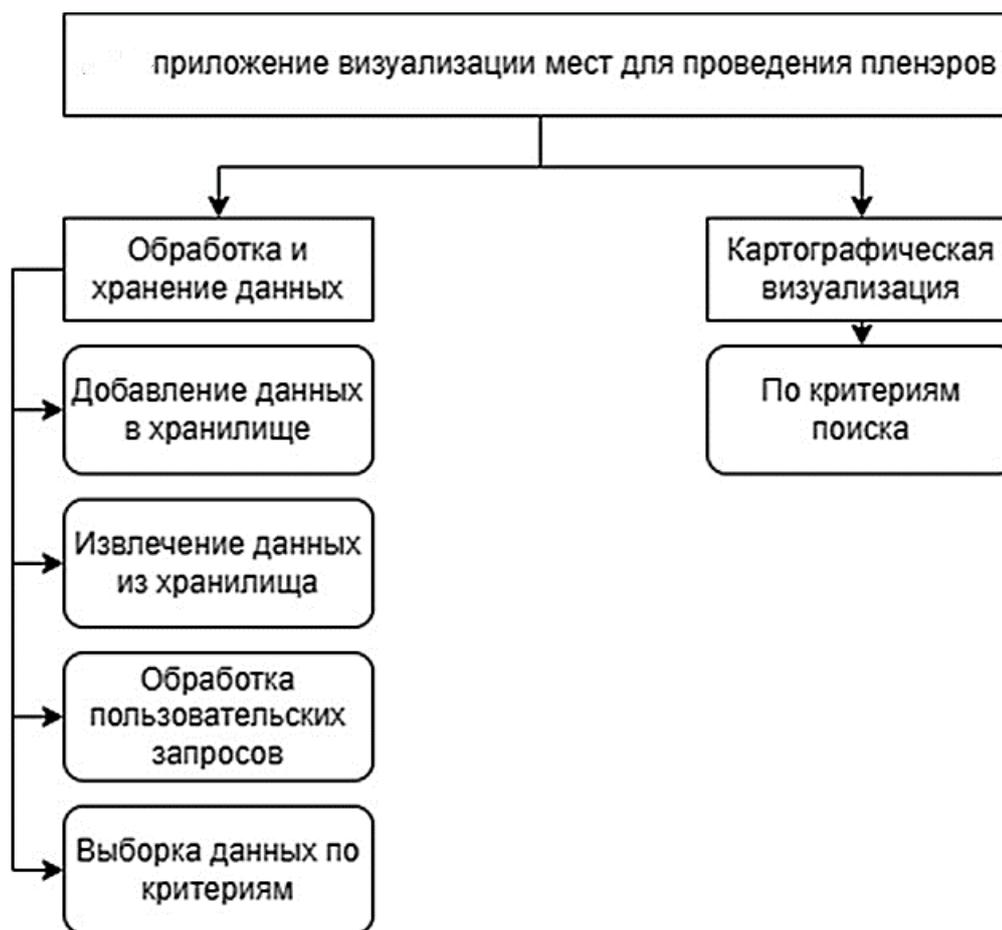


Рис. 1. Задачи приложения визуализации

Итогом решения поставленных задач является приложение, которое наделено следующим функционалом:

- авторизация пользователя;
- управление учетной записью;
- манипуляции данными мест для проведения пленэров;
- добавление комментариев.

Приложение с таким функционалом удовлетворит большинство требований пользователей, а также станет незаменимым помощником.

Рассмотрим работу приложения на контрольном примере. При его открытии пользователь попадает на домашнюю страницу (рис. 2), на которой находится список мест с их краткой информацией. На странице также отображается интерактивная карта, на которую нанесены метки, обозначающие местоположение мистических мест. Внизу находятся кнопки фильтрации мест по тегам и/или рейтингу, а также кнопка добавления нового мета для проведения пленэра.

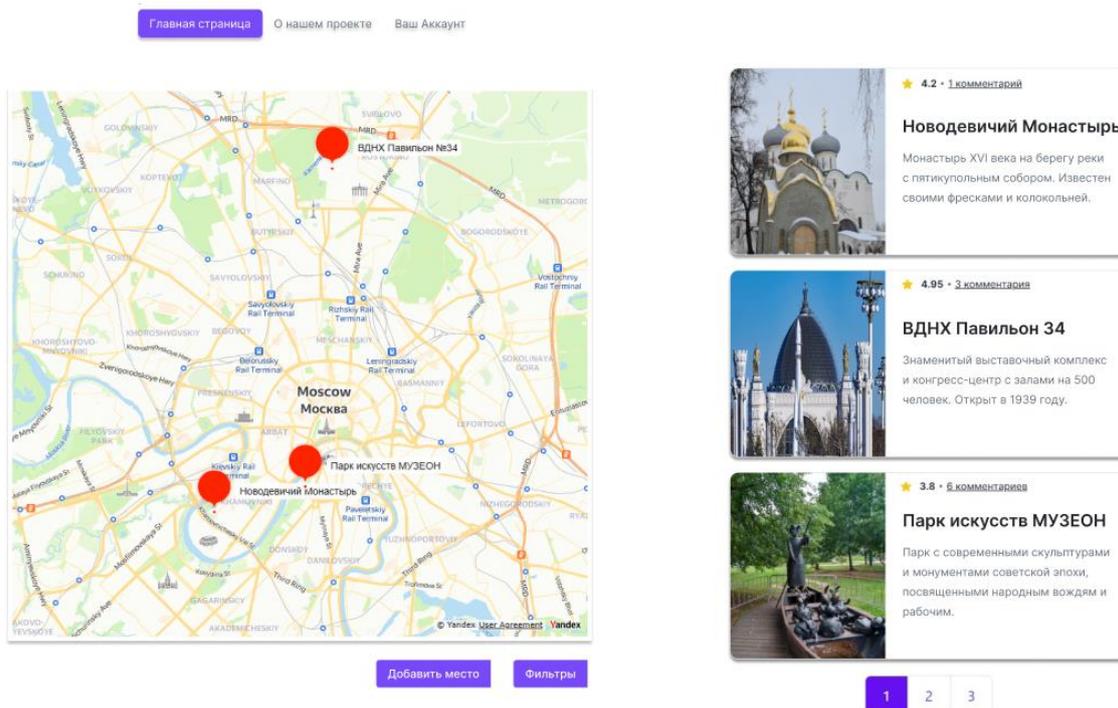


Рис. 2. Главная страница приложения

Нажав на карточку конкретного места, пользователь попадает на страницу детального просмотра (рис. 3), на которой он может получить информацию о заинтересовавшем его месте проведения пленэра: название, рейтинг, теги, детальное описание, как добраться, фотогалерею с фотографиями места, кто добавил место, список комментариев.

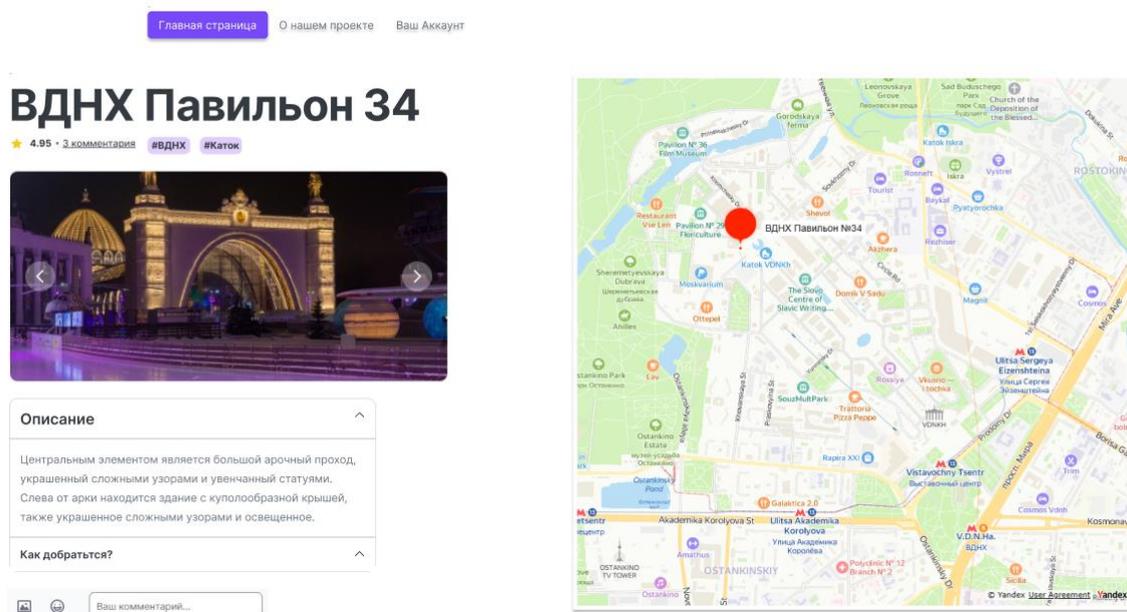
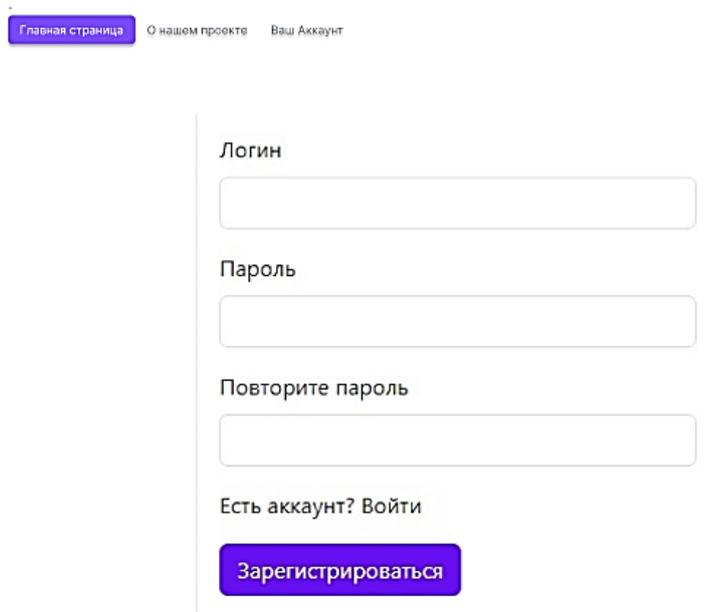


Рис. 3. Детальная страница просмотра

Для того, чтобы пользователь имел возможность добавлять места, оставлять комментарии, выставлять местам рейтинг, ему необходимо авторизоваться. Нажав кнопку «Ваш Аккаунт» в верхнем правом углу страницы, пользователь попадет на страницу авторизации, где ему будет предложено ввести логин и пароль от своего аккаунта.

Если пользователь не имеет аккаунта в приложении, со страницы авторизации он может попасть на страницу регистрации аккаунта (рис. 4), используя соответствующую гиперссылку. На странице регистрации пользователю будет необходимо придумать и ввести логин и пароль от своего аккаунта. Если пользователь с придуманным логином уже зарегистрирован в приложении, то будет выведена ошибка. После успешной регистрации пользователь вновь попадает на страницу авторизации, для того чтобы войти в зарегистрированный аккаунт.



The image shows a registration form with the following elements:

- Navigation links: [Главная страница](#), [О нашем проекте](#), [Ваш Аккаунт](#)
- Form fields:
 - Логин (Login)
 - Пароль (Password)
 - Повторите пароль (Repeat password)
- Text: [Есть аккаунт? Войти](#)
- Button: [Зарегистрироваться](#)

Рис. 4. Страница регистрации аккаунта

Авторизованные пользователи могут воспользоваться кнопкой «Добавить место», которая находится под интерактивной картой на главной странице приложения. При нажатии на кнопки сплывает модальное окно (рис. 5), на котором пользователю будет предложено ввести информацию о месте пленэра, а также отметить место на карте точкой. Обязательные для ввода поля помечены знаком «*». Пользователь также имеет возможность загружать фотографии места, которые после будут доступны на странице детального просмотра.

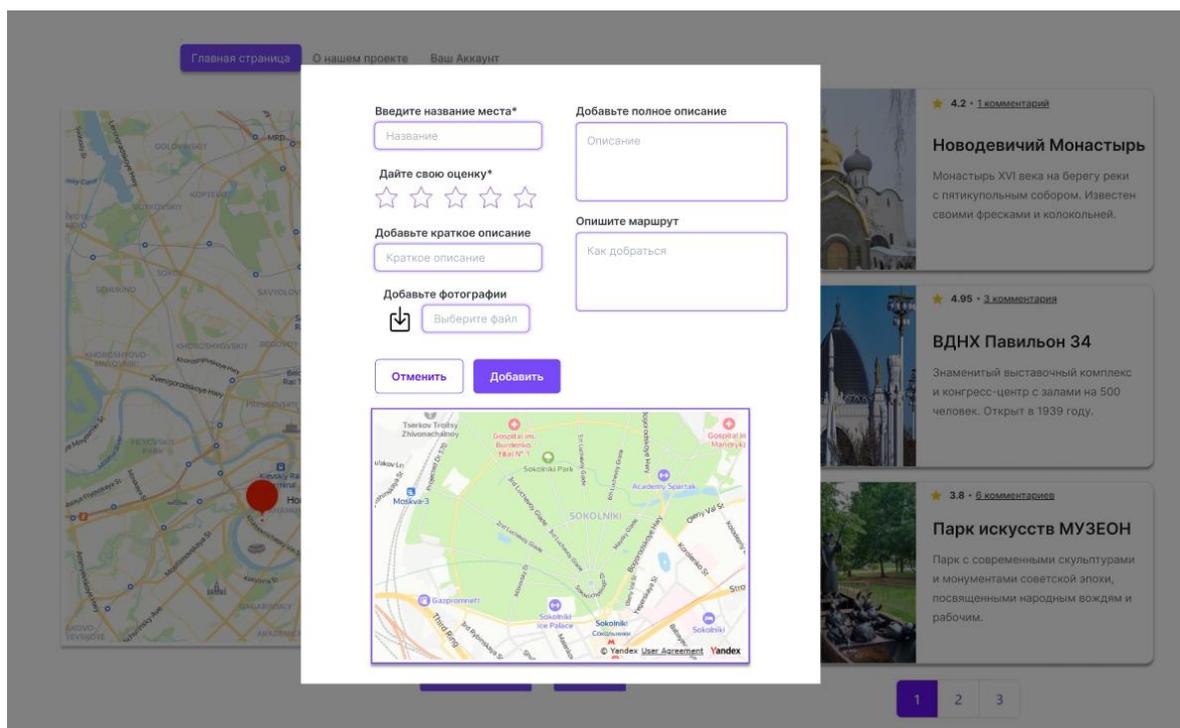


Рис. 5. Модальное окно добавления нового места на карту

Таким образом, можно констатировать, что цель работы достигнута. Результатом проделанной работы явилось приложение, которое позволяет на карте отображать места для проведения пленэров, что, безусловно, полезно не только художникам, но и всем желающим запечатлеть красивые места на открытом воздухе.

Список используемых источников

1. Пленэр – восхитительное и яркое искусство живописи на природе. URL: <https://veryimportantlot.com/ru/news/blog/plener> (дата обращения: 16.01.2024)

УДК 004.934.2
ГРНТИ 27.21.21

ГЕНЕРАЦИЯ АНИМАЦИИ МИМИКИ ДЛЯ ТРЕХМЕРНОЙ МОДЕЛИ С ИСПОЛЬЗОВАНИЕМ ВОКАЛЬНЫХ ДАННЫХ

Д. Д. Балакирев

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

Данная работа посвящена генерации анимации мимики для трёхмерной модели на основе вокальных данных. Идея анимации мимики не нова, но она требует аппаратные средства для отслеживания черт лица. Эта работа посвящена генерации мимики программным методом с задействованием искусственных нейронных сетей, что позволяет удешевить и упростить её создание. Это может быть использовано в киноиндустрии, видеоигровой индустрии, а также во время виртуальных конференций и стриминга с использованием виртуальных аватаров.

анимация, 3D, моделирование, трехмерная модель, нейросеть, нейронная сеть, генерация, синтез, мимика лица, аватар, видеоигровая индустрия, киноиндустрия, симуляция

Человечество практически на протяжении всего своего существования стремится воссоздать элементы реальности, в которой живет, будь то изображения, звук, тактильные ощущения. Наскальные рисунки, живопись, литература, песни или фильмы – все они в той или иной степени являются отражением мира, в котором мы живем. И с развитием компьютерных технологий люди добились возможности создания виртуальных миров с использованием компьютерной графики.

Компьютерную графику можно сделать реалистичной разными способами: воссоздать точное поведение световых лучей, сделать реалистичные модели реальных объектов и наделить их материал свойствами металличности, шероховатости и пористости для их реалистичной реакции на свет и прочие условия окружающей среды. Все они серьезно приближают изображение к реальности, но лишь в статике. Чтобы ощущения от визуальной составляющей были реалистичными, в нее необходимо вдохнуть жизнь, внести реалистичную анимацию.

Аnima в переводе с латинского означает слово «душа». Таким образом, прорабатывая анимацию трехмерной модели мы «одушевляем» ее, делаем реалистичнее и живее. И одним из элементов, которые чаще всего пытаются воплотить в виртуальном мире, является сам человек. Именно поэтому создание реалистичной анимации человека является очень важной задачей для приближения виртуального мира к реальному.

Анимирование трехмерной модели человека является комплексной и сложной задачей. И это неудивительно: одних лишь скелетных мышц насчитывают около 640 штук. В реальной жизни человек очень много внимания уделяет другим людям, а человеческое лицо для человека является сильным природным визуальным акцентом. Поэтому при воссоздании движений человека в виртуальном мире очень просто допустить оплошность, разрушив иллюзию неестественными движениями, которые быстро замечаются человеком, создавая эффект так называемой «зловещей долины».

Разработку анимации человека можно разбить на много разных подзадач, которые сами по себе могут быть довольно непросты: движения конечностей, их взаимодействие с окружающими объектами, влияние движения человека на положение ног в пространстве, напряжение разных групп мышц при определённых движениях. В данной научной статье рассматривается анимация мимических мышц и то, как на них влияет человеческая речь.

Анимирование мимики лица вручную – это очень трудоемкий и затратный по времени процесс, который может привести к недостоверному качеству. Для улучшения и упрощения этого процесса создали средства захвата движения. Захват осуществляется с помощью реального человека, но такой вариант требует дополнительного оборудования и может быть дорогостоящим. В качестве компромиссного варианта в данной работе рассматривается создание динамической анимации мимики в зависимости от речи человека.

Динамическая анимация, помимо упрощения и удешевления производства в киноиндустрии, может также использоваться в видеоигровой индустрии, симуляторах или виртуальных чатах / конференциях с использованием трехмерных аватаров. И в последнем случае, о ручном анимировании не может быть и речи, ведь полагаться приходится на действия конечного пользователя.

Сама по себе данная идея далеко не нова [1]. Существует множество реализаций движений рта в зависимости от услышанной речи: программные средства динамически конвертируют звук в набор фонем (минимально различимыми звуковыми единицами) [2], для которых заранее заготавливают положение мышц рта трехмерной модели, которые плавно сменяют друг друга, аппроксимируя позиции вершин меша между состояниями. Однако, эти системы касаются анимирования исключительно движения области губ и челюсти, не затрагивая другие мимические мышцы и аспект эмоций.

Идея, которая продвигается в этой работе – предсказание эмоций в речи человека с помощью искусственных нейронных сетей и создание динамики переключения состояний анимации лица на их основе.

В реализации этой идеи присутствуют следующие сложности:

– Различия голосов людей разного возраста, пола и рас. Разные люди звучат с разной высотой голоса. И при использовании частоты звука записи

их речи в качестве входного данного, можно столкнуться с тем, что эмоции будут определяться некорректно. Эту проблему можно решить эффектом памяти и динамического вычисления усредненного значения высоты голоса для конкретного человека, позволив системе адаптироваться и учитывать отклонения именно от этого значения.

– Наличие посторонних шумов. Посторонние шумы могут интерпретироваться системой как человеческая речь, в зависимости от которой могут возникать нежелательные анимации. К счастью, на данный момент уже существует множество хороших систем, которые удаляют посторонний шум в реальном времени, в том числе созданных на базе искусственного интеллекта, например, Krisp или RTX Voice.

– Неверная интерпретация эмоции. Разные люди испытывают их по-разному. Из-за этой проблемы к виртуальной трехмерной модели могут применяться не те мимические движения, которые на самом деле испытывает человек. Эту проблему можно решить с помощью объемного датасета для тренировки нейронной сети. Впрочем, это не такая и большая проблема, поскольку не так важно, чтобы анимации видел носитель голоса, сколько важно, чтобы они выглядели убедительно для окружающих или для конечного пользователя.

Для реализации предложенной в данной статье идеи, решено выделить следующие эмоции:

- радость;
- грусть;
- страх;
- гнев;
- смятение;
- презрение;
- отвращение.

Каждой из этих эмоций соответствует заранее заготовленное состояние лица трехмерной модели с выставленными в нужном положении вершинами модели. У каждого из состояний существует вес, который может колебаться от 0 до 1.0, где нижняя граница соответствует отсутствию конкретной эмоции, а верхняя граница – ее пику.

Таким образом, при считывании эмоции речи человека каждое из этих состояний одновременно может иметь разный вес, который меняется со временем в зависимости от речи. Благодаря этому могут визуализироваться смешанные эмоции, являющиеся промежуточными между активными состояниями. Это реализуется с помощью аппроксимации (усреднения) положения вершин разных состояний с зависимостью от их веса. При отсутствии речи каждая эмоция автоматически стремиться к нулю, возвращая лицо в нейтральное безэмоциональное состояние.

В некоторых работах отдельно выделяют нейтральную эмоцию, но в данной работе она выделена как отсутствие всех остальных эмоций, являясь состоянием по-умолчанию, что немного облегчает систему.

Аппроксимация положения вершин мышц лица в зависимости от состояния лица можно описать следующей формулой:

$$p = \frac{(\sum_{i=1}^7 e_i w_i) + e_n}{8},$$

где p – вектор позиции вершины лица, e – вектор заданной позиции вершины для состояния мимики лица, w – вес эмоции, соответствующий состоянию мимики, e_n – вектор заданной позиции вершины для нейтрального состояния лица.

Механизм считывания эмоций описан в научном труде «Нейросетевой подход к определению эмоций человека по речи» [3].

Список использованных источников

1. Корсун В. А. Генерация мимики и жестов по речи: дис. к-та техн. наук: 2.3.8 / Корсун Владислав Андреевич. М., 2022. 88 с.
2. Колесникова Д. С., Рудниченко А. К., Верещагина Е. А., Фоминова Е. Р. Применение современных технологий распознавания речи при создании лингвистического тренажера для повышения уровня языковой компетенции в сфере межкультурной коммуникации. Интернет-журнал «Наукovedение», 2017. Том 9. № 6. С. 1212. URL: <https://naukovedenie.ru/PDF/20TVN617.pdf> (дата обращения 30.03.2024)
3. Барышев Д. А., Макаревич И. В., Зубанков А. С., Розалиев В. Л. Нейросетевой подход к определению эмоций человека по речи. «Инженерный вестник Дона». 2022. № 5. С. 1–11. URL: <https://cyberleninka.ru/article/n/neyrosetevoy-podhod-k-opredeleniyu-emotsiy-cheloveka-po-rechi/viewer> (дата обращения 30.03.2024)

Статья представлена научным руководителем, заведующим кафедрой ИКД СПбГУТ, доктором технических наук, профессором Д. В. Волошиновым.

УДК 004.42:78.074
ГРНТИ 50.05.13

ФОРМИРОВАНИЕ МОДЕЛИ TELEGRAM-БОТА ДЛЯ ПОИСКА МУЗЫКАНТОВ И СОЗДАНИЯ КОЛЛАБОРАЦИЙ

С. Д. Балыбердин, И. Б. Бондаренко, А. О. Жаранова

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

Рассмотрен инновационный подход к организации музыкальных коллабораций с использованием Telegram-бота. Проведен анализ существующих сервисов для поиска музыкантов, выявлены их недостатки. Представлены основные алгоритмы для осуществления поиска и фильтрации данных. Описан алгоритм и способ вычисления метрики сходства для выдачи рекомендаций пользователю. Предложена модель информационной системы для поиска музыкантов и создания коллабораций. Приведен спектр технологических решений для будущей разработки.

рекомендательные алгоритмы, метрика сходства, рекомендательная система, Telegram-бот

В последние годы наблюдается рост интереса со стороны музыкальных сообществ к формированию разнообразных коллективов с целью создания инновационного звучания в музыкальной индустрии. Это ведет к возросшей потребности в новых жанрах и одновременно повышает сложность поиска соответствующего коллектива для каждого музыканта [1]. В связи с этим актуализируется вопрос разработки сервиса музыкальных коллабораций.

Предлагается инновационный подход к организации музыкальных коллабораций с помощью Telegram-бота, предоставляющего возможности для эффективного поиска соавторов в сфере музыкального искусства.

При выборе платформы для размещения подобного функционала стоит обратить внимание именно на Telegram из-за ряда преимуществ, таких как: популярность мессенджера; удобный и уже широко распространенный канал общения; мгновенные уведомления; поддержка высокого уровня безопасности и конфиденциальности; возможности автоматизации процессов с помощью встроенных алгоритмов Telegram-бота, которые способствуют эффективной фильтрации и категоризации информации, позволяют пользователям находить наиболее предпочтительных соавторов, что значительно сокращает время поиска подходящих музыкантов.

Проведен анализ существующих решений, направленных на поддержку и развитие музыкального сообщества:

– «BandLab» позволяет загружать, дорабатывать и совместно работать над музыкальными композициями независимо от местоположения;

– «SoundBetter» представляет собой платформу, где начинающие музыканты могут найти профессионалов из различных областей музыкальной индустрии для поддержки и сотрудничества;

– «Vampr» предлагает возможность знакомиться и вступать в сотрудничество через видеочаты для создания музыки и обмена идеями.

В ходе анализа конкурентоспособных систем выделены их недостатки относительно предлагаемого решения: необходимость загрузки и установки приложения; медленная и менее удобная навигация; отсутствие мгновенных уведомлений и обратной связи; большое количество шагов для регистрации и входа в систему; большое потребление ресурсов в случае реализации web-версии; языковые и культурные барьеры из-за ориентированности на мировую аудиторию; некоторые платформы взимают процент от каждой сделки музыкантов на платформе.

В результате анализа существующих решений выделены основные функции сервиса для поиска музыкантов и создания коллабораций:

- удобная регистрация в формате обмена сообщениями;
- указание собственных навыков и предпочтений;
- получение мгновенной обратной связи по заявкам на коллаборацию;
- отсутствие необходимости поиска контактов и перехода на сторонний сервис для связи;
- использование алгоритма рекомендаций для поиска коллаборантов.

При построении рекомендательной системы сервиса могут быть задействованы следующие методы и алгоритмы для осуществления поиска и фильтрации данных: коллаборативная фильтрация (collaborative filtering), контентная фильтрация (content-based), основанная на знаниях (knowledge-based) и гибридная фильтрация (hybrid).

Метод коллаборативной фильтрации использует данные о взаимодействиях и предпочтениях пользователей для предсказания того, что может понравиться новому пользователю, сравнивая его с другими, а также анализирует, какие события или характеристики профилей понравились одним пользователям для рекомендации данной информации другим [2]. Показывать хорошие рекомендации новым пользователям в рамках данного подхода не получится, ведь о них нет никакой информации.

Метод контентной фильтрации использует информацию о самих пользователях и их предпочтениях для выдачи рекомендаций. Не полагается на историю взаимодействий пользователей между собой, а анализирует содержание пользовательских профилей для выдачи подходящих объектов.

Метод фильтрации, основанной на знаниях, работает на основе знаний о предметной области: о пользователях, товарах и других данных, которые могут помочь в ранжировании. Однако определение качества предметов в предметной области может быть сложной задачей, что особенно актуально в сферах, где оценка субъективна, а критерии качества неоднозначны.

Метод гибридной фильтрации подразумевает комбинирование нескольких алгоритмов в рамках одной платформы с целью минимизации их недостатков. Нельзя не учитывать сложность разработки алгоритма, что связано с отсутствием универсальной инструкции по реализации метода.

По отношению к моделируемой системе в качестве наиболее подходящего алгоритма поиска и фильтрации данных выступает контентная фильтрация, исходя из ряда преимуществ:

- система использует информацию из профилей и может предоставлять рекомендации даже новым пользователям без истории взаимодействий;
- алгоритм учитывает конкретные интересы и характеристики пользователей, что делает рекомендации более персонализированными;
- простота разработки в сравнении с предыдущими методами.

В рамках системы алгоритм сопоставляет пользователей на основе сходства их профилей. Telegram-бот будет предлагать рекомендации на основе анализа данных в виде характеризующих атрибутов, внесенных пользователями в свои анкеты при регистрации. Исходя из данных условий, процесс регистрации включает обязательные для заполнения пользователем пункты, содержащие основную информацию для алгоритма, и атрибуты в виде «хэштегов», необходимые для обработки и сопоставления анкет.

В качестве способа вычисления метрики сходства в сочетании с алгоритмом контентной фильтрации выбран способ «Сходство Жаккара». Данный подход эффективно работает с множествами, что соответствует структуре данных в виде атрибутов в профилях музыкантов, не учитывает порядок элементов в множествах, измеряет схожесть профилей по количеству общих атрибутов, а также устойчив к масштабу множеств – размер самих множеств не влияет на результат вычисления схожести.

Сходство Жаккара является эффективной метрикой сходства, индекс которой варьируется от 0 до 1. Чем ближе к 1, тем более похожи два набора данных. Расчет можно представить в виде следующей формулы:

$$J(A, B) = |A \cap B| / |A \cup B|,$$

где A – первый набор данных, B – второй набор данных.

Метрика работает по следующему принципу: чтобы вычислить сходство между двумя наборами данных, сначала определяется общее количество наблюдений в обоих наборах, а затем делится на количество всех различных наблюдений в наборах. Если два набора данных имеют одни и те же элементы, их индекс сходства Жаккара будет равен 1. И наоборот, если у них нет общих элементов, их сходство будет равно 0 [3].

Процесс формирования рекомендаций пользователям можно представить в виде схемы, представленной на рис. 1. Сначала бот получает данные от пользователей при регистрации, тем самым по завершению регистрации формируются анкеты пользователей. Затем информация из анкет преобразуется в структуры данных, где каждый элемент соответствует конкретному

атрибуту. Данные атрибуты извлекаются, создаются наборы или же множества. Алгоритм производит расчет и сопоставление извлеченных данных, а следом на основе анализа в системе принимается решение о рекомендации профиля другому пользователю.

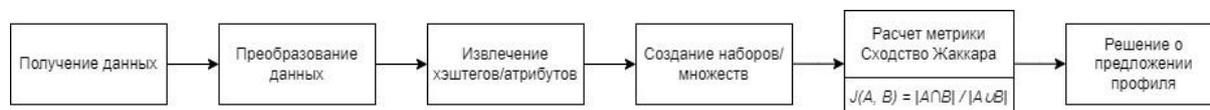


Рис. 1. Процесс формирования рекомендаций пользователю

В результате анализа сформирована модель информационной системы Telegram-бота для поиска музыкантов и создания коллабораций, представленная на рис. 2.



Рис. 2. Модель Telegram-бота для поиска музыкантов и создания коллабораций

Создание музыкальных коллабораций достигается путем использования описанных ниже модулей.

«Telegram API»: взаимодействие бота с Telegram API для отправки и приема сообщений от пользователей Telegram, обработка входящих и исходящих сообщений от пользователей, взаимодействие с кнопками.

Модуль «Обработка запросов пользователя»: обработка запросов, поступающих от пользователей через Telegram API, анализ текста сообщений, получение данных о предпочтениях пользователей в виде характеризующих атрибутов.

Модуль «Сессия выбора»: управление процессом выбора, хранение решений и выбора пользователей, отправка приглашений на коллаборацию.

Модуль «База данных»: обеспечение доступа к базе данных, где хранится информация о пользователях, их анкетах, характеризующих атрибутах, рейтингах и других связанных данных.

Модуль «Кэширование данных»: кэширование данных для ускорения доступа к часто используемой информации, такой как анкета или результаты предыдущих запросов, повышение быстродействия сервиса, сокращение количества обращений к API и снижение нагрузки на систему.

Модуль «Обработка запросов администратора»: интерфейс для администратора бота, который позволит управлять настройками бота, просматривать статистику использования, вносить изменения в базу данных и выполнять другие административные задачи.

Модуль «Управления коллаборациями»: сбор статистики о решениях пользователей, успешных коллаборациях и результатах работы алгоритма.

Модуль «Аутентификация и регистрация»: обработка новых пользователей, сбор указанной пользователями информации для формирования анкеты.

Модуль «Анкета пользователя»: отображение информации о пользователе, наличие готовой виртуальной анкеты, возможность редактирования профиля.

Модуль «Поиск и фильтрация»: работа алгоритма, обработка анкет и сопоставление атрибутов, поиск музыкантов по различным критериям (навыки, инструменты, жанры), фильтрация результатов поиска.

Модуль «Уведомления»: оповещения о новых сообщениях через Telegram API, запросах на коллаборацию и других событиях, а также возможность настройки уведомлений пользователями.

К спектру технологических решений для данного сервиса можно отнести следующие: интегрированная среда разработки «VS Code»; язык программирования «Python»; библиотека для работы с «Telegram API» «Aiogram», которая подходит для обработки запросов от множества пользователей в режиме реального времени, что обеспечит эффективное взаимодействие бота с пользователями; реляционная СУБД «PostgreSQL», обеспечивающая структурированное и эффективное управление информацией о пользователях, их предпочтениях и характеристиках.

Таким образом, рассмотрен инновационный подход к организации музыкальных коллабораций с использованием Telegram-бота. Предложена модель Telegram-бота для поиска музыкантов и создания коллабораций.

К достоинствам данного подхода можно отнести: доступность и удобство за счет реализации в виде Telegram-бота; решение проблемы поиска музыкальных партнеров и единомышленников в сфере музыкальных жанров; содействие в развитии музыкальных талантов; помощь в создании музыкальных сообществ; простота разработки и внедрения.

В перспективах развития сервиса возможна интеграция более продвинутых рекомендательных алгоритмов и расширение функционала для возвращения к взаимодействию музыкантов.

Список используемых источников

1. Снежинская М. Г. Музыкальная индустрия в эпоху больших данных: перспективы социологических и маркетинговых исследований // Российское правоведение: трибуна молодого ученого. 2018. № 4(24). С. 162–169.
2. Олянич И. А., Серафимович П. Г. Сравнительное исследование алгоритмов проектирования рекомендательных систем // Онтология проектирования. 2018. Т. 8. № 4(30). С. 628–631.
3. James Briggs, Semantic Search: Measuring Meaning from Jaccard to Bert. PineconeIO. 2021. URL: <https://www.pinecone.io/learn/semantic-search> (дата обращения: 26.01.2024)

УДК 004.056
ГРНТИ 81.93.29

ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРОВ И КОМПЬЮТЕРНОЙ СЕТИ В СРЕДНЕМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

Л. С. Беккель, А. Д. Николаев

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

С ростом числа киберпреступлений, средним общеобразовательным учреждениям необходимо уделять внимание вопросу безопасности собственных компьютеров и компьютерных сетей. Сначала необходимо разделять единую школьную сеть на сеть для учителей и администрации и сеть для учащихся. Так же для большей безопасности необходимо, чтобы на компьютерах было установлено антивирусное программное обеспечение, а к некоторым компьютерам должен быть ограничен доступ.

компьютер, компьютерная сеть, безопасность, среднее общеобразовательное учреждение, атака

Постепенно компьютерные технологии все больше и больше проникают в нашу жизнь, становясь важной частью разных сфер человеческой деятельности. Однако возникновение и развитие компьютеров принесло не только пользу, но и новые риски и угрозы, связанные с новым видом преступлений, известных как киберпреступления [1]. Киберпреступления – это противоправные действия, совершаемые людьми при помощи информационных технологий. Киберпреступность начала активно развиваться в последние несколько лет. По данным главного информационно-аналитического центра МВД в период с 2019 по 2021 год число совершаемых киберпреступлений в год выросло в 1,7 раза, достигнув в 2021 году 517 тысяч, и их число продолжает расти [1]. В связи с ростом и развитием киберпреступности всем компаниям и организациям необходимо уделять внимание вопросам безопасности собственных компьютерных технологий и компьютерных сетей.

В последние несколько лет в средние общеобразовательные учреждения начали массово внедрять компьютерные технологии. Если в 2016 году на внедрение компьютерных технологий школы было потрачено 450 млн. рублей, то в 2021 году на это уже потратили более 27 млрд. рублей [2]. Поэтому вопрос безопасности собственных компьютеров и компьютерных сетей стал актуален и для средних общеобразовательных учреждений. Однако так как компьютеры и иные компьютерные технологии начали появляться в средних общеобразовательных учреждениях совсем недавно, не все школы еще обращают внимание на вопрос защиты собственных компьютеров и

компьютерной сети. Из-за отсутствия защиты, школьное оборудование может быть успешно атаковано и в результате чего будет нанесен ущерб, как работе сотрудников среднего общеобразовательного учреждения, так и образовательному процессу.

Прежде чем выстраивать защиту компьютеров и компьютерной сети в среднем общеобразовательном учреждении, необходимо выяснить, кто в большинстве случаев будет совершать атаки на школьное оборудование. Средние общеобразовательные учреждения не относятся к объектам критической инфраструктуры. Атака на школьное оборудование способна навредить только сотрудникам учреждения и образовательному процессу, не давая почти никакой материальной выгоды злоумышленнику. И так как материальная выгода является одной из основных мотиваций киберпреступников, совершать атаку на школьное оборудование по этой причине, не будут [3]. Из мотивов проведения кибератаки у злоумышленника остаются только хулиганство и месть [3]. Чтобы такие мотивы появились, злоумышленник должен быть как-то связан со средним общеобразовательным учреждением. Сотрудник учреждения вряд ли будет хулиганить, тем самым вредя своей работе или работе своих коллег, если только не из чувства мести. Однако чувство мести является мотивацией, лишь у двух процентов киберпреступников [3]. Следовательно, атаки на школьное оборудование со стороны сотрудников учреждения, мотивированные местью, будут редкими. Остаются только учащиеся. И скорее всего в большинстве случаев именно они будут совершать атаки на школьное оборудование с целью похулиганить или отомстить. У учащихся есть мотив и в старших классах некоторые из учеников могут обладать знаниями для проведения простых атак на компьютеры. При этом своим поступком они навредят только сотрудникам школы, никак не вредя себе.

Так как в большинстве случаев совершать атаки на школьное оборудование будут именно учащиеся, то защищать компьютерное оборудование нужно не только снаружи, но и изнутри, так как учащиеся имеют доступ к школьному оборудованию.

Организовывая безопасность школьного оборудования, стоит обратить внимание на внутреннюю компьютерную сеть среднего общеобразовательного учреждения. К ней обычно подключены компьютеры учителей и администрации учреждения, а также электронные базы данных. Бывает так, что для удобства учащихся к этой же сети подключают учебные компьютеры, чтобы учащиеся могли свободно обмениваться файлами, как между собой, так и с учителем. В таких случаях это является одной из главных уязвимостей компьютерной сети среднего общеобразовательного учреждения. Ведь используя доступ к этой сети, учащийся может произвести атаку на все школьное оборудование и получить доступ к электронным базам данных, к

которым у него не должно быть доступа. Поэтому для повышения безопасности необходимо разделить единую школьную компьютерную сеть на две независимые друг от друга сети. К одной из них будут подключены компьютеры учителей, администрации, электронные базы данных и иное оборудование, предназначенное для работы учреждения. Ко второй сети будут подключены учебные компьютеры и оборудование, предназначенные для учащихся. В такой ситуации в случае успешной атаки пострадает только одна из сетей.

Теперь необходимо организовать защиту каждой из двух сетей независимо друг от друга.

Идеальнейшим вариантом организации безопасности сети, к которой подключены компьютеры учителей и администрации, является тот, при котором учащиеся вообще не имеют доступа к устройствам, подключенным к данной сети. Однако полностью исключить доступ учащихся к компьютеру учителя является сложной задачей. На каждом компьютере учителя и администрации должна быть учетная запись, защищенная паролем. Для повышения безопасности можно создать несколько учетных записей для каждого, кто имеет право работать за данным компьютером. Каждая учетная запись должна быть защищена паролем, который будет отвечать всем требованиям надежности, и будет своевременно меняться. Учитель должен следить за компьютером и не оставлять компьютер без присмотра, не выйдя из своей учетной записи.

Однако создание защищенных паролем учетных записей не исключит полностью доступ учащихся к компьютеру учителя. Всегда остается шанс, что сотрудник учреждения, работающий за компьютером, оставит его без присмотра, не выйдя из своей учетной записи. Но при грамотном обучении и информировании сотрудников, шанс такой ситуации невелик. Этот шанс можно еще уменьшить, настроив время бездействия, по истечению которого, если компьютер не использовался, будет происходить автоматический выход из учетной записи.

И, несмотря на это, учащиеся все еще имеют возможность получить доступ к компьютеру учителя, например, под видом сдачи презентации, доклада или электронного реферата. Зараженный файл может быть скопирован с флешки или прислан по электронной почте. В таком случае учителю нужно придумать способ приема заданий от учеников так, чтобы оно не требовало доступа к школьному компьютеру учителя, иначе полностью исключить доступ к компьютеру учителя со стороны учащихся невозможно.

Если возможность исключить доступ учащихся к компьютеру учителя отсутствует, то необходимо на каждый компьютер установить антивирусное программное обеспечение, которое было бы способно распознать большинство зараженных файлов. На основе исследования информационно-аналитического центра Anti-Malware.ru, можно сделать вывод, что наиболее

предпочтительными являются такие антивирусы, как Kaspersky Internet Security, сработавший в 100 % случаев, и Dr. Web Security Space, сработавший в 99 % случаев [4]. То, какое установлено антивирусное ПО и его настройки, не должно быть общедоступной информацией.

Кроме внутренней защиты сети, к которой подключены компьютеры учителей и администрации учреждения, должна быть еще и внешняя, ведь такая сеть должна иметь выход в Интернет. Учителям необходим доступ к электронному журналу. Так же образовательной программой может быть предусмотрено использование интернет-платформ. Для внешней защиты на границе сети должен быть установлен межсетевой экран, который будет контролировать проходящий трафик, и защищать от внешних атак. Для повышения уровня безопасности можно настроить межсетевой экран так, чтобы у устройств был доступ только к определенным интернет-ресурсам. Однако это зависит от условий работы конкретного среднего общеобразовательного учреждения и не всегда может быть реализовано. Поэтому все сотрудники школы, которые имеют право работать с компьютером, должны быть осведомлены об опасности перехода на не доверенные сайты по неизвестным ссылкам и скачивании файлов из неизвестных источников.

Без внимания не стоит оставлять и компьютерную сеть, к которой подключены учебные компьютеры, а также устройства, подключенные к данной сети. Атака на них способна нанести ущерб образовательному процессу. К учебным компьютерам учащиеся имеют доступ. Поэтому на учебных компьютерах должны быть как минимум две учетные записи. Одна с правами администратора, для настройки компьютера, к которой учащиеся не будут иметь доступ, и вторая без прав администратора, для работы самих учащихся. Дополнительно можно создать каждому учащемуся свою учетную запись или зарегистрировать их иначе, чтобы можно было знать, кто и в какое время работал за конкретным компьютером. Это не увеличит уровень защиты, но в случае происшествия может помочь установить личность атаковавшего, а, следовательно, это позволит предпринять профилактические меры необходимые для предотвращения подобных инцидентов в будущем.

Для того чтобы защитить учебный компьютер, на учетную запись учащегося должны быть наложены определенные ограничения, которые должны быть согласованы с образовательной программой и особенностью образовательного процесса конкретного среднего общеобразовательного учреждения. Например, можно запретить скачивание и установку дополнительных приложений. То есть, чтобы учащийся мог работать только с предустановленным заранее программным обеспечением. Кроме того, у учащегося не должно быть возможности изменять ключевые настройки компьютера. Так же можно запретить подключение внешних носителей информации, таких как флешек, чтобы исключить возможность заразить компьютер при помощи внешних носителей информации. Однако возможность

реализации данного запрета зависит от учебной программы и особенности образовательного процесса конкретного среднего общеобразовательного учреждения. Поэтому в случае, если невозможно запретить подключение внешних носителей информации к учебному компьютеру, на компьютере обязательно должно стоять антивирусное программное обеспечение, например, Kaspersky Internet Security или Dr. Web Security Space, которые имеют почти стопроцентный шанс срабатывания на зараженный файл [4].

Для большего уровня безопасности у данной сети не должно быть выхода в Интернет, чтобы избежать внешних атак.

Предложенный выше вариант защиты школьного оборудования и школьной компьютерной сети способен защитить только от простых атак. Однако его преимущество в простоте реализации и в том, что он не требует значительных дополнительных денежных вложений для организации компьютерной безопасности среднего общеобразовательного учреждения. И в большинстве случаев такой защиты будет достаточно, так как большинство атак на школьное оборудование будут простыми, ведь их будут совершать учащиеся, а они в большинстве случаев еще вряд ли обладают знаниями и навыками для проведения сложных атак. Однако на случай, если все-таки будет произведена успешная атака на школьное оборудование, среднему общеобразовательному учреждению необходимо в определенное время производить резервное копирование состояния системы и всех электронных баз данных. Например, один раз в неделю. Тогда в случае, если атака окажется успешной, будет возможность восстановить утраченные базы данных и состояние системы с минимальными потерями.

Список используемых источников

1. Мухамедович А. А. Развитие киберпреступности в цифровом обществе // Журнал прикладных исследований. 2023. № 5. С. 53–57.
2. Отчет Счетной палаты Российской Федерации о результатах экспертно-аналитического мероприятия. Оценка мер внедрения цифровых технологий в образовательных учреждениях общего образования. 2022. С. 21.
3. Пучков О. А. Мотивация действий хакеров в современной цифровой среде: междисциплинарный подход // Проблемы современного педагогического образования. 2020. № 67-3. С. 306–308.
4. Тетерина Е. В., Черненко В. В. Анализ эффективности работы современных антивирусных программ // Решетневские чтения. 2010. № 1. С. 559–560.

УДК 654.739
ГРНТИ 49.33.29

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

К. В. Белоус, А. Ю. Горбач, В. И. Матюхина

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

Программные продукты мониторинга сетевого телекоммуникационного оборудования предназначены для оперативного мониторинга происходящих в сетях процессов, что позволяет оперативно выявлять и устранять сбои, а также отслеживать внештатные и нейтрализовать внештатные ситуации с минимальными затратами. Существующие программные продукты не всегда позволяют удовлетворить потребности конкретного пользователя, в связи с чем задача создания автоматизированной системы данного класса является актуальной задачей.

компьютерная сеть, оборудование, база данных, контроль

Компьютерные сети (КС) представляют собой системы с большим количеством элементов и взаимосвязей между ними [1]. От бесперебойной работы КС зависит множество процессов, среди которых банковские операции, процессы управления движением, контроль несанкционированного доступа, операции по покупке и продаже товаров и др. В связи с вышеизложенным создание системы контроля параметров КС является актуальной задачей. Несмотря на то, что в настоящее время на рынке существует большое количество программных продуктов, позволяющих решать данную задачу, они не всегда удовлетворяют требованиям конкретного пользователя, а с учётом того, что большая часть из них – это продукты зарубежных компаний, их использование в системах критической инфраструктуры является небезопасной, о чём говорят последние исследования в данной области. Кроме того, актуальность внедрения автоматизированной системы контроля телекоммуникационного оборудования связана с постоянным повышением сложности эксплуатации и наладки данного оборудования [2].

Предлагаемая система в основу своей функциональности ставит оперативное получение информации о состоянии объекта, что дает возможность нормирования и контроля параметров качества сети оператором. Обобщённая структура системы контроля телекоммуникационного оборудования представлена на рис. 1.

Далее представим краткий анализ существующих систем контроля телекоммуникационного оборудования, выделив их преимущества и недостатки.



Рис.1. Общая структура автоматизированной системы контроля телекоммуникационного оборудования

Виды автоматизированных систем контроля:

System Center Operations Manager (SCOM) – система сквозного мониторинга и активного наблюдения за любыми сетевыми устройствами, поддерживающими протокол обмена информацией SNMP (до уровня порта), обнаружения виртуальных локальных вычислительных сетей (VLAN) и коммутаторов в них, слежения за их техническим состоянием. Система разработана корпорацией Microsoft [3].

SCOM предназначен для организаций с числом сетевых устройств более 500 и числом серверов более 30. В последнее десятилетие SCOM относят к сервису высокой доступности, благодаря отсутствию серверов управления. При сопряжении с несколькими серверами нагрузка балансируется, обеспечивая доступность. Также, на каждом из серверов работает служба конфигурации, и хранение данных реализовано не в памяти или XML-файлах, а в базе данных. К основным преимуществам SCOM относятся:

- высокая производительность и работоспособность;
- обеспечение сквозного управления службами для сервисов центра обработки данных;
- унифицированный контроль частных и общедоступных облачных сервисов;
- существенное повышение эффекта в управлении средой центров обработки данных.

Одним из главных достоинств SCOM является система визуализации, позволяющая строить графики и диаграммы процессов, протекающих в системе.

Несмотря на очевидные преимущества, SCOM имеет и ряд недостатков:

- охват множества общих показателей системы, но невозможность слежения за специфическими параметрами;
- поддержка операционных систем, отличных от Windows, затруднена;
- громоздкость и трудоемкость настройки для решения конкретных задач
- система больше подходит для мониторинга общего состояния и сбора основных сведений о глобальной структуре;
- высокая стоимость.

Zabbix – свободно распространяемая система для проведения комплексного мониторинга сетевого оборудования, серверов и сервисов. Zabbix позволяет осуществлять распределённый мониторинг до 1000 узлов, где конфигурация младших узлов в иерархии контролируется старшими. Также имеется возможность создавать вручную по шаблону карты сетей, выполнять запросы в различные БД и генерировать отчёты. Преимущества Zabbix заключаются в следующем:

- автоматическое обнаружение IP-адресов по диапазону;
- доступные сервисы;
- проведение SNMP проверок;
- автоматическое удаление отсутствующих устройств и автоматический мониторинг обнаруженных сетевых устройств с распределением их по шаблонам, группам.

В качестве недостатков Zabbix стоит отметить:

- громоздкость сервиса;
- отсутствие полной документированности возможностей;
- необходимость установки Zabbix-агентов на все машины, сложность делегирования прав.

Система управляется операционной системой семейства UNIX, что делает трудоёмким взаимодействие с Windows.

Nagios – свободно распространяемое ПО для мониторинга КС разработанное для операционных систем на базе Linux.

К достоинствам Nagios можно отнести:

- мониторинг безопасности ИТКС;
- выявление проблем сразу после их возникновения;
- мониторинг сетевых служб (SMTP, HTTP, SNMP, POP3, NNTP, ICMP);
- мониторинг состояния хостов в большинстве сетевых ОС (загрузка процессора, системные логи, использование диска);
- поддержка удаленного мониторинга через зашифрованные туннели SSH, SSL;
- возможность построения карт сетей;
- параллельный мониторинг служб;

– возможность создания распределенной системы мониторинга путем организации совместной работы нескольких систем мониторинга с целью повышения эффективности.

Недостатками использования Nagios является:

- слабые функциональные возможности;
- необходимость поиска и установки расширений для создания полнофункциональной системы мониторинга;
- проблемы взаимодействия с серверами под ОС Windows.

Обобщение преимуществ и недостатков рассмотренных систем представлено в таблице 1.

ТАБЛИЦА 1. Функциональные возможности систем контроля

Системы мониторинга	Функции модели управления информационно-телекоммуникационными сетями					Функции системы мониторинга			
	Управление отказами	Управление конфигурацией	Учет	Управление производительностью	Управление безопасностью	устройства	соединения	сети	сервисы
SCOM	+/- мониторинг сервисов	+ управление конфигурацией сервисов	+ учет сервисов	+	+	-	-	-	+
Zabbix	+	+/- только устройства и сервисы	+	+	-	+	+/- отсутствует понятие канала	+/- (rmon)	+
Nagios	+		+/-	+	-	+	+/- отсутствует понятие канала	+/- (rmon)	+

Предлагаемое программное обеспечение будет реализовывать следующие характеристики (рис. 2):

- бесплатное программное обеспечение;
- ориентация на малые и средние предприятия;
- простой и понятный пользовательский интерфейс на русском языке;
- возможность контроля каждого элемента системы в отдельности.

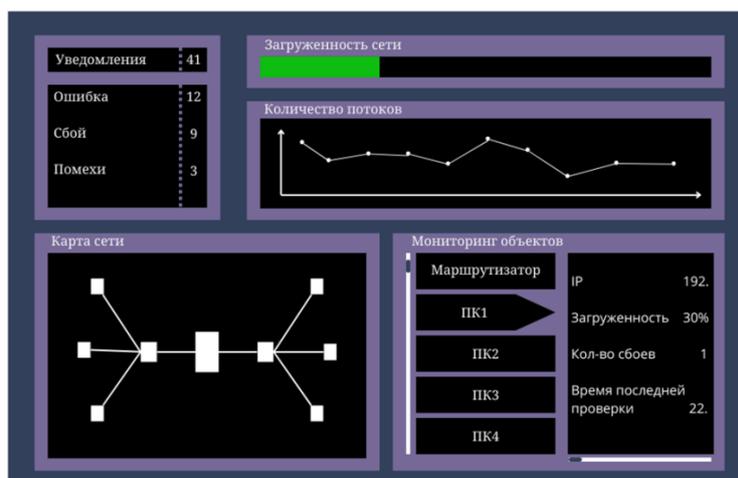


Рис. 2. Модель интерфейса предлагаемой системы

Функционал предлагаемой системы:

- мгновенный приход уведомлений о возникших проблемах;
- разделение проблем по категориям;
- контроль загруженности системы;
- мониторинг каждого объекта системы;
- построение карты сетей;
 - возможность визуального представления данных в виде графиков.

Для разработки системы был выбран язык программирования C# и СУБД PostgreSQL.

Список используемых источников.

1. Кузин А. В., Демин В. М. Компьютерные сети: Учебное пособие. М.: ФОРУМ: ИНФРА-М, 2005. 192 с. (Профессиональное образование).
2. Назаров С. В. Администрирование локальных сетей Windows NT/2000/.Net: Учеб. пособие. 02-е изд., перераб. и доп. М.: Финансы и статистика, 2003. 480 с.: ил.
3. Шашлов С. Азбука сисадмина. Энциклопедия iXBT.com. СПб.: Притер, 2008.

УДК 654.739
ГРНТИ 49.33.29

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ВИЗУАЛИЗАЦИИ КОМАНД УПРАВЛЕНИЯ ПЛК OMRON

К. В. Белоус, А. А. Демидов

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

В современном информационном обществе автоматизация и управление процессами становятся одним из основных аспектов для обеспечения эффективности и надежности работы различных систем. Развитие технологий виртуализации и программирования логических контроллеров открывает новые возможности для создания гибких и масштабируемых систем управления. В статье представлено программное обеспечение, позволяющее эффективно управлять виртуальными объектами с использованием программируемых логических контроллеров.

автоматизация, контроллер, управление, обучение

Программируемый логический контроллер является одним из наиболее важных инструментов при создании систем автоматического и автоматизированного управления технологическими процессами и производствами, которые связаны с обработкой больших объемов данных, как поступающих от нижних уровней, так и передаваемых на верхние уровни для дальнейшей обработки в ручном или автоматическом режиме с целью принятия решений. Обобщенная структурная схема ПЛК представлена на рис. 1 [1].



Рис. 1. Обобщенная структурная схема ПЛК

Несмотря на то, что стандартное программное обеспечение реализует все функции в области программирования ПЛК, оно не обладает способностью достаточной визуализации выполнения операций и детального просмотра управляющих команд, следовательно, актуальной становится задача создания дополнительного программного продукта, который совместно с базовым ПО реализует функции визуализации. Данное ПО может быть полезно при обучении специалистов в области программирования ПЛК, а также позволит более детально понимать процессы, происходящие на низком уровне при выполнении команд [2].

Анализ программных средств, позволяющих достичь цели ВКР, а именно, разработать приложение для визуализации команд управления ПЛК, позволил сделать выбор в пользу интегрированной среды разработки Visual Studio, языка программирования C# и технологии настольных приложений под ОС MS Windows. Выбор среды разработки и языка обусловлен тем, что в настоящее время существует динамически подключаемая библиотека, которая позволяет передавать контроллеру команды управления [3].

Порядок работы с визуализатором включает следующие шаги.

Первоначально происходит написание программного обеспечения на языке LD или ST в среде программирования CX-Programmer, при этом особое внимание необходимо уделить выбору адресного пространства входов, выходов и хранения промежуточных результатов. После этого происходит загрузка программы в контроллер стандартным образом.

На следующем этапе выполняется запуск визуализатора и подключение его к ПЛК.

Далее из главного меню производится выбор технологического объекта или процесса.

На заключительном этапе выполняется задание адресов входов, выходов и работа с визуализатором.

Первоначально производится написание ПО в CX-Programmer с подключённым контроллером по последовательному интерфейсу или с использованием Ethernet. Производятся отладка и заливка кода в контроллер штатными средствами CX Programmer.

Пользовательский интерфейс представлен на рис. 2 и 3. При запуске приложения открывается форма приложения, на которой располагаются основные элементы управления: поля для задания IP-адреса и порта подключения, кнопки управления подключением.

Элементы записи данных в регистры СЮ. Выбор режима работы, в нашем случае Светофора или Бегущих огней. Кнопки СТАРТ и СТОП для включения и выключения программы.

При выборе светофора появляется окно с вводом адресов выходов каждого сигнала и условное изображение светофора. Также присутствует

checkbox, который позволит включить Ночной режим светофора, при котором будет мигать желтый свет. При включении по кнопке СТАРТ начнется проверка, при которой недопустимо использование одинакового адреса в нескольких сигналах, а также проверка на то, не пустые ли эти адреса. После проверки произойдет блокировка, которая не позволит производить какие-либо действия с адресами и включится таймер, который в определенный интервал будет считывать значения с ПЛК и в зависимости от того, где установлена в этот момент логическая единица, будет менять изображения, иллюстрируя красный, желтый и зеленый свет светофора.



Рис. 2. Виртуальный объект «Светофор»

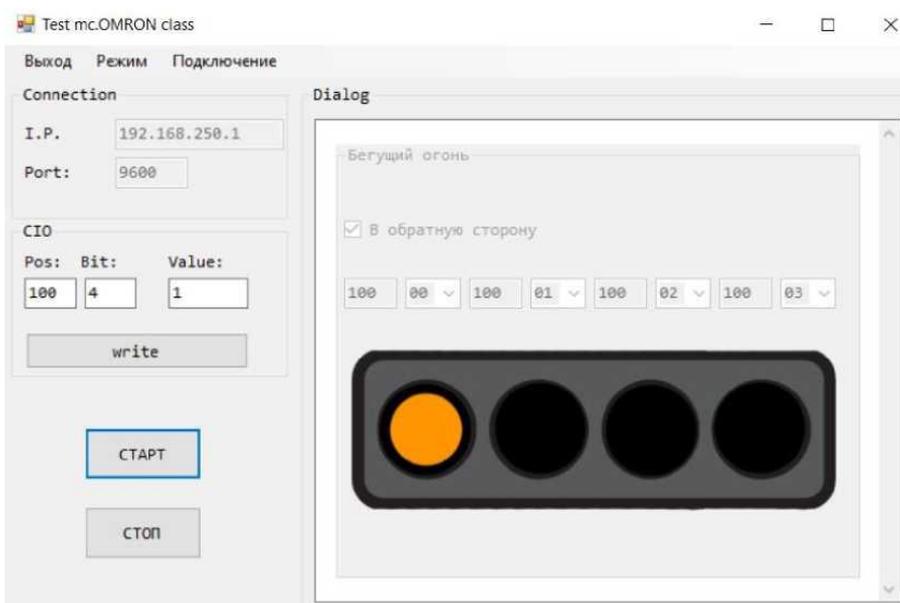


Рис. 3. Виртуальный объект «Бегущий огонь»

При выборе бегущего огня появляется окно с вводом адресов выходов каждой лампочки и условное изображение этих лампочек. Также присутствует checkbox, который позволит включить режим Обратного направления, при котором лампочки будут загораться в обратном направлении. При включении по кнопке СТАРТ начнется проверка, при которой недопустимо использование одинакового адреса, а также проверка на то, не пустые ли эти адреса. После проверки произойдет блокировка, которая не позволит производить какие-либо действия с адресами и включится таймер, который в определенный интервал будет считывать значения с ПЛК и в зависимости от того, где установлена в этот момент логическая единица, будет менять изображения, иллюстрирую бегущий огонь.

Разработанное программное обеспечение может быть востребовано при обучении инженеров-программистов контроллеров, для проведения обучающих занятий и тестирования знаний.

Список используемых источников

1. Ватсон Б. С# 4.0 на примерах. СПб.: БХВ-Петербург, 2011. 608 с.: ил.
2. Шишов О. В. Программируемые контроллеры в системах промышленной автоматизации: учебник / О. В. Шишов. М.: ИНФРА-М, 2021. 365 с. Доп. Материалы (Высшее образование). Бакалавриат. DOI 10.12737.17505
3. Кангин В. В. Разработка SCADA-систем: учебное пособие / В.В. Кангин, М. В. Кангин, М. Д. Ямолдинов. Москва; Вологда: Инфра-Инженерия, 2019. 564 с.: ил., табл.

УДК 004.738.5
ГРНТИ 49.33.01

АНАЛИЗ ПРИНЦИПОВ РАБОТЫ DNS-СЕРВЕРОВ И DDoS-АТАК

М. Д. Беседин, В. А. Задбоев, В. Р. Полищук

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

В статье сосредотачивается внимание на взаимосвязь между DNS являющейся критической инфраструктурой интернета, обеспечивающей преобразования необходимые для маршрутизации сетевого трафика, а также DDoS-атак, представляющих серьезную угрозу для стабильности сетевой инфраструктуры методами распределенного отказа в обслуживании.

DNS, DDoS, принципы работы, способы атаки, методы воздействия

Исследование принципов работы DNS-серверов и DDoS-атак играет ключевую роль в обеспечении стабильности и безопасности интернет-инфраструктуры. DNS является основным механизмом преобразования доменных имён в IP-адреса, потому представляет из себя незаменимое звеном сетевой коммуникации, так как его надежность влияет на доступность миллионов веб-ресурсов. В тоже время тщательное изучение механизмов работы DDoS-атак необходимо для обеспечения безопасности информационной сети.

Анализ принципов работы DNS-серверов

Перед тем, как рассматривать принципы работы DNS-серверов, необходимо разобраться в самом протоколе DNS.

DNS (англ. Domain Name System «система доменных имён») – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене.

Основой DNS является представление об иерархической структуре имени и зонах. Каждый сервер, отвечающий за имя, может передать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Доменное имя – буквенно-числовой набор символов, составляющих определённую последовательность и служащих для идентификации ресурсов в сети Интернет. Доменное имя состоит из нескольких областей, называемые «Домены». С помощью них упрощается возможность цифровой адресации интернет-узлов, а также принадлежащим им сетевым ресурсам, такие как веб-сайты, сервера электронной почты и другим. Также благодаря доменному имени все соответствующие интернет-узлы представляются в удобной для человека форме.

Полное доменное имя состоит из всех имен доменов, в которые они входят, разделенных точками. Например, полное имя `ru.example.com` говорит, что домен третьего уровня `ru`, входит в домен второго уровня `example`, входящий в свою очередь в домен верхнего уровня `com`, обозначающий, что веб-ресурс принадлежит коммерческой организации. В обыденной речи полное доменное имя просто называют сайтом [1].

DNS – распределенная система доменных имен, должна быть способна обрабатывать запросы на преобразование доменных имен в IP-адреса и наоборот, оставаться доступной даже при возникновении сбоев или атак, иметь низкую скорость ответа на внешние запросы, обеспечивать сохранность данных и продолжать работу при сбое одного из узлов, включать в себя механизмы защиты от различных видов атак, таких как DDoS-атаки, эффективно масштабироваться при необходимости для обработки растущего объема запросов без потери производительности, анализировать производительность сервера, обнаруживать аномалии и проблемы для дальнейшей оптимизации своей работы.

DNS-сервер, Domain name server – это сервер, предназначенный для обработки и последующие ответы на DNS-запросы. Также DNS-сервер может быть просто хостом с запущенным соответствующим приложением.

По выполняемым функциям и зонам деятельности DNS-серверы разделяются на различные группы, таким образом сервера могут относиться к определённой для них конфигурации, такие как:

Авторитетный DNS-сервер (DNS authoritative server) – сервер, который содержит записи только для определенной для него зоны влияния.

Мастер, так же известный по терминологии BIND первичный сервер, – имеет право на осуществление изменений в определенных зонах. Каждой соответствующей зоне принадлежит только один мастер-сервер. Однако в Microsoft, DNS-сервера и его интеграции с Active Directory существует несколько мастер-серверов. Так происходит из-за особенностей их работы, где все репликации изменений фиксируются в Active Directory.

Слейв, так же известный по терминологии BIND вторичный сервер, это сервер, который не имеет права на какие-либо изменения в определенных зонах, поэтому все изменения они получают от в виде сообщений от первичного сервера. В отличие от первичного сервера, слейв-серверов бывает

неограниченное количество. Слейв-сервера также являются авторитетными серверами. Обычный пользователь не увидит разницу между первичным и вторичным сервером.

Кэширующий DNS-сервер – сервер, обслуживающий запросы клиентов. Такой сервер получает рекурсивный запрос и обрабатывает его, используя нерекурсивные запросы к авторитетным серверам. В других случаях может передать запрос на рекурсию DNS-серверу в иерархии.

Перенаправляющий DNS-сервер (англ. Forwarder) – соответственно отвечает за перенаправление полученных от других рекурсивные запросы следующему в иерархии кэширующему серверу. Предназначен в основном для уменьшения нагрузки на кэширующий DNS-сервер.

Корневой DNS-сервер – сервер, отвечающий за корневую зону. Таких серверов всего 13 в мире, а их доменные имена находятся в зоне root-servers.net и называются соответственно только с приставками спереди от a до m.

Регистрирующий DNS-сервер – это сервер, который отвечает за прием динамических обновлений от обычных пользователей. Часто совмещается с DHCP-сервером.

DNSBL-сервер (DNS Blacklist) – сервер с черными списками адресов и имён. Используется для определения и блокировки IP-адресов, которые участвуют в нежелательной или вредоносной активности в сети Интернет.

Анализ принципов работы DDoS-атак

DDoS (аббр. англ. Distributed Denial of Service «распределенный отказ в обслуживании») – хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию – например, версию, часть программного кода и т. д.). Но чаще это мера экономического давления: потеря простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют по карману «цели». В настоящее время такие атаки наиболее популярны, так как позволяют довести до отказа практически любую плохо написанную систему, не оставляя юридически значимых улик [2].

Причины использования DDoS-атак

В настоящее время специалисты в области защиты информации выделяют следующий список причин использования DDoS-атак:

Конкуренция и личная неприязнь. Причина заключается в том, что конкуренты или недовольные личности могут запускать DDoS-атаки в качестве мести или чтобы нанести ущерб бизнесу или организации;

Вымогательство заключается в использовании злоумышленниками DDoS-атаки для вымогательства денег, угрожая прекращением атак только после выплаты выкупа;

Политические мотивы сопровождаются активистами и группами с политическими убеждениями, которые могут направлять DDoS-атаки против веб-сайтов или сервисов, которые они считают нежелательными или противоречащими их взглядам;

Саботаж заключается в виде атак, которые могут быть направлены на нарушение работы критически важных систем или услуг с целью нарушения обычного функционирования.

Некоторые DDoS-атаки могут быть мотивированы просто желанием destabilизировать сетевые ресурсы или вызвать неудобства для пользователей чаще всего просто для развлечения.

Тестирование защиты. Некоторые организации могут проводить DDoS-атаки, как часть тестирования своей собственной защиты от таких атак или для оценки уязвимостей своих систем.

Виды DDoS-атак:

- HTTP(S) GET-флуд – на сервер отправляется ничего не значащая информация, забивающая канал передачи данных и расходующая ресурсы сервера;
- smurf-атака – взломщик отправляет операционной системе запрос с подменным mac-адресом. Все ответы с сервера пересылаются на пинг-запрос хаккера, а жертва бесконечно долго ждет пакеты, который у нее умыкнул воришка;
- HTTP(S) POST-запрос – передача больших объемов данных, помещенных в тело запроса;
- UDP-флуд – в данном типе атаки превышает время ожидания ответа от сервера, соответственно, пользователь получает отказ в обработке запроса;
- SYN-флуд – одновременно запускается целый рой TCP-соединений, упакованных в SYN-пакеты с недействующим или несуществующим обратным адресом – «посылка на деревню дедушке»;
- POST-флуд – по аналогии с GET-флуд передает большое количество запросов, что приводит к подвисанию сервера. Если используется протокол с автоматическим шифрованием данных HTTPS, дополнительные ресурсы расходуются на дешифровку, что только облегчает задачу хакера «положить» сервер;

- программы-эксплоиты – используются более продвинутыми взломщиками, цель которых – коммерческие организации. Программное обеспечение выискивает ошибки кода, бэкдоры, уязвимости;
- layer 7 HTTP-флуд – на виртуальном сервере нагружает только отдельные площадки. Такой вид DDoS трудно определить, потому что трафик похож на обычный пользовательский. Основная цель – повышенная нагрузка сервера;
- переполнение HDD – если на сайте настроена ротация лог-файлов, жертве отправляются все новые логи, которые займут все свободное пространство на винчестерах. Очень примитивный способ – закидать мусором, эффективен и опасен. Скорость «закидывания» мусорных файлов очень высокая, уже через 5 минут сайт будет недоступен клиентам;
- атака на VoIP и SIP устройства связи – осуществляется через специальное ПО, для организации необходимо узнать IP-адрес пользователя;
- атаки на уровне приложения DNS-сервера. В большинстве случаев жертвами становятся владельцы площадок на CMS Drupal, WordPress, Joomla, Magento. Выделенный Amazon VPS-сервер может справиться с 180 000 пакетов в секунду, обычный сервер обрабатывает в среднем 500 запросов за то же время [3].

Выводы

Проведен анализ принципов работы DNS-серверов и DDoS-атак. Изучены понятия DNS и DNS-сервер, доменные имена, DDoS-атака, а также определены характеристики DNS, виды и причины DDoS-атак.

Изучение предложенных аспектов поможет в дальнейшем планировании информационно-вычислительной сети, что положительно сказывается на её безопасности.

Список используемых источников

1. Коваленко Т. А. Роль DNS в интернете. Актуальные вопросы развития науки и образования на современном этапе: опыт, традиции, инновации. 2020. С. 17–23.
2. Кадыров Р. Р. Методы обнаружения и предотвращения DDOS-атак. Политехнический молодежный журнал. 2019. № 7(36). С. 1.
3. Репин Д. С., Краснов А. Е., Надеждин Е. Н. Способ защиты от DDoS-атак на основе классификации трафика. Пат. 2704741 Российская Федерация; заявитель и патентообладатель Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий». № 2018109398; заявл. 16.03.18; опубл. 30.10.19.

УДК 004.453.2
ГРНТИ 20.51.19

АНАЛИЗ ВОЗМОЖНОСТЕЙ ВЫСОКОУРОВНЕВОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ PYTHON ПО АВТОМАТИЗАЦИИ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

М. Д. Беседин, В. А. Задбоев, В. Е. Садовников

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

Постановка задачи: в настоящее время возникает всё большая потребность в автоматизации различных процессов, происходящих в сетях передачи данных, в том числе и в ситуациях, когда необходимо автоматизировать конфигурацию большого числа сетевых устройств. Целью данной статьи является рассмотрение вопроса оптимального выбора инструмента для автоматизации процессов взаимодействия сетевых устройств. Результаты: в рамках работы описаны основные инструменты, выделены их недостатки и преимущества, а также приведен примеры применения данных инструментов в конкретных ситуациях.

программирование, сети, информационная безопасность, автоматизация

В настоящее время конфигурация сети значительно усложнена высокой дефрагментацией в сети, вызванной необходимостью применять множество различных образцов оборудования от нескольких вендоров, для решения поставленных задач [1].

Существует несколько различных методов автоматизации, применяемые в существующих системах передачи данных. Данные методы можно разделить на несколько основных типов (рисунок 1):

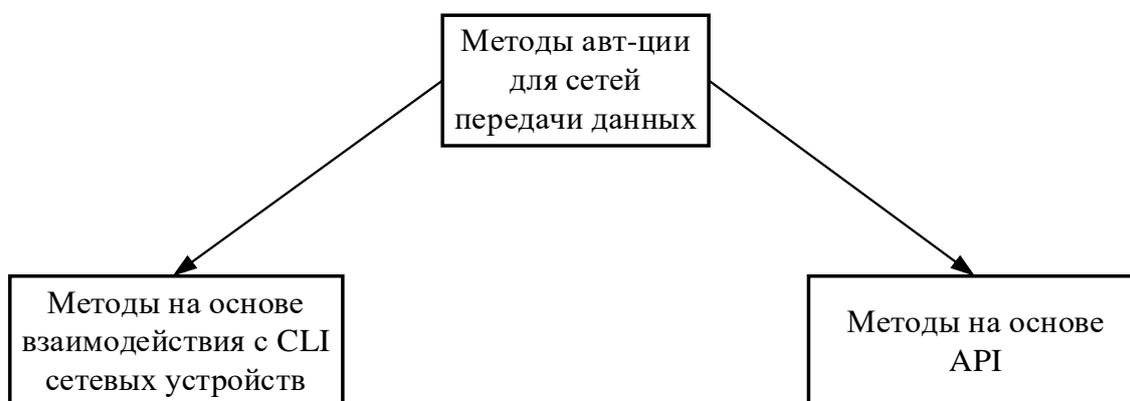


Рис. 1. Классификация методов автоматизации для сетей передачи данных

Из рисунка 1 видно, что существует два основных типа, классифицирующих методы автоматизации, современных сетей. В данной статье будут рассмотрены методы на основе взаимодействия с *CLI* (*command line interface*). Применение такого способа взаимодействия заключается в запуске интерактивного дочернего процесса и наблюдении за тем, как процесс общается с целевым устройством [2]. Проверив полученное значение, родительский процесс предпринимает последующие действия. В основном для взаимодействия с *CLI* применяются библиотеки и фреймворки написанные на языке *Python*:

- 1) *Pexpect*;
- 2) *Paramiko*;
- 3) *Netmiko*;
- 4) *Nornir*.

Библиотеки, обозначенные выше, применяются для взаимодействия с *CLI* сетевого оборудования, создавая дочерний процесс и осуществляя наблюдение за ним [3].

Для более детального рассмотрения данных библиотек языка *Python* было разработано программное обеспечение (ПО), которое позволяет автоматизировать процесс конфигурирования сетевого оборудования на примере оборудования компании *Cisco*.

Используя одну из представленных библиотек, напишем простую программу, которая будет загружать определённую конфигурацию на несколько устройств сразу.

Для этого создадим в директории программы три файла:

- 1) *commands.txt*;
- 2) *devices.json*;
- 3) *netmiko_script.py*.

В файле *commands.txt* (рис. 2) находятся команды, которые необходимо отправить на устройства в процессе работы программы. Файл *devices.json* (рис. 3) содержит параметры устройств для подключения к ним такие как: IP-адрес, логин и пароль для авторизации и тип устройства. Файл *netmiko_script.py* (рис. 4) содержит алгоритм работы программы. Сначала в программу подключается сама библиотека *netmiko* и библиотека для работы с файлами, использующими расширение *json*. После чего в программе открываются два файла *commands.txt* и *devices.json*, которые необходимы для её работы и запускается цикл, который рассылает команды из файла *commands.txt* по устройствам из файла *devices.json*. Стоит отметить, что данный способ позволит заметно ускорить процесс конфигурирования сетей передачи данных, а также снизить вероятность ошибки администратора. Такой подход к конфигурированию и изменению параметров сети позволяет

значительно ускорить процесс развёртывания распределённых систем передачи данных. При дальнейшем развитии данного способа появится возможность реализовать полностью автоматизированный комплекс, использующий все возможности языка *Python*.

```
home > flartvision > Рабочий стол > Проекты > Автоматизация сети с Python > Программа > commands.txt
1 config t
2 interface gigabitEthernet 0/0/0
3 description Link to LAN
4 ip address 192.168.10.1 255.255.255.0
5 no shutdown
6 exit
7 interface gigabitEthernet 0/0/1
8 ip address 192.168.10.1 255.255.255.252
9 no shutdown
10 exit
11 end
12 copy run start
13 interface gigabitEthernet 0/0/1
14 ip address 209.165.200.225 255.255.255.252
15 no shutdown
16 exit
17 end
18 copy run start
19
```

Рис. 2. Команды, которые будут отправляться на устройства в ходе работы скрипта

```
home > flartvision > Рабочий стол > Проекты > Автоматизация сети с Python > Программа > devices.json
1 {
2   "iosv-1": {"device_type": "cisco_ios", "host": "192.168.1.20", "username": "cisco", "password": "cisco"},
3   "iosv-2": {"device_type": "cisco_ios", "host": "192.168.1.21", "username": "cisco", "password": "cisco"},
4   "iosv-3": {"device_type": "cisco_ios", "host": "192.168.1.22", "username": "cisco", "password": "cisco"}
5 }
```

Рис. 3. Первичная конфигурация устройств, которая будет применяться для подключения

```
home > flartvision > Рабочий стол > Проекты > Автоматизация сети с Python > Программа > netmiko_test.py
1 from netmiko import ConnectHandler
2 import json
3
4 with open('devices.json', 'r') as f:
5     devices = json.load(f)
6
7 with open('commands.txt', 'r') as f:
8     commands = f.readlines()
9
10
11 for device in devices.values():
12     connection = ConnectHandler(**device)
13     configuration = connection.send_config_set(commands)
```

Рис. 4. Разработанный скрипт

В качестве дальнейшего развития будут добавлены модули мониторинга активности сети, база данных для хранения различной информации, используемой инфраструктурой, а также добавление управления инфраструктурой с выделенного сервера, использующего веб страницу для управления всеми модулями.

Список используемых источников

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание 6-е. СПб: Питер, 2020. 1008 с.
2. Чоу Э. *Python* для сетевых инженеров. Автоматизация сети, программирование и *DevOps*. 3-е издание. СПб.: Питер, 2024. 528 с.
3. Любанович Б. Простой Python. Современный стиль программирования, 2-е издание. СПб.: Питер, 2022. 592 с.

Статья представлена начальником научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, кандидатом технических наук, А. С. Дворниковым.

УДК 621.376.6
ГРНТИ 47.47.29

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ С ИСПОЛЬЗОВАНИЕМ RFID-МЕТОК

В. Р. Бикбулатов, А. С. Мешков, Д. Ф. Ткачев

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

Технология уникальной идентификации с использованием радиоволн и применением RFID-метки, в которой содержится микрочип, с записанным особым идентификатором и антенну для приема и передачи сигнала на специальные считыватели. RFID-метка размещается в определенный предмет для определения в реальном времени человека, животного или какой-либо продукции. Таким образом, рассмотрим концепцию технологии RFID-меток, принцип работы, преимущества применения и недостатки.

радиочастотная идентификация, RFID-метки, стандарты ISO

Радиочастотная идентификация (RFID) – технология, позволяющая производить считывание и запись данных с помощью радиосигналов [1]. Принцип работы технологии связан с передачей при помощи радиоволн информации о пользователе, которая нужна для опознавания различных объектов, с размещенными метками, передающие информацию о пользователе для прохождения идентификаций. Технология радиочастотной идентификаций продолжает развитие штриховой кодовой идентификации, сохраняя все достоинства и устраняя практически все ее минусы.

На данный момент времени технология RFID получает распространение в множестве различных отраслей производства, благодаря возможности получить информацию без непосредственного контакта. Рабочее расстояние, записи и чтения данных, различается от десятка миллиметров до нескольких сотен метров и зависит, в первую очередь, от применяемой технологий [2]. Рабочая система представляет из себя два отдельных объекта, которая состоит из RFID-метки и считывающего устройства, которая считывает данные с метки и перерабатывает полученную информацию для дальнейшей обработки [3].

Считыватель – это некий прибор, выполненный с одной или несколькими антеннами, для передачи радиоволны к RFID-метке и приему полученного уже измененного сигнала.

RFID-метка имеет возможность сохранить большой объем различной информации, до нескольких страниц различных данных. Устройство возможно сделать мобильным, удобным для переноса в руке или же закрепить на столб, здание или любой другой объект.

Транспондеры (другое название RFID-меток) может быть выполнена в любой форме, из различного материала, разного размера и цвета. Ограничения конструкций в первую очередь зависит от требования использования. Общая черта всех транспондеров, это внутренняя структура, состоящая из двух компонентов: из микрочипа и выполненной антенны [4].

Основа работы RFID системы основывается на чтении информации, которая записывается на чипе метки, и постобработке в считывателе. После демодуляции полученных данных выполняется заложенное действие. Порядок работы представлен на рис. 1 и описан ниже:

- 1. С помощью специализированного оборудования, например, принтера или дубликатора, на радиометку записываются идентификационные данные.
- 2. Транспондер крепится к объекту.
- 3. Считыватель наводит при помощи антенны магнитное поле, при попадании в него транспортер активизируется и сигнал принимает.
- 4. Ответная передача сигнала от транспортера уже на считыватель.
- 5. Приемник внутри считывателя принимает сигнал от радиометки и производит демодуляцию.
- 6. Выполнение полученной команды, это может быть открытие двери в системе контроля доступа, оплата товара, разрешение на посадку на аттракцион, включение сигнализации или запись в базу данных о том, что объект прошел определенную точку [5].

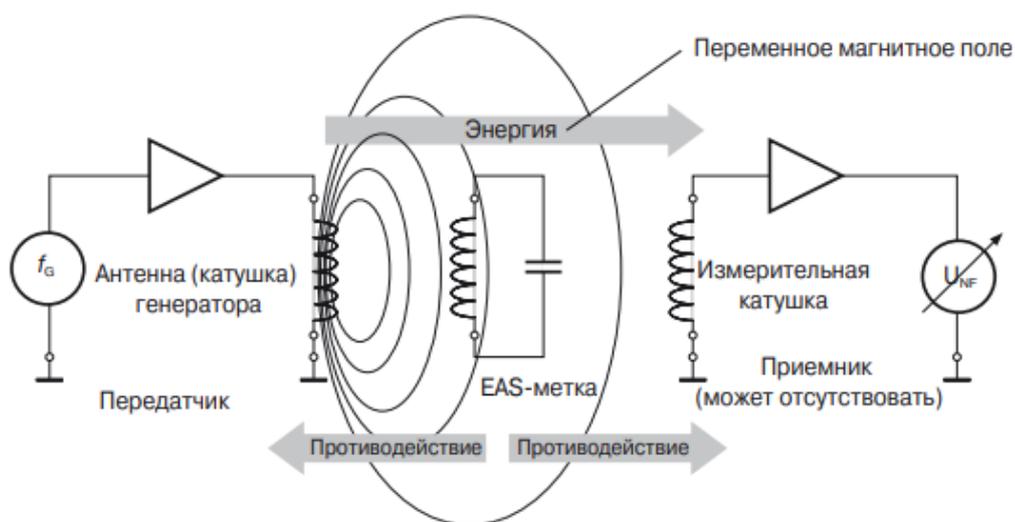


Рис. 1. Принцип работы радиочастотной идентификации

RFID-метки обладают широкой классификацией, которая предопределяет возможную конфигурацию для эффективной работы в любых условиях, независимо от способов их применения. Радиочастотные метки возможно разделить следующим образом, для упрощения представления это показано на рис. 2.

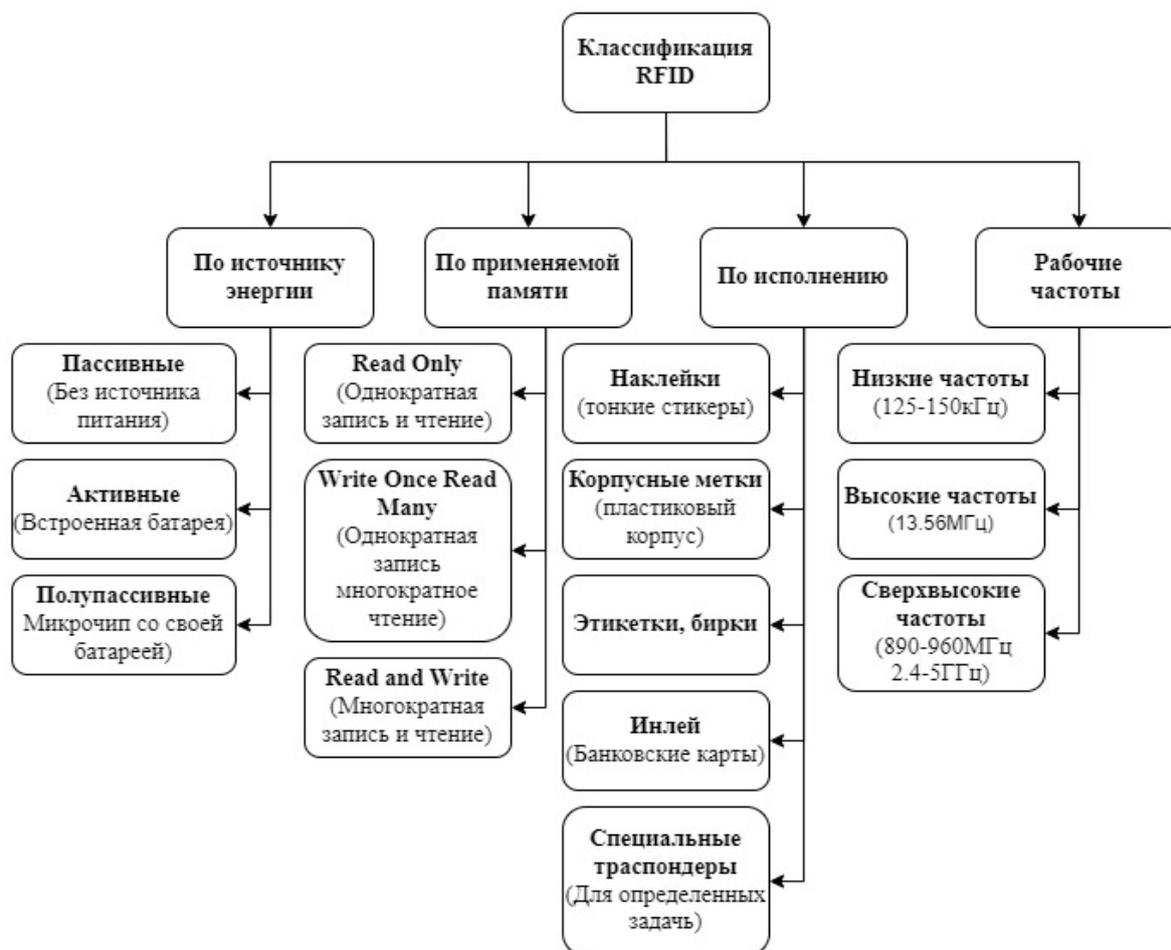


Рис. 2. Классификация RFID-меток

К достоинствам технологии относятся:

- 1. возможность перезаписи;
- 2. отсутствие необходимости в прямой видимости;
- 3. большое расстояние чтения;
- 4. поддержка чтения нескольких меток;
- 5. считывание данных метки при любом её расположении;
- 6. устойчивость к воздействию окружающей среды;
- 7. высокая степень безопасности [6].

Недостатки радиочастотной идентификации:

- 1. Высокая стоимость системы;
- 2. Возможность подмены RFID-меток;
- 3. Сложность самостоятельного изготовления;

- 4. Подверженность помехам в виде электромагнитных полей;
- 5. Недостаточная открытость выработанных стандартов [7].

Сфера применения RFID-технологии постоянно расширяется. Основными областями применения технологии радиочастотной идентификации являются:

1) В библиотеках и архивах представлено оборудованием на пунктах приема и учета выдачи книг, для инвентаризаций и выполнение поиска книг.

2) Идентификация автомобильного транспорта – это системы учета автомобилей, выполняемое в виде оборудования, которое устанавливается на пропускных пунктах.

3) Применение в логистике железнодорожной транспортной сети. Путем повышения эффективности в управление поставками и мониторингом контейнеров, посредством контроля за возвратной тарой, инвентаризацией и учетом продукции.

4) В промышленном производстве представлены в виде системы слежения за специализированной техникой. Через увеличение расстояния работы, точности передачи данных и скорости работы считывателя.

Другой направление развития – это симбиоз с другими имеющимся технологиями, например, как датчики, IoT (Internet of Things) и систем, связанные с искусственным интеллектом (ИИ). Таким образом создавая все более совершенные системы для автоматизаций каких-либо процессов. Примером послужит использование систем умного дома с целью повышения эффективности и комфортной жизни пользователя [9].

Следующий этап развития технологии RFID направлен на улучшение безопасности данных и защищенности системы от кражи данных. Этот процесс связан с разработкой защитных протоколов связи для передачи данных, дополнительное шифрование данных и применение разных методик аутентификации защиты от нелегального доступа. Такое направление становится более важным в настоящее время в связи с повышением угрозы кражи данных, развитие кибербезопасности и способов защиты конфиденциальных данных [10].

Технология облачного хранения и виртуализации данных, с применением радиочастотной идентификации позволит использовать более гибкие и масштабируемые модели. Например, это даст возможность удаленно производить управление и отслеживание благодаря RFID-системам, а также обеспечит централизованное хранение данных и позволит проводить аналитику. Такой подход позволит легко масштабировать системы и предоставлять удобные возможности для управления и анализа данных.

Развивающаяся технология RFID открывает новые возможности для введения инноваций в разных отраслях. С использованием более компактных и производительных устройств, объединяясь с другими технологиями

для повышения безопасности. Также получает важную роль в формировании smart-городов, технологий интернет вещей (IoT). Предоставляя возможность собирать и обмениваться информацией между разными объектами системы, позволяя создавать интеллектуальную городскую среду с высокой эффективностью, с управлением распределением ресурсов, для обеспечения высококачественного образа жизни.

С развитием RFID технологии и ее вхождением в умные-города и IoT, будет появляться еще большее число инновационных идей для улучшения городского управления, и, следовательно, качества жизни в городе.

Список используемых источников

1. Черепков С. Стандарты и тенденции развития RFID-технологий. Компоненты и технологии. 2006. № 1. С. 8–12.
2. Радиочастотная идентификация Режим доступа: <http://www.ibs.ua/spravka/181> (дата обращения: 04.01.2024)
3. Гудин М., Зайцев В. Технология RFID: реалии и перспективы. Компоненты и технологии. 2003. №4. С. 11–13.
4. Финкенцеллер К. RFID-технологии. Справочное пособие / К. Финкенцеллер; перевод с немецкого Союнханова Н.М. М.: Додэка-XXI, 2010. 496 с.
5. Принцип работы технологии RFID и ее применение. Режим доступа: https://rtlservice.com/ru/company/blog/princip_raboty_tehnologii_rfid_i_ee_primenenie (дата обращения: 04.01.2024)
6. RFID-технология. Описание и преимущества использования RFID. Режим доступа: <http://www.rstinvent.ru/about/technology> (дата обращения: 04.01.2024)
7. Григорьев П. В. Особенности технологии RFID и ее применение // Молодой ученый. 2016. № 11. С. 317–322.
8. Бондаревский А. С. Проектирование средств радиочастотной идентификации (RFID) – проблемная ситуация / А.С. Бондаревский, Р.В. Золотов // Современные наукоемкие технологии. 2009. № 9. С. 19–23.
9. Инновации и будущее RFID. Режим доступа: https://rfid-scan.ru/company/news/innovatsii_i_budushchee_rfid (дата обращения: 04.01.2024)
10. Власенко А. В. Обзор инструментов машинного обучения и их применения в области кибербезопасности / А. В. Власенко, П. И. Дзьобан, Р. В. Жук // Прикаспийский журнал: управление и высокие технологии. 2020. № 1. С. 144–155.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ АВТОМАТИЗАЦИИ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ В ИСПДН

Э. В. Бирих, М. Д. Булова, А. А. Казанцев, А. А. Миняев

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

В данной статье представлена разработка программного модуля, написанного на языке Python, позволяющего автоматизировать процесс формирования требований защищенности информации в информационных системах персональных данных в соответствии с требованиями Федеральной службы по техническому и экспортному контролю России.

защита информации; защищенность данных; информационная безопасность; уровень защищенности, автоматизированная система, угроза безопасности, информационная система персональных данных, объект информатизации

В настоящее время проблематикой использования и применения различных информационных технологий является обеспечение безопасности конфиденциальной информации. На законодательном уровне принято очень много различных мер по защите информации, постоянно актуализируются угрозы безопасности, методы защиты. Для обеспечения безопасности необходимо использовать актуальные меры защиты: технические и программные средства.

Мир информационных технологий постоянно растет и угроз безопасности с каждым днем становится все больше. Поэтому важной частью проблемы обеспечения информационной безопасности является определение и анализ актуальных и возможных угроз безопасности ИС (ИС).

В соответствии с приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК № 21) [1] меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановле-

нием Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (далее – Постановление Правительства № 1119) [2], и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

В соответствии с Постановлением Правительства № 1119 при обработке конфиденциальной информации в ИСПДн устанавливаются четыре уровня защищенности (УЗ) и необходимость обеспечения конкретного уровня защищенности устанавливается определенными условиями.

В соответствии с вышесказанными условиями для автоматизации процесса определения уровня защищенности в ИСПДн был разработан программный модуль (далее – desktop-приложение), написанный на языке Python.

При открытии desktop-приложения на экране появляется окно, в котором необходимо выбрать актуальные для своей ИСПДн данные (рис. 1).

Определение уровня защищенности (УЗ)

Какие персональные данные обрабатываются:

- Иные
- Специальные
- Общедоступные
- Биометрические

Тип субъектов:

- Сотрудники
- Не сотрудники

Количество субъектов:

- Более чем 100 000
- Менее чем 100 000

Тип актуальных угроз:

- 1-й тип: Актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей (НДВ) в системном программном обеспечении
- 2-й тип: Актуальны угрозы, связанные с наличием НДВ в прикладном программном обеспечении
- 3-й тип: Актуальны угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении

Результат

Рис. 1. Desktop-приложение для определения УЗ

При регистрации в системе ПДн, пользователю предлагается выбрать тип данных, которые он будет обрабатывать. Существуют несколько вариантов: данные, не относящиеся к другим типам (иные), специальные данные, общедоступные данные и биометрические данные.

Из определения, данные, не относящиеся к другим типам, включают все ПДн, которые не подпадают ни под одну из других категорий данных. Специальные данные охватывают информацию о расовой принадлежности, национальности, политических взглядах, состоянии здоровья и интимной жизни.

Общедоступные данные представляют собой ПДн, полученные из общедоступных источников, созданных в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» [3].

Биометрические данные, в свою очередь, относятся к физиологическим и биометрическим особенностям человека, которые позволяют определить его личность. Оператор использует такие данные для идентификации личности субъекта.

В следующем шаге пользователю предлагается выбрать тип и количество субъектов, чьи данные обрабатываются в системе. По типу субъекты делятся на сотрудников и несотрудников оператора, а по количеству они могут быть более или менее 100 000 [2].

Затем нужно выбрать актуальный тип угроз безопасности. Актуальные угрозы безопасности персональных данных (ПДн) представляют собой совокупность условий и факторов, которые могут создать опасность несанкционированного или случайного доступа к данным в информационной системе (ИС). Это может привести к уничтожению, блокировке данных и совершению других незаконных действий.

Угрозы первого типа являются актуальными для ИС, если они также связаны с наличием недокументированных или недеklarированных возможностей (НДВ) в системном программном обеспечении (СПО), используемом в ИС [2].

Угрозы второго типа являются актуальными для информационных систем (ИС), если они включают в себя угрозы, связанные с наличием НДВ в прикладном программном обеспечении (ППО), используемом в ИС [2].

Угрозы третьего типа являются актуальными для ИС, если они включают в себя угрозы, которые не связаны с наличием НДВ в СПО и ППО, используемом в ИС [2].

Результат выбранных данных можно увидеть на рис. 2-3.

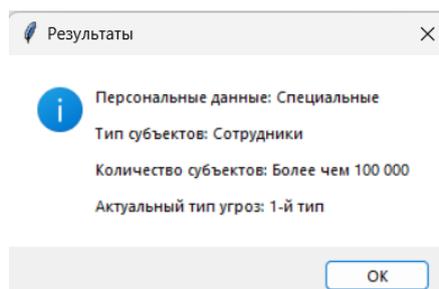


Рис. 2. Фиксирование введенных данных

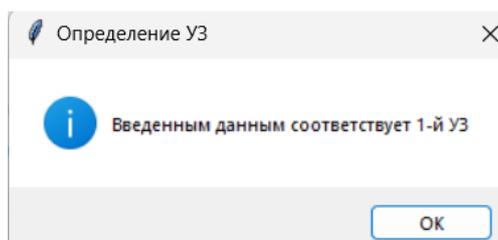


Рис. 3. Определение УЗ

Для формирования требований защиты информации в ИСПДн используется ранее созданная база данных на основе Приказа ФСТЭК № 21 [1]. В соответствии с рассчитанным УЗ модуль открывает обязательные требования (меры), соответствующие данному УЗ (рис. 4).

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Уровень защищенности ПДн
		1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, односторонняя передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование	+

Рис. 4. Требования защиты, соответствующие рассчитанному УЗ

Следующим шагом пользователю предлагается выбрать те подсистемы, которые не реализованы в его ИС (рис. 5). Выбрав необходимые подсистемы, пользователю предлагается пример средств защиты информации, при помощи применения которых можно закрыть недостающую подсистему (рис. 6). Если пользователь ничего не выбрал, то на экране отображается окно, обозначающее завершение работы программы (рис. 7). Ниже, на рисунке 8, можно увидеть блок-схему работы desktop-приложения.



Рис. 5. Выбор нереализованных мер

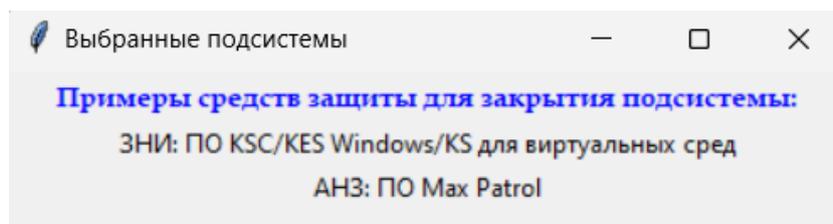


Рис. 6. Пример средств защиты для выбранной подсистемы

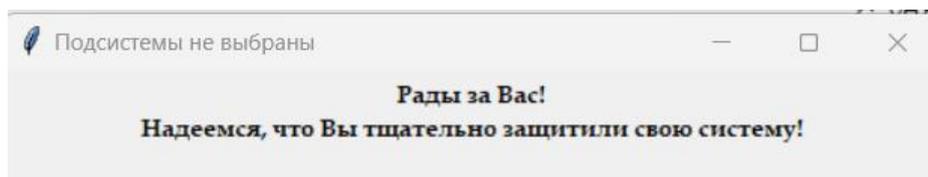


Рис. 7. Завершение работы программы

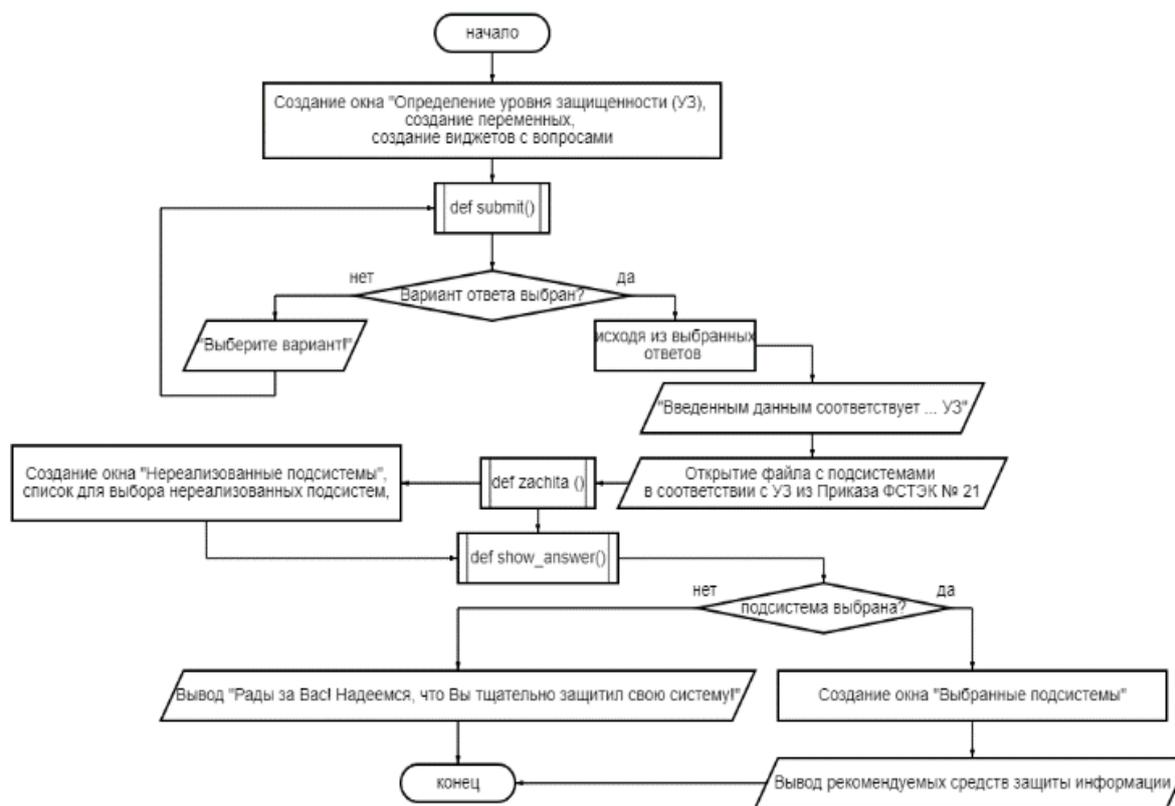


Рис. 8. Блок-схема работы алгоритма программы

Заключение

В этой статье был рассмотрен разработанный программный модуль для автоматизации определения УЗ. Данный модуль поможет перепроверить персонал и уменьшить затраты времени на данную процедуру для ИСПДн. Также он дает возможность самостоятельного определения УЗ и формирования необходимых требований без привлечения компаний специализирующихся на проведении мероприятий по определению УЗ и формированию мер, необходимых для защиты ИСПДн.

Список используемых источников

1. Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения: 25.10.2023)
2. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL: <https://base.garant.ru/70252506> (дата обращения: 25.10.2023)
3. Федеральный закон № 152 «О персональных данных» URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=447363> (дата обращения: 25.10.2023)

УДК 004
ГРНТИ 28.29.03

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПРИНЯТИЯ РЕШЕНИЙ В ЗАДАЧАХ КОНФИГУРИРОВАНИЯ ПРОГРАММНО- АППАРАТНЫХ КОМПЛЕКСОВ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

П. П. Бовшик, В. Л. Литвинов

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

В современном мире, где практически каждое предприятие борется за сокращение времени простоя рабочей деятельности и соответствующих экономических затрат из-за человеческого фактора, остро встает вопрос автоматизации того или иного процесса. Для решения данного вопроса уже сейчас применяются системы поддержки принятия решений. В работе рассмотрена концепция принятия решений с целью автоматизации процесса работы системных администраторов. В качестве результата научного исследования представлена базовая концепция принятия решений в задачах конфигурирования программно-аппаратных комплексов для хранения и обработки информации.

система поддержки принятия решений, конфигурирование программно-аппаратных комплексов, хранение информации, обработка информации

На сегодняшний день, одним из самых современных решений по автоматизации каких-либо процессов является система поддержки принятия решений (далее – СППР) [1-3]. Подобные системы уже применяются в банковской сфере для финансового анализа [4-6], для автоматизации процесса управления проектами [7-9], СППР осуществляют поддержку при проведении медицинской диагностики [10], применяются в маркетинговых исследованиях [11] и во многих других областях и задачах.

Главные задачи систем поддержки принятия решений включают в себя [12]:

- сбор и анализ данных для принятия решений;
- построение моделей и сценариев для прогнозирования результатов;
- оценка альтернативных вариантов и выбор оптимального решения;
- предоставление рекомендаций и поддержка в принятии решений.

Другими словами, целью СППР является улучшение процесса принятия решений, в том числе посредством сокращения роли человеческого фактора, а задачи отражают методы достижения цели СППР.

В рамках данной работы будет рассмотрен процесс принятия решений в задачах конфигурирования программно-аппаратных комплексов (далее – ПАК) хранения и обработки информации для автоматизации работы таких

специалистов как системные инженеры и администраторы при разработке соответствующих ПАК. Целью исследования является разработка концепции автоматизации процесса принятия решений в задачах конфигурирования программно-аппаратных комплексов хранения и обработки информации. Для достижения поставленной цели будут рассмотрены следующие вопросы:

- определение проблемы;
- определение Лица, Принимающего Решение (ЛПР);
- определение формализации модели;
- постановка задач принятия решений и формулировка ряда утверждений, характеризующих СППР;
- определение метода принятия решений;
- определение архитектуры СППР.

Определение проблемы и ЛПР

Цель работы – минимизировать «механическую» работу человека в процессе конфигурирования ПАК.

Рассмотрим, в каком виде процесс конфигурирования программно-аппаратных комплексов представлен сейчас. Рассматриваемый процесс содержит следующие этапы (в общем виде):

1. Определение требований к ПАК согласно ТЗ;
2. Определение общих и числовых (по возможности) технических характеристик ПАК, удовлетворяющим требованиям ТЗ;
3. Подбор аппаратного и программного обеспечения, удовлетворяющего требуемым техническим характеристикам;
4. Утверждение подобранного обеспечения;
5. Поиск поставщиков, закупка и логистика подобранного оборудования и программного обеспечения;
6. Получение, монтаж и настройка ПАК.

На данный момент этот процесс нельзя назвать автоматизированным в большей степени, так как конфигурирование от уточнения технического задания до подбора необходимого аппаратного и программного обеспечения осуществляется специалистом, а именно системным инженером, вручную на просторах сети «Интернет», или же используя опыт прошлых разработок. То есть фактическое «механическое» состояние процесса не соответствует желаемому «автоматизированному», что говорит о наличии проблемы функционирования системы, которая в данный момент не обеспечивает достижение цели.

В рамках данной статьи будет рассматриваться вопрос минимизации «механической» работы человека в процессе конфигурирования ПАК на

этапе подбора аппаратного и программного обеспечения. В дальнейших работах будет рассмотрена возможность автоматизации процесса определения требований и технических характеристик ПАК согласно ТЗ.

В рассматриваемой системе субъектом решения является индивидуальное лицо, принимающее решение – системный инженер.

Постановка задачи принятия решений

В условиях необходимости составления спецификации (выбора оборудования) для конфигурирования ПАК хранения и обработки информации, располагаемого времени, уточненного ЛПР, и ресурсов, уточненных ЛПР, опираясь на цели и ограничения, уточненные ЛПР, необходимо произвести оценку предпочтений и сформулировать некоторое множество альтернативных решений руководствуясь критериями, определенными ЛПР.

Определение метода оценивания и выбора решений

Для решения подобной слабоструктурированной многокритериальной задачи подходит метод анализа иерархий [13-15]. Данный метод позволит учитывать несколько критериев оценивания и выбора, определить приоритеты критериев сравнения и вычислить альтернативное решение с максимальным значением приоритета.

Критерии и их приоритеты определяются для каждого вида оборудования и ПАК отдельно ЛПР. Конечным критерием выбора альтернативного решения для конфигурирования ПАК является совместимость выбранного оборудования.

Определение архитектуры СППР

Исходя из задачи, сформулированной ранее, обобщенная архитектура рассматриваемой системы принятия решений может включать в себя [16]: блок ввода данных (БВД), блок поиска данных/блок пополнения данных (БПД), валидатор, базу знаний (БЗ), аналитическую базу данных (АБД), хранилище данных (ХД), блок анализа данных (БАД), блок методов принятия решений (БМПР) и блок принятия решений (БПР) (рис. 1).

На начальном этапе имеет смысл рассматривать систему принятия решений без использования интеллектуальных методов анализа с целью упрощения алгоритма работы, но в дальнейшем, при корректной работе системы, включить соответствующие элементы в алгоритм и внедрить в работу системы.

Необходимым элементом предлагаемой структуры СППР является валидатор, который проверяет и «очищает» найденные БПД или вводимые ЛПР данные. Механизм пополнения данных (БПД) на начальном этапе мо-

жет осуществляться ЛПР, но в перспективе развития системы не исключается возможность пополнения данных автоматически с помощью сети Интернет.

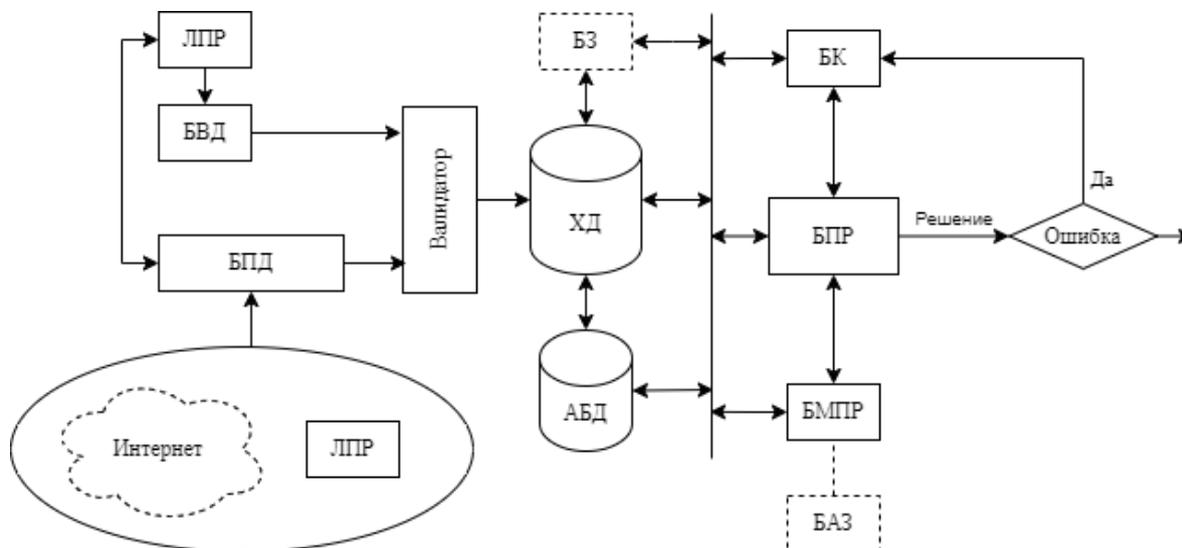


Рис. 1. Обобщенная архитектура СППР

Эта работа является началом исследования вопроса автоматизации процесса принятия решений в задачах конфигурирования программно-аппаратных комплексов и определяет базовую концепцию системы принятия решений, которая в дальнейшем будет рассматриваться более детально и по мере продвижения исследования модернизироваться. В рамках продолжения данной работы будут рассмотрены метод анализа иерархий в задаче конфигурирования программной и аппаратной частей ПАК; автоматизация процесса оценки требований технического задания; интеллектуальные методы анализа данных и конфигурирования базы знаний и многое другое.

Список используемых источников

1. Назарова О. О. Эволюция систем поддержки принятия решений / О. О. Назарова // Дневник науки. 2022. № 3(63).
2. Шагарова И. Х. Обзор существующих систем поддержки принятия решения / И. Х. Шагарова, Е. С. Морозова // Современные проблемы научной деятельности. перспективы внедрения инновационных решений: сборник статей Международной научно-практической конференции, Челябинск, 10 июня 2019 года. Челябинск: Общество с ограниченной ответственностью "Аэтерна", 2019. С. 53-55.
3. Кузнецов М. А. Современная классификация систем поддержки принятия решений / М. А. Кузнецов, С. С. Пономарев // Прикаспийский журнал: управление и высокие технологии. 2009. № 3(7). С. 52–58.
4. Глушенко С. А. Система нечеткого моделирования рисков инвестиционно-строительных проектов / С. А. Глушенко, А. И. Долженко // Бизнес-информатика. 2015. № 2(32). С. 48–58.

5. Кравченко Т. К. Аналитическое обоснование выбора объекта венчурных инвестиций / Т. К. Кравченко // Финансовая аналитика: проблемы и решения. 2015. № 41(275). С. 35–46.
6. Колодко Д. В. Экспертное краткосрочное прогнозирование валютного рынка Forex / Д. В. Колодко // Управление экономическими системами: электронный научный журнал. 2012. № 4(40). С. 99.
7. Сазанова Л. А. Применение современных СППР для решения управленческих задач / Л. А. Сазанова // Наука и бизнес: пути развития. 2022. № 5(131). С. 60–63.
8. Колосов С. П. Применение метода построения моментальных состояний в мониторинге производственно-технологических процессов в интеграции с СППР, с целью оптимизации документооборота (на примере мебельного производства) / С. П. Колосов // Стратегия социально-экономического развития общества: управленческие, правовые, хозяйственные аспекты: Материалы Международной научно-практической конференции: в 2-х томах, Курск, 25 ноября 2011 года / Ответственный редактор Горохов А. А. Том 1. Курск: Юго-Западный государственный университет, 2011. С. 156–165.
9. Фомичева Т. Л. Использование информационных систем поддержки принятия решений как способ повышения эффективности работы предприятия / Т. Л. Фомичева, А. М. Афонин // Инновационная траектория развития современной науки: теория, методология и практика: сборник статей Международной научно-практической конференции, Петрозаводск, 29 октября 2019 года / МЦНП «Новая наука». Петрозаводск: Международный центр научного партнерства «Новая Наука», 2019. С. 132–136.
10. Загорулько Г. Б. Методология разработки интеллектуальных СППР и ее применение для задач медицинской диагностики / Г. Б. Загорулько // Информационные технологии и системы: Труды Седьмой Всероссийской научной конференции с международным участием, Ханты-Мансийск, 12–16 марта 2019 года / Ответственные редакторы Ю.С. Попков, А.В. Мельников. Ханты-Мансийск: Автономное учреждение Ханты-Мансийского автономного округа Югры «Югорский научно-исследовательский институт информационных технологий», 2019. С. 211–216.
11. Ахиджак Д. А. Перспективы использования систем поддержки принятия решений в маркетинговых исследованиях / Д. А. Ахиджак // Аллея науки. 2018. Т. 4. № 11(27). С. 944–951.
12. Засканов В. Г. Системы поддержки принятия решений: электрон. курс в системе дистанц. обучения Moodle / М-во образования и науки РФ, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т); авт.-сост. В. Г. Засканов, Д. Ю. Иванов, Г. М. Гришанов. Электрон. текстовые и граф. дан. Самара, 2013.
13. Богданова П. А, Сахаров Д. М, Васильева Т. В. Обзор методов многокритериальной оптимизации в задачах принятия решений // Инновационные аспекты развития науки и техники. 2021. № 6. (дата обращения: 15.02.2024)
14. Курбанова Э. Р. Метод анализа иерархий: характеристика / Э. Р. Курбанова // Форум молодых ученых. 2019. № 5(33). С. 749–752.
15. Латыпова В. А. Сравнительный анализ и выбор программных средств, реализующих метод анализа иерархий / В. А. Латыпова // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 4(23). С. 322–347.
16. Ключко В. И, Шумков Е. А, Власенко А. В, Карнизьян Р. О. Архитектуры систем поддержки принятия решений // Научный журнал КубГАУ. 2013. № 86. URL: <https://cyberleninka.ru/article/n/arhitektury-sistem-podderzhki-prinyatiya-resheniy> (дата обращения: 15.02.2024)

УДК 621.391.
ГРНТИ 49.46.29

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СВЕТОВОГО ПУТИ В УПРАВЛЕНИИ СПЕКТРАЛЬНЫМ РЕСУРСОМ ОПТИЧЕСКИХ ТРАНСПОРТНЫХ СЕТЕЙ

А. П. Бойко¹, П. И. Кузин², Е. И. Кузина¹, И. А. Потапов¹, Н. А. Усов¹

¹Военная академия связи имени Маршала Советского Союза С. М. Буденного

²Санкт-Петербургский Государственный лесотехнический университет имени С. М. Кирова

В статье дано строгое определение светового пути. Понятие светового пути расширено и уточнено за счёт объединения маршрута прохождения и назначенного спектра оптического сигнала. Множество допустимых световых путей предлагается формировать на основе отношения мощности оптического сигнала к мощности шума в полосе пропускания светового пути для конкретного вида сигнала. Представлен ряд критериев оптимальности для решения задач поиска и распределения световых путей. Разработана математическая модель светового пути, позволяющая повысить эффективность управления спектральным ресурсом в оптических транспортных сетях. На основе предложенной модели возможно решение подзадач поиска маршрутов световых путей с учётом требований к непересекаемости спектров, смежности элементарных частотных интервалов каждого светового пути, непрерывности спектра на всем маршруте.

оптическая транспортная сеть, световые пути, качество передачи, распределение спектра

Введение. Современные оптические транспортные сети (ОТС) строятся на базе волоконно-оптических систем передачи со спектральным разделением каналов (ВОСП СР). В настоящее время оптические сети связи формируются по принципу "точка-точка", при этом оптические сигналы преобразуются в электрический вид в каждом узле и заново в оптический для дальнейшей передачи. Затраты на электронную коммутацию и обработку данных на узлах потенциально могут быть очень высокими.

Особый интерес в ОТС на основе ВОСП СР, представляют полностью оптические соединения между двумя корреспондирующими узлами, позволяющие передавать оптические сигналы без опто-электро-оптического (ОЕО-) преобразования в транзитных узлах. Образованные отдельными спектральными каналами между двумя соседними узлами, данные оптические соединения являют собой составные оптические каналы и носят название световых путей (lightpath) [1–3]. Отсутствие ОЕО-преобразования в процессе коммутации, мультиплексирования и ретрансляции оптических сигналов способствует тому, что оптические сети на основе концепции световых путей имеют большой ряд преимуществ [4–6].

Математическая модель светового пути. Для моделирования светового пути, представим ОТС в виде неориентированного графа $G(A, E, S)$, где: $A = \{a_i\}$, $i = \overline{1, N_y}$ – множество узлов сети; $E = \{e_{ij}\}$, $i \neq j$, $i, j = \overline{1, N_y}$ – множество ВОЛС между узлами сети, $S = \{s_{ij}^{n,m}\}$, $i \neq j$, $i, j = \overline{1, N_y}$ – спектральный ресурс сети. Соединения между узлами на основе волоконно-оптических линий связи (ВОЛС) являются двунаправленными, и на них базируются противоположно направленные световые пути, а используемые в узлах транспондеры действуют одновременно как передатчики и приемники. Элемент $s_{ij}^{n,m} \in S$ характеризует доступный для передачи оптических сигналов диапазон частот в соответствующей ВОЛС $e_{ij} \in E$. Так, $s_{12}^{10,40}$ означает, что в ВОЛС e_{12} для передачи сигналов выделен поддиапазон частот шириной $\Delta f_{12} = m \cdot \Delta f^{\text{эчи}} = 40 \cdot 12.5 = 500$ ГГц и граничными значениями нижней (1) и верхней (2) частот:

$$f_{12}^{\text{H}} = f_{12}^{\text{Ц}} - \frac{\Delta f_{12}}{2} = 193.1 + 10 \cdot 0.00625 - \frac{0.5}{2} = 192.9125 \text{ ТГц}, \quad (1)$$

$$f_{12}^{\text{B}} = f_{12}^{\text{Ц}} + \frac{\Delta f_{12}}{2} = 193.1 + 10 \cdot 0.00625 + \frac{0.5}{2} = 193,4125 \text{ ТГц}. \quad (2)$$

Формирование световых путей в ОТС осуществляется на основе требований к скоростям передачи в цифровых каналах заданного качества $B^{\text{TP}} = \{b_k^{\text{TP}}\}$, $k = \overline{1, K}$ между корреспондирующими парами узлов $Z = \{z_k | z_k = (a_i, a_j), i \neq j\}$, где $a_i, a_j \in A$.

Расширим понятие светового пути и добавим в его описание назначенные центральную частоту и полосу пропускания. Тогда под световым путем будем понимать совокупность смежных элементарным частотным интервалам (ЭЧИ) в последовательности ВОЛС, обеспечивающих распространение оптического сигнала в заданной полосе частот между двумя узлами без оптико-электро-оптического преобразования.

Более строго световой путь $LP_{ij}^{n,m}$ из a_i в a_j определяется, как упорядоченная последовательность ВОЛС $(e_{iy}, e_{yu}, \dots, e_{nj})$, начинающаяся в узле a_i , заканчивающаяся в узле a_j и не проходящая через один и тот же узел ОТС ВСР дважды, причем каждые две соседних ВОЛС имеют общий узел подключения, и в каждой ВОЛС выделен одинаковый набор смежных ЭЧИ в диапазоне $f_{LP_{ij}^{n,m}}^{\text{H}} \dots f_{LP_{ij}^{n,m}}^{\text{B}}$, где $f_{LP_{ij}^{n,m}}^{\text{H}}$ и $f_{LP_{ij}^{n,m}}^{\text{B}}$ – соответственно нижняя и верхняя границы частот светового пути $LP_{ij}^{n,m}$, определяемые выражениями:

$$f_{LP_{ij}^{n,m}}^{\text{H}} = 193.1 + n \cdot 0.00625 - \frac{m \cdot \Delta f^{\text{эчи}}}{2}, \quad (3)$$

$$f_{LP_{ij}^{n,m}}^{\text{B}} = 193.1 + n \cdot 0.00625 + \frac{m \cdot \Delta f^{\text{эчи}}}{2}. \quad (4)$$

Ширина светового пути $\Delta f_{LP_{ij}^{n,m}}^K$ определяется выражением:

$$\Delta f_{LP_{ij}^{n,m}}^K = m \cdot \Delta f^{\text{ЭЧИ}} = f_{LP_{ij}^{n,m}}^B - f_{LP_{ij}^{n,m}}^H. \quad (5)$$

Так как световые пути формируются для КПУ, можно заменить индексы i, j на индекс $k = \overline{1, K}$ если узлы a_i и a_j образуют k -ю КПУ. Кроме того, множество световых путей из a_i в a_j может содержать элементы с одинаковыми значениями n и m , но отличающиеся друг от друга маршрутами. Чтобы их различать введем дополнительный индекс v . Тогда световой путь k -й КПУ $z_k = (a_i, a_j)$ с v -м маршрутом и полосой пропускания определяемой индексами n и m , будет обозначаться так: $LP_{k,v}^{n,m}$. Подмножества ВОЛС и узлов, через которые проходит световой путь $LP_{k,v}^{n,m}$ соответственно можно обозначить, как $E_{k,v}$ и $A_{k,v}$, а занимаемую полосу частот, как $(f_{LP_{k,v}^{n,m}}^H, f_{LP_{k,v}^{n,m}}^B)$.

Множество всех возможных световых путей k -й КПУ на основе v -го маршрута будем обозначать:

$$LP_{k,v} = \{LP_{k,v}^{n,m}\}.$$

Тогда множество всех возможных световых путей k -й КПУ имеет вид:

$$LP_k = \bigcup LP_{k,v}.$$

В общем случае в сети могут присутствовать световые пути из a_i в a_j с одинаковым маршрутом, но в непересекающихся частотных областях. Кроме того, между полосами пропускания соседних световых путей должен быть дополнительный интервал частот, называемый защитной полосой. Обычно защитная полоса определяется в процентах от ширины полосы пропускания каждого оптического канала [7, 8]. Одно из распространенных значений защитной полосы составляет 10 % от ширины полосы пропускания канала. Например, если ширина полосы пропускания канала составляет , то защитная полоса будет составлять $\Delta f^3 = 5$ ГГц. Значение защитной полосы может быть адаптировано в реальном времени в зависимости от динамики сетевой нагрузки, уровня помех или других факторов. Защитная полоса может быть задана значением количества ЭЧИ: m^3 . Чаще всего, значение защитной полосы между световыми путями составляет один ЭЧИ: $m^3 = 1$. Математически, условие непересечения спектров двух световых путей с учётом защитной полосы можно выразить с помощью индексов n и m . Разница между n_1 и n_2 двух световых путей при заданных m_1 и m_2 и защитной полосой равной m^3 ЭЧИ должна быть:

$$|n_1 - n_2| \geq m_1 + m_2 + 2 \cdot m^3, \quad (6)$$

где множитель «2» означает, что ширина 1 ЭЧИ равна двум шагам дискретизации спектра $\Delta f^{\text{эчи}} = 2 \cdot 6.25$ ГГц.

При назначении частот световому пути необходимо, чтобы его полоса пропускания оставалась в пределах спектрального ресурса всех ВОЛС принадлежащих ν -му маршруту, т.е. $f_{LP_{k,v}}^H \geq f_{ij}^H$, $f_{LP_{k,v}}^B \leq f_{ij}^B$ для $\forall ij: e_{ij} \in E_{k,v}$. С помощью выражений (1)-(4) можно сформулировать условия в виде:

$$\begin{cases} 193.1 + n_{LP_{k,v}} \cdot 0.00625 - \frac{m_{LP_{k,v}} \cdot \Delta f^{\text{эчи}}}{2} \geq 193.1 + n_{e_{ij}} \cdot 0.00625 - \frac{m_{e_{ij}} \cdot \Delta f^{\text{эчи}}}{2} \\ 193.1 + n_{LP_{k,v}} \cdot 0.00625 + \frac{m_{LP_{k,v}} \cdot \Delta f^{\text{эчи}}}{2} \geq 193.1 + n_{e_{ij}} \cdot 0.00625 + \frac{m_{e_{ij}} \cdot \Delta f^{\text{эчи}}}{2} \Leftrightarrow \\ \begin{cases} n_{LP_{k,v}} - m_{LP_{k,v}} \geq n_{e_{ij}} - m_{e_{ij}} \\ n_{LP_{k,v}} + m_{LP_{k,v}} \geq n_{e_{ij}} + m_{e_{ij}} \end{cases} \forall e_{ij} \in E_{k,v}, \end{cases}$$

где $n_{LP_{k,v}}, n_{e_{ij}} \in \mathbb{Z}$ и $m_{LP_{k,v}}, m_{e_{ij}} \in \mathbb{Z}^+$ – числа, используемые для описания спектрального ресурса и полосы пропускания светового пути [9].

Предположим, что каждый ЭЧИ $\Delta f^{\text{эчи}}$ обеспечивает скорость передачи $B^{\text{эчи}} = M \cdot \Delta f^{\text{эчи}}$, где M – уровень модуляции, определяющий количество битов, передаваемых одним символом. Тогда скорость передачи в каждом ЭЧИ при использовании сигналов BPSK, QPSK, 8-QAM, 16-QAM, 32-QAM, 64-QAM, будет составлять: 12.5 Гбит/с, $2 \cdot 12.5$ Гбит/с, $3 \cdot 12.5$ Гбит/с, $4 \cdot 12.5$ Гбит/с, $5 \cdot 12.5$ Гбит/с, $6 \cdot 12.5$ Гбит/с соответственно, а множество уровней модуляции составит: $M \in \{1, 2, 3, 4, 5, 6\}$. На основе выражения (7), полученного в [9], запросы на соединения между корреспондирующими узлами могут быть выражены в количестве требуемых ЭЧИ $m^{\text{тр}} = \{m_k^{\text{тр}}\}$, $k = \overline{1, K}$, для формирования цифровых каналов с заданной скоростью передачи:

$$m^{\text{тр}} = \left\lceil \frac{b^{\text{тр}}}{M \cdot \Delta f^{\text{эчи}}} \right\rceil + m^3. \quad (7)$$

Для передачи формируемого оптического сигнала $*b$ для k -й КПУ, из множества всех возможных световых путей LP_k формируется множество допустимых световых путей $LP_k^A \in LP_k$ между узлами a_i и a_j ($z_k = (a_i, a_j)$) таких, что $OSNR_{\text{вх}j}$ на входе j -го узла не меньше $OSNR^T + A_3$, где $A_3 \cong 3 \dots 5$ дБ – запас по $OSNR$, $*b$ – скорость передачи сигнала, $*$ – вид передаваемого сигнала.

Заключение. Таким образом, множество световых путей $LP_k^A(*b)$, допустимых для передачи сигнала $*b$ между узлами z_k – это совокупность таких световых путей, которые обеспечивают передачу оптических сигналов с $OSNR_{\text{вх}j}$ не хуже требуемого (с запасом) $OSNR^T + A_3$:

$$LP_k^A(*b) = \{LP_k \mid OSNR_{\text{вх}j}(LP_k) \geq OSNR^T + A_3\}.$$

На основе модели светового пути, представленной в статье, возможно решение множества оптимизационных задач. Дальнейшие направления исследований необходимо направить на повышение объективности оценки качества световых путей с учётом линейных и нелинейных искажений оптических сигналов, а также взаимных влияний совместно-передаваемых сигналов с различными видами модуляции и/или типами кодирования.

Список используемых источников

1. Липатников В. А., Кузин П. И., Метод повышения оперативности смены параметров адаптации при приеме информации в системах радиосвязи КВ- и УКВ-диапазонов // Автоматизация процессов управления. 2016. № 4 (46). С. 18–22.
2. Lipatnikov V. A., Kuzin P. I., Rabin A. V. The method of increasing the reliability of noise immunity when receiving information in radio communication systems of the shf and ehf ranges. В сборнике: Journal of Physics: Conference Series. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnoyarsk, Russian Federation, 25 сентября 2020 г. P. 52100.
3. Липатников В. А., Кузин П. И., Рабин А. В. Передачи сигналов в каналах связи с замираниями Накагами // Успехи современной радиоэлектроники. М.: «Издательство Радиотехника». 2019. № 11. С. 71–78.
4. Rabin A. V., Lipatnikov V. A., Kuzin P. I. Signal protection methods in channels with nakagami fading. В сборнике: JOP Conference Series: Metrological Support of Innovative Technologies. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnoyarsk, Russia, 25 сентября 2020 г. P. 52078.
5. Липатников В. А., Кузин П. И., Рабин А. В. Метод повышения надежности помехозащищенности при приеме информации в системах радиосвязи СВЧ- и КВЧ-диапазонов // Радиотехника. 2020. Т. 84. № 8(16). С. 5–12.
6. Бойко А. П., Кузин П. И. Совершенствование математических моделей волоконно-оптического линейного тракта // Вестник компьютерных и информационных технологий. 2022. Т. 19. № 2(212). С. 26–31.
7. Бойко А. П., Кузин П. И. К проблеме автоматического обнаружения топологии физического уровня оптической транспортной сети специального назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 5-6(179-180). С. 65–70.
8. Lipatnikov V., Kuzin P., Rabin A. Methodology for determining the connectivity of communication networks. В сборнике: AIP Conference Proceedings. Krasnoyarsk Scientific Centre of the Siberian Branch of the Russian Academy of Sciences. Melville, New York, United States of America, 2021. P. 70059.
9. ITU-T Rec. G.694.1, Spectral grids for WDM applications: DWDM frequency grid.

УДК 004.054
ГРНТИ 81.93.29

АНАЛИЗ ПОРЯДКА ВЗАИМОДЕЙСТВИЯ ПРОГРАММНЫХ СРЕДСТВ, УСТАНОВЛЕННЫХ НА ПОЧТОВЫХ СЕРВЕРАХ СИСТЕМЫ ЭЛЕКТРОННОЙ ПОЧТЫ

К. М. Большебратский, М. М. Добрышин

Академия Федеральной службы охраны Российской Федерации

Статья представляет анализ порядка взаимодействия программных средств, установленных на почтовых серверах системы электронной почты. Исследование направлено на выявление и анализ последовательности действий и взаимодействия компонентов программного обеспечения, работающих на почтовых серверах. Полученные результаты могут применяться для повышения эффективности работы почтовых систем путем обеспечения их защищенности за счет анализа возможности взаимодействия между программами и их уязвимостями.

электронная почта, межпроцессное взаимодействие, сервер

Задачу обеспечения информационной безопасности средств обработки, хранения и передачи информации, в том числе серверов электронной почты, возможно представить, как задачу выявления известных уязвимостей, с целью их устранения и недопущения реализации компьютерных атак. Однако современный этап развития средств и способов реализации атак свидетельствует о том, что для достижения цели злоумышленники эксплуатируют несколько уязвимостей [1].

С целью выявления возможных переходов между уязвимостями в работе проведен анализ различных вариантов взаимодействия программного обеспечения, которое может устанавливаться на почтовом сервере. Для примера рассмотрим почтовый сервер системы электронной почты, функционирующий на базе операционной системы Astra Linux Server версии «Смоленск» v. 1.6 с версией ядра 4.5.13-1-generic.

В комплект программного обеспечения входит:

1. Пользовательские приложения:
 - Средства работы с документами (пакет Libreoffice);
 - Средства электронной почты (Thunderbird);
 - Web-браузер Firefox;
 - Средства работы с мультимедиа и изображениями.
2. Серверные приложения:
 - Система управления базами данных (PostgreSQL);
 - Комплекс программ печати и маркировки документов;

- Комплекс программ ЭП (DOVECOT, CXIM);
- WEB-сервер;
- Комплекс программ резервного копирования и восстановления (BACULA, rsync, tar).

В операционных системах семейства UNIX реализация взаимодействия процессов подразделяется на несколько видов [2]. Классификация видов взаимодействия процессов приведена на рис. 1.

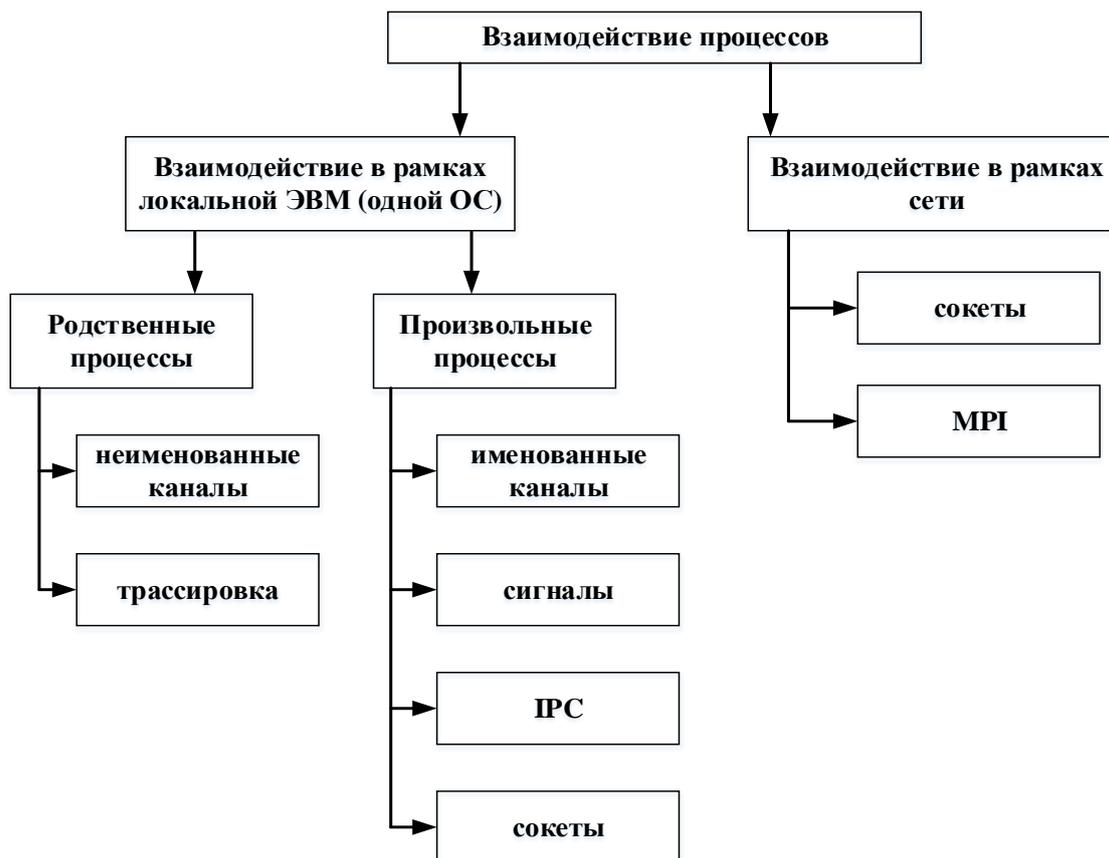


Рис. 1. Классификация видов взаимодействия процессов

В рамках рассматриваемого в данной работе объекта возможны все приведенные виды межпроцессного взаимодействия, рассмотрим их подробнее [3].

1. **Сигналы** в операционной системе (ОС) уведомляют о различных событиях, их инициируют другие процессы или сама ОС. Они могут указывать на строго определенные ситуации, такие как завершение процесса или нажатие комбинации клавиш. Количество сигналов около 30, каждый имеет уникальный номер и имя. Процессы могут реагировать на сигналы стандартным образом, устанавливая специальные обработчики или игнорировать их.

2. **Именованные каналы**, или FIFO, позволяют процессам связываться друг с другом независимо от времени создания канала. При открытии

канала процесс блокируется до того момента, пока другой процесс не откроет его для противоположной операции. Есть возможность избежать блокировки при открытии с помощью специального флага.

3. **Трассировка процессов** предоставляет одному процессу контроль над выполнением другого. В UNIX это возможно только между родственными процессами. Трассировка начинается после получения разрешения от трассируемого процесса и позволяет анализировать и изменять данные в его адресном пространстве.

4. **Механизмы межпроцессного взаимодействия (IPC)** включают очереди сообщений, семафоры и разделяемую память, они широко применяются в различных версиях UNIX.

5. **Сокеты** представляют собой средство взаимодействия между процессами в операционной системе. Процессы создают и конфигурируют сокеты для установления соединения, после чего могут обмениваться данными. По завершении взаимодействия сокеты уничтожаются. Этот механизм широко используется при разработке клиент-серверных приложений.

6. **Библиотека MPI (Message Passing Interface)** позволяет организовать взаимодействие параллельных процессов независимо от их местонахождения. Она предоставляет набор функций для обмена данными между процессами через передачу сообщений. MPI автоматически выбирает оптимальный механизм обмена данными в зависимости от характеристик вычислительной системы и взаимного расположения процессов.

7. **Неименованные каналы (pipe)** представляют собой средство взаимодействия между процессами в операционной системе. Создаются они с помощью системного вызова `pipe()`, который выделяет буфер ограниченного размера в оперативной памяти и возвращает два файловых дескриптора: один для записи в канал, другой для чтения из него.

Отличия каналов от обычных файлов:

- К каналу невозможен доступ по имени, единственный способ использования – через файловые дескрипторы.
- Канал существует только в рамках процесса, который его создал, и автоматически уничтожается при закрытии всех связанных с ним дескрипторов.
- Канал работает по принципу FIFO (первым пришел, первым обслужен), операция позиционирования недоступна.
- При чтении из канала процесс блокируется, если данных недостаточно. При записи процесс блокируется, если канал переполнен.
- Система гарантирует атомарность операции записи, чтобы данные не перемешивались при одновременной записи нескольких процессов.

Примером межпроцессного взаимодействия на сервере электронной почты может являться процесс получения и сохранения сообщения в хранилище сообщений. Данный процесс для наглядности изображен на рис. 2.

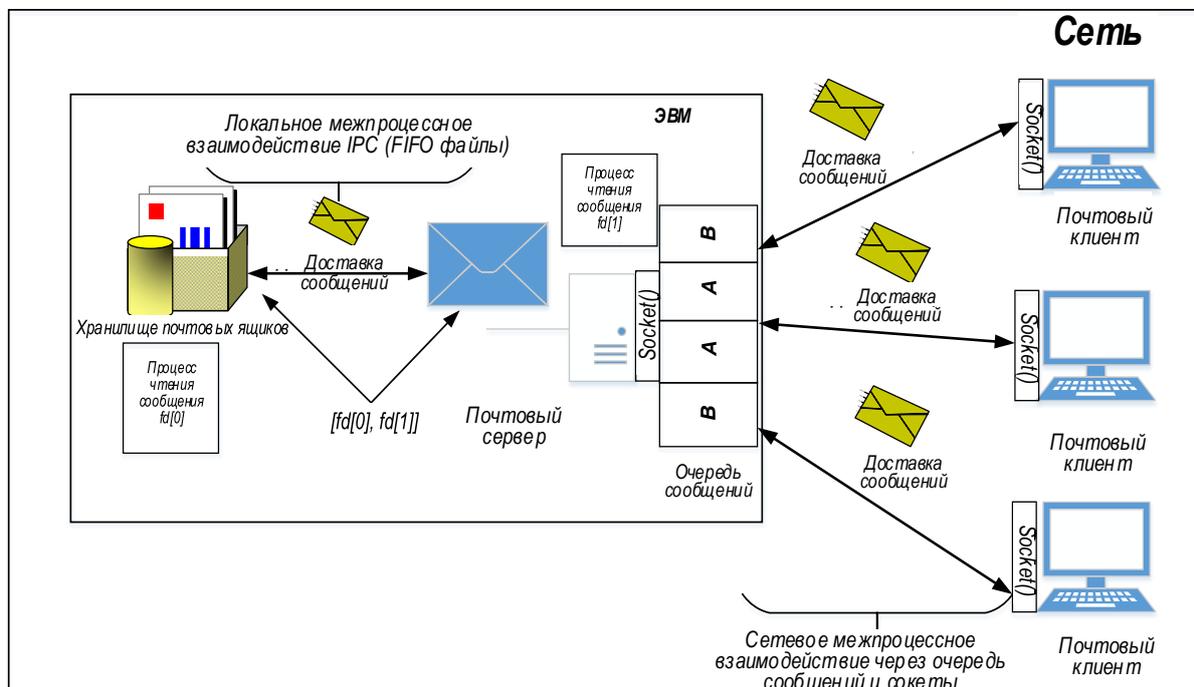


Рис. 2. Пример межпроцессного взаимодействия сообщениями электронной почты

В процессе обмена электронной почтой задействуются оба вида межпроцессного взаимодействия: локальное и сетевое. Сетевое реализуется между отдельными ЭВМ, расположенными в сети при обмене электронной почтой. На клиенте электронной почты процесс отправки сообщения передает его контекст через сокет по сети в специальном формате (приведен на рис. 3).

```

From: <vasy@list.ru> // адрес отправителя
To: <pety@kfti.knc.ru> // адрес получателя
Subject: С новым годом! // тема сообщения
Mime-Version: 1.0 // инициализация Mime
X-Mailer: mPOP Web-Mail 2.19 // тип и версия почтовой программы клиента
Date: Fri, 19 Sep 2003 08:37:43 +0400 // дата отправки сообщения
Reply-To: <vasy@list.ru> // адрес для ответа
Content-Type: text/plain; charset=koi8-r // тип и подтип MIME
Content-Transfer-Encoding: 8bit // идентификатор типа кодировки
Message-Id: <E1A0D1b-000AnC-00.vasy-list-ru@f15.mail.ru> // уникальный идентификатор сообщения

С новым годом Петя! //Тело сообщения
    
```

Рис. 3. Формат сообщения электронной почты

На стороне сервера электронной почты процесс приема сообщений электронной почты от клиентов формирует очередь сообщений в которую помещаются сообщения от всех клиентов. Далее они обрабатываются сокетом, и он вызывает процесс сохранения принятого сообщения в хранилище почтовых сообщений. Взаимодействие между этими процессами реализуется с помощью механизма IPC, а именно через FIFO-файлы. Процесс сохранения сообщения создает файл в предопределённой директории и формирует массив дескрипторов доступа к данному файлу. Дескриптор записи (fd[1]) выдается процессу, отвечающему за запись контекста сообщения в файл. После окончания записи, дескриптор чтения (fd[0]) выдается процессу сохранения сообщения, он считывает контекст сообщения и сохраняет его в определенную область памяти хранилища.

Провести анализ межпроцессного взаимодействия достаточно сложная задача и набор инструментов, позволяющих сделать это весьма ограничен. Такими инструментами, функционирующими в ОС Astra Linux SE, могут являться Process Monitor, Glances, Noriben (рис. 4, 5).

The screenshot displays the Glances monitoring tool interface. At the top, it shows system information: 'ops (Ubuntu 14.04 64bit / Linux 3.13.0-63-generic) IP 192.168.0.3/24 Uptime: 1 day, 17:38:44'. Below this are various system metrics including CPU usage (99.9%), memory usage (28.1%), and network activity. A 'CONTAINERS' section shows two containers: 'grafana-grafana.1' and 'grafana-influxdb.1'. The 'TASKS' section lists 228 tasks, and the 'RUNNING' section shows processes like 'Dropbox' and 'Python'. A detailed process list at the bottom shows columns for CPU, MEM, VIRT, RES, PID, USER, NI, S, TIME+, IOR/s, IOM/s, and Command.

Рис. 4 Пример работы средства Glances

The screenshot displays the Noriben monitoring tool interface. It is divided into several sections: 'Processes Created' showing the creation of 'Explorer.exe' and 'python.exe'; 'File Activity' showing file operations like 'C:\WINDOWS\system32\cmd.exe'; 'Registry Activity' showing registry changes; and 'Network Traffic' showing network connections to 'google-public-dns-a.google.com:53' and '216.146.38.70:80'. The interface uses a tree-like structure to show the hierarchy of monitored activities.

Рис. 5 Пример работы средства Noriben

В итоге можно сделать вывод, что подход к оценке защищенности в котором не учитывается взаимосвязь уязвимостей между программными продуктами системы является не актуальным. Все приложенные установленные в ОС имеют возможность взаимодействовать и

обмениваться различными видами информацией между собой и зачастую отследить эти процессы достаточно сложно так как все они функционируют внутри процессора. В свою очередь факт того, что в один и тот же момент времени в ОС может существовать два приложения с разными уязвимостями, которые при последовательной эксплуатации позволяют повысить уровень привилегий или добиться иного успеха в рамках атаки, вынуждает разработать новый подход к оценке защищенности систем [4].

Список используемых источников

1. Белов А. С., Добрышин М. М., Шугуров Д. Е. Функциональный подход к комплексной оценке уровня информационной безопасности элемента корпоративной сети связи / Приборы и системы. Управление, контроль, диагностика. 2023. № 3. С. 30–39.
2. Основы безопасности операционной системы специального назначения Astra Linux Special Edition. Управление доступом. Учебное пособие / Девянин П. Н., Тележников В. Ю., Третьяков С. В. М.: Телеком, 2023. 148 с.
3. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие / Буренин П. В., Девянин П. Н., Лебедеко Е. В., Цибуля А. Н. и др. М.: Телеком, 2020. 404 с.
4. Белов А. С., Добрышин М. М., Шугуров Д. Е., Большебратский К. М. Подход к оценке защищенности компьютерной сети связи на основе количества уязвимостей / Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 20–25.

УДК 004.65
ГРНТИ 50.41.21

ИССЛЕДОВАНИЕ МЕТОДОВ МИГРАЦИИ ПРОГРАММ PL/SQL С СУБД ORACLE НА PL/PgSQL СУБД POSTGRESQL

Л. И. Борганова, О. Ю. Сабинин

Санкт-Петербургский Политехнический университет Петра Великого

В данной статье обосновывается актуальность перехода в открытые системы управления базами данных и рассматривается вопрос миграции между Oracle и PostgreSQL. Проводится обзор современных решений по конвертации кода программных компонент, написанных на процедурном языке PL/SQL, используемом в Oracle, в PL/pgSQL, используемом в PostgreSQL, и анализируются задачи подготовительного этапа миграции. В результате приводится описание алгоритма миграции программ между двумя системами и рассматриваются процессы конвертации функций, процедур, триггеров и пакетов.

система управления базами данных, реляционная база данных, Oracle, PostgreSQL, миграция программных компонент, миграция PL/SQL, PL/pgSQL

В настоящее время наблюдается тенденция перехода с использования проприетарных СУБД, являющихся частной собственностью компании и не удовлетворяющих критериям свободного программного обеспечения, в открытые СУБД, например, переход с СУБД Oracle Database в PostgreSQL. Обусловлено это рядом причин [1]:

1. финансовые аспекты:

Это одна из главных причин, поскольку затраты на приобретение и поддержку проприетарного продукта могут быть значительными особенно при масштабировании системы.

2. функциональные возможности:

Хотя открытые СУБД и могут иметь менее обширные функциональные возможности по сравнению с проприетарными, их как правило достаточно для решения многих задач.

3. открытый исходный код и сообщество поддержки:

Преимущество открытых продуктов в возможности взаимодействия с сообществом разработчиков и возможности адаптации и расширения системы под нужды пользователей.

4. риски, связанные с прекращением работы продукта:

Политические события или другие факторы могут привести к остановке или прекращению деятельности компании-поставщика проприетарного продукта, создавая тем самым риски для предприятий.

Процесс перехода с одной СУБД в другую именуется как миграция. Вопрос миграции между СУБД Oracle и СУБД PostgreSQL является и по сей день актуальным. Особенно выделяется проблема миграции программных компонент, написанных на процедурном языке PL/SQL, используемом в Oracle, в PL/pgSQL, используемом в PostgreSQL, поскольку данный процесс подразумевает ряд исключительных моментов и сложностей.

Поэтому целью данной статьи стало исследование методов миграции программ PL/SQL с СУБД Oracle на PL/pgSQL СУБД PostgreSQL.

Актуальность использования СУБД PostgreSQL для создания баз данных

СУБД PostgreSQL – это объектно-реляционная система управления базами данных. Она обладает рядом преимуществ [2]:

- Во-первых, наличие бесплатной и полнофункциональной версии в отличие, например, от СУБД Oracle, где бесплатная версия “Express Edition” сильно ограничена, и по ресурсам, и по функциям.
- Во-вторых, это открытый исходный код, благодаря чему пользователи могут свободно его изменять и распространять для любых целей.
- В-третьих, это расширяемость архитектуры, благодаря чему пользователи могут создавать собственные типы данных и функции.
- В-четвертых, существуют активные сообщества разработчиков, которые создают расширения и модули для PostgreSQL.

Таким образом, СУБД PostgreSQL является мощным и гибким инструментом, который может успешно применяться в различных проектах, от небольших веб-приложений до крупных корпоративных систем, что способствует его активному спросу преимущественно при выборе целевой СУБД для миграции.

Обзор современных решений по конвертации кода с PL/SQL в PL/pgSQL

Конвертация программного кода с PL/SQL в PL/pgSQL является не тривиальной задачей, поскольку данные языки имеют существенные отличия. Возможны два подхода: использование автоматизированных инструментов миграции или ручное преобразование кода.

К доступным автоматизированным инструментам с открытым кодом можно отнести, к примеру, Ora2pg и SQLines SQL Converter. А к закрытым – SQLWays и Ora2pgpro. Эти инструменты поддерживают перенос SQL-запросов, конвертацию процедур, функций и других объектов БД.

Другой подход подразумевает полностью ручное преобразование кода. Обычно это включает в себя изменение специфических типов данных, синтаксиса хранимых программных компонент, обработку исключений и многое другое.

Первый способ является наиболее удобным и эффективным, но в представленных инструментах некоторые объекты базы данных не поддерживаются для переноса, конвертация процедурного языка PL/SQL в PL/pgSQL

требует ручной доработки или совсем отсутствует, кроме того, некоторые инструменты являются платными, что также сокращает возможность их обширного применения.

Задачи подготовительного этапа

Прежде чем перейти к исследованию алгоритма миграции, нужно выполнить несколько подготовительных задач.

Во-первых, провести анализ особенностей написания кода на программных языках PL/SQL и PL/pgSQL и выявить сходства и различия между ними. Например, нужно учитывать, что Oracle и PostgreSQL имеют разный набор типов данных, поэтому важно выбрать наилучший аналог для замены тех типов, которые отсутствуют в целевой СУБД.

Также внутри процедур, функций, триггеров могут быть использованы SQL-запросы, команды языка определения данных (DDL), манипулирования данными (DML) и управления данными (DCL), встроенные в Oracle функции, циклы, исключения и ограничения, которые могут либо не иметь прямых аналогов в PostgreSQL, либо иметь отличия в синтаксисе и функциональности [3]. Например, в PostgreSQL для получения текущей даты вместо функции SYSDATE, используемой в Oracle, применяется функция CURRENT_DATE. А для функции NEXT_DAY, используемой для определения следующего дня недели после указанной даты, и для функции ADD_MONTHS, прибавляющей указанное количество месяцев к дате, аналогов нет [4]. В случае необходимости их использования нужно выполнить замену на соответствующие арифметические операции.

Также нужно учитывать, что синтаксис написания программ тоже отличается.

Во-вторых, нужно либо выбрать готовый инструмент миграции, либо взять за основу разработанный алгоритм, либо придумать свой и реализовать его.

В данном контексте предполагается разработка собственного алгоритма миграции, который учитывает все ключевые особенности, связанные с конвертацией PL/SQL программ таких как функции, процедуры, триггеры и пакеты. Это обусловлено стремлением к максимальной адаптации к специфике PL/SQL и PL/pgSQL и обеспечению полной и точной миграции программных компонент.

Алгоритм миграции программных компонент между Oracle и PostgreSQL

Алгоритм миграции состоит из нескольких этапов:

- 1) экспорт в текстовый файл DDL-кода программных компонент из СУБД-источника;
- 2) выделение каждого объекта в полученном файле;

- 3) выполнение синтаксического анализа кода для каждого выделенного на втором этапе объекта и определение фрагментов кода, которые будут модифицированы;
- 4) модификация кода (замена типов данных, добавление ключевых слов и конструкций, изменение синтаксиса команд и т. п.);
- 5) сбор всех сконвертированных программных компонент в единый текстовый файл;
- 6) импорт объектов в целевую СУБД;
- 7) тестирование и анализ полученных результатов.

Здесь важно отметить, что в ходе выполнения второго этапа для лучшей организации кода и для удобства изменения и хранения данных программные компоненты будут разделены на четыре категории: пакеты, функции, процедуры и триггеры. Для выделения программ, ключевых слов, типов данных и т.п. будут применяться регулярные выражения, позволяющие по заданному шаблону находить нужные фрагменты текста, а затем вырезать их, заменять частично или полностью.

В ходе выполнения третьего этапа каждый код будет проанализирован на наличие символов и фрагментов, модифицируемых в дальнейшем. Идея состоит в том, чтобы разделить найденные элементы на категории, например, «типы данных», «исключения», «ключевые слова» и т. д., и затем обрабатывать отдельно каждую группу.

Конвертация функций

Как упоминалось ранее, конвертация программных компонент подразумевает, во-первых, изменение самого синтаксиса. Так у функций нам необходимо произвести замену ключевых слов, например, RETURN, используемое для определения возвращаемого значения функции, в PL/SQL требует замены на RETURNS, а ключевые слова IS/AS в PL/SQL, которые вводят раздел объявлений перед телом блока кода, подлежат замене на DECLARE. Также необходимо добавить новые конструкции такие как, конструкция LANGUAGE plpgsql, указывающая, что функция написана на языке PL/pgSQL и маркеры \$\$, обозначающие начало и конец тела функции.

Во-вторых, нужно провести модификацию SQL-запросов, встроенных функций, исключений – весь код, расположенный внутри самих функций.

Конвертация процедур

PostgreSQL поддерживает две реализации процедур.

Первая – создается при помощи ключевого слова PROCEDURE и не возвращает значение, вторая – создается при помощи ключевого слова FUNCTION и имеет тип возвращаемого значения void. При конвертации кода в первый тип необходимо помимо обработки содержимого процедуры добавить маркеры \$\$ и конструкцию LANGUAGE plpgsql а при конвертации во второй тип необходимо дополнительно заменить ключевое слово

PROCEDURE на FUNCTION и добавить тип возвращаемого значения RETURNS void.

Конвертация триггеров

Для того, чтобы создать триггер в PostgreSQL, нужно создать сам триггер через команду CREATE TRIGGER и дополнительно создать функцию, вызываемую триггером, в которой выполняются все действия триггера. Важно в конце кода триггера прописать команду вызова связанной с ним функции.

Также важно заметить, что в PostgreSQL при обращении к псевдозаписям OLD и NEW прописывать знак «:» не нужно.

Конвертация пакетов

Версия Postgres Pro Enterprise 15, выпущенная в начале 2023 года, внесла поддержку пакетов. К сожалению, данная версия является платной, что ограничивает доступность этой возможности для большинства пользователей. В качестве альтернативы пакетам в PostgreSQL используются схемы, однако при этом отсутствует возможность явного определения спецификации и тела пакета.

При миграции пакетов требуется, помимо преобразования кода, создать схему в базе данных через команду CREATE SCHEMA. Затем содержимое пакета следует добавить в созданную схему.

Заключение

Таким образом, анализ миграции программных компонент с процедурного языка PL/SQL в PL/pgSQL выявил, что данная задача остается актуальной в силу существенных различий между языками и спецификой СУБД Oracle и СУБД PostgreSQL. Неполная поддержка необходимых объектов базы данных в имеющихся инструментах миграции подчеркивает сложность процесса. Результаты, полученные в ходе данного исследования, могут быть применимы к решению задачи миграции между другими реляционными СУБД.

Список используемых источников

1. Horstmann Jutta. Migration to Open Source Databases: Ph.D. thesis: Technical University Berlin, 2005. 115 p.
2. Документация к PostgreSQL 16.2. URL: <https://postgrespro.ru/docs/postgresql/16/index> (дата обращения: 15.02.2024)
3. Андреева Н. В., Кожевников В. А., Сабинин О. Ю. Программирование баз данных: основы PL/SQL: учебник. СПб.: изд-во Политехн. ун-та, 2019. 183 с.
4. Новиков Б. А., Горшкова Н. Г., Графеева Н. Г.; под ред. Е. В. Рогова. Основы технологии баз данных: учебное пособие. 2-е изд. М.: ДМК Пресс, 2020. 582 с.

УДК 003.6
ГРНТИ 81.95.33

ИСПОЛЬЗОВАНИЕ ВИЗУАЛЬНЫХ СРЕДСТВ КАК ИНСТРУМЕНТА ОБЕСПЕЧЕНИЯ ПОНИМАНИЯ ДАННЫХ, ПРЕДСТАВЛЕННЫХ С ПОМОЩЬЮ ИНФОГРАФИКИ

Е. П. Бояшова, М. В. Мельников, Д. Н. Шеремет

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

В работе затрагиваются аспекты, связанные с искажениями восприятия информации, а также с объективностью визуализации. Рассматриваются факторы, влияющие на эффективность восприятия представленной информации, а также на извлечение из потока информации только тех данных, которые являются полезными. При этом данные должны трансформироваться в последовательные выводы, способствующие продуктивной коммуникации. Кроме того, в работе уделяется внимание ошибкам, допускаемым при проектировании инфографики, а также предлагаются рекомендации по её созданию.

инфографика, визуальные средства, восприятие информации, коммуникация, информация, данные, представление данных

В настоящее время человека окружают большие объёмы информации, и ее потоки постоянно увеличиваются. Несмотря на обилие информации, она должна эффективно восприниматься аудиторией.

Под эффективностью восприятия З. Д. Чихладзе и Р. В. Шевченко понимают скорость восприятия по отношению к затратам когнитивных ресурсов [1]. Информация воспринимается человеком с помощью его органов чувств. Графическое представление информации является наиболее удобным для восприятия, поскольку визуальные образы ускоряют усвоение информации, а также способствуют усилению мыслительной деятельности.

Для визуального представления информации используется инфографика.

Несмотря на то, что ключевую роль в инфографике играет информация, крайне важна и форма её представления, поскольку одни и те же данные визуально можно представить множеством различных способов. Наглядной демонстрацией такой возможности является проект «dataset 100 visualisations» [2].

Некоторые варианты инфографики, основанной на простом наборе данных, показаны на рис. 1.

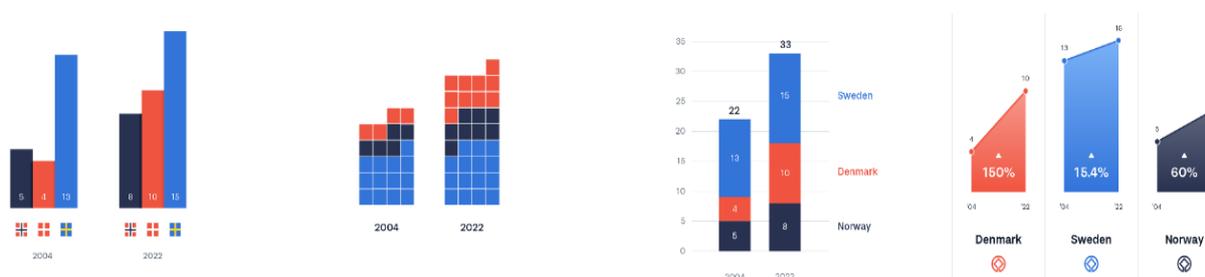


Рис. 1. Различное представление одного набора данных

Необходимо выбирать такой тип инфографики по способу визуализации информации, который позволит представить отдельно взятые данные в наглядной, удобной для анализа, восприятия и рассмотрения форме, поскольку одну и ту же информацию можно по-разному интерпретировать, и в этом случае существует опасность ее неоднозначного прочтения.

На эффективность восприятия данных оказывает влияние ограниченное время для принятия решений на основании значимости имеющихся признаков предъявленной информации. Немаловажную роль играет извлечение из потока информации только тех данных, которые являются важными и полезными, их структурирование и систематизация. Автор книги «Инфографика. Визуальное представление данных» Р. Крам отмечает, что людям важны именно выводы, получаемые на основе исходных данных [3].

На основе исходных данных инфографика позволяет представить закономерности, тенденции и заключения.

Отметим, что восприятие информации человеком субъективно – она может восприниматься не в полной мере, ошибочно или неточно. На восприятие оказывают влияние когнитивные искажения.

Когнитивные искажения – это «систематические ошибки в мышлении или шаблонные отклонения, которые возникают на основе дисфункциональных убеждений, внедренных в когнитивные схемы, и которые легко обнаруживаются при анализе автоматических мыслей» [4].

К когнитивным искажениям относят, в частности, эффект превосходства изображения [5] – явление, при котором люди лучше запоминают информацию, представленную с помощью графики, чем та, которая отображена в форме текста. Для усвоения информации задействуется ассоциативное мышление, и визуальные образы помогают быстро уловить их суть. Так, например, изображение стрелки, стремящейся на графике вниз, указывает на нисходящую динамику.

К когнитивным искажениям также относят закон Миллера. Человеку проще усваивать информацию по группам, разделяя её на смысловые блоки.

В кратковременной памяти человека может одновременно удерживаться 5-9 блоков информации. Именно поэтому рекомендуется не отображать большое количество разных блоков с данными.

Кроме того, на восприятие информации аудиторией можно влиять, используя манипуляции восприятия – методы воздействия на восприятие путем внедрения искажений, нарушающих правила визуализации данных.

Среди наиболее используемых манипуляций можно выделить:

- изменение минимальных значений на оси гистограммы с целью преувеличения изменения значений. В таком случае показывается лишь малая часть тренда, что приводит к ошибочному восприятию тенденции и принятию неверного решения;
 - искажение масштаба объектов;
 - использование трёхмерных объектов. При отображении круговой диаграммы в 3D или в перспективе нарушаются пропорции отображаемых частей диаграммы;
 - отображение лишь части данных из всей их совокупности.
- Отдельно можно выделить некоторые ошибки, которые достаточно часто допускаются при проектировании инфографики (табл. 1).

ТАБЛИЦА 1. Ошибки, допускаемые при проектировании инфографики

Ошибка	Возможные последствия
неверный выбор вида инфографики по способу визуализации информации	возможность разного прочтения представленной информации наблюдателями
отображение объекта в пространстве в том случае, когда в этом нет необходимости	возможное искажение информации
избыток отображаемой информации	увеличение когнитивной нагрузки; невозможность целостного восприятия информации; сложность формирования выводов и принятия решения
нарушение правил типографики и колористики	усложнение восприятия информации

Для обеспечения понимания представленных данных необходимо создавать инфографику, характеризующуюся следующими качествами:

- наглядность – способность инфографики быть легко воспринимаемой наблюдателем, ясность;
- информативность – насыщенность изображения объективной информацией;

- целостность – полнота, завершённость инфографики, представление в ней всех необходимых данных;
- простота – отсутствие перегруженных элементов, которые не являются необходимыми для наглядного отображения информации.

Кроме того, представленная с помощью инфографики информация должна быть актуальной, значительной для аудитории. При создании инфографики необходимо также руководствоваться основными принципами графического и коммуникационного дизайна.

Список используемых источников

1. Чихладзе З. Д., Шевченко Р. В. Сильные и слабые стороны различных методов визуализации информации // Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство: сб. науч. ст. VII Междунар. науч. конф., Казань, 31 августа 2019 г. Казань: ООО «Конверт», 2019. С. 128–134.

2. 1 dataset. 100 visualisations URL: <https://100.datavizproject.com> (дата обращения: 12.02.2024)

3. Крам Р. Инфографика. Визуальное представление данных. СПб: Питер, 2015. 384 с.

4. Боброва Л. А. Когнитивные искажения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 3. Философия: Реферативный журнал. 2021. № 2. С. 69–79.

5. Когнитивные искажения в презентациях URL: <https://presium.pro/blog/cognitive-biases-in-presentations> (дата обращения: 16.02.2024)

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

УДК 004.056.55
ГРНТИ 81.93.29

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ

Д. Б. Быков, А. А. Климов, К. А. Ромашкин

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

В статье проанализированы алгоритмы асимметричного шифрования данных (Rivest-Shamir-Adleman, Digital Signature Algorithm, ElGamal algorithm и Elliptic Curve Digital Signature Algorithm). Оценка проведена с учетом уровня защищенности, скорости шифрования и дешифрования, а также удобства в реализации. Кроме того, рассмотрены размеры ключей каждого алгоритма и их соответствующий анализ. Наиболее предпочтительными оказались Elliptic Curve Digital Signature Algorithm и Rivest-Shamir-Adleman.

криптография, шифрование, асимметричные методы, дешифрование, алгоритмы

Шифрование – процесс преобразования информации таким способом, чтобы ее могли понять только те, кому это разрешено. Это операция, при которой данные преобразуются в зашифрованный код для безопасной передачи через общедоступные сети. В современности большинство криптографических процессов происходят в цифровой форме, когда исходный текст, или «открытый текст», преобразуется в зашифрованный вариант, известный как «шифротекст» с помощью разнообразных шифровальных алгоритмов. Расшифровка шифротекста осуществляется на получающей стороне, превращая его обратно в открытый текст для обеспечения безопасности передаваемых данных. Это метод, направленный на предотвращение несанкционированного доступа к информации. Процесс шифрования включает в себя один или несколько ключей, которые обеспечивают защиту данных от несанкционированного доступа злоумышленников и неправомерного использования [1].

Существует разделение методов криптографии на основе выбора ключа. В этом разделе обсуждаются преимущества разнообразных криптографических методик.

Симметричный метод шифрования заключается в том, что обе стороны-участники обмена данными имеют одинаковые ключи для шифрования и расшифровки информации. Симметричный метод шифрования может быть реализован на основе разных алгоритмов. Например, часто используются алгоритмы DES, 3-DES (тройной DES), RC2, RC4. Сегодня самым

надежным симметричным алгоритмом считается расширенный стандарт AES.

В асимметричном шифровании, принято использовать два ключа – открытый и закрытый. Такой способ шифрования обеспечивает максимальную защищенность данных, проходящих через нестабильные каналы. В данных ключах используются достаточно большие числа, сделано это для того чтобы, процесс расшифровки был максимально трудным [2].

Рассмотрим алгоритмы асимметричного шифрования данных.

RSA (Rivest Shamir Adleman, фамилии создателей алгоритма) асимметричный алгоритм шифрования, который использует два ключа, один для шифрования, другой для расшифрования. Этот метод строится на сложности факторизации простых чисел.

Для передачи сообщения (m) от одного человека к другому, нужно взять открытый ключ второго (e, n) и зашифровать его по формуле (1):

$$c = E(m) = m^e \bmod n \quad (1)$$

Для дешифрования получатель принимает зашифрованное сообщение (c), использует свой закрытый ключ (d, n), и расшифровывает сообщение по формуле (2):

$$m = D(c) = c^d \bmod n \quad (2)$$

Стойкость алгоритма определяется при помощи сложности вычисления обратной функции к функции шифрования (1).

ELGAMAL (фамилия основателя алгоритма, Эль-Гамаль) – алгоритм шифрования с открытым ключом, который базируется на сложных задачах дискретного логарифмирования. Он позволяет зашифровать данные с использованием открытого ключа и расшифровать их с помощью соответствующего закрытого ключа. Этот метод стоит на одном уровне по популярности с таким метод как RSA [3].

DSA (Digital Signature Algorithm) – алгоритм цифровой подписи, предназначенный для обеспечения аутентификации данных. В отличие от некоторых других алгоритмов, DSA предназначен исключительно для создания и проверки электронных подписей, не предоставляя возможности для шифрования и расшифрования данных. Он используется для подтверждения подлинности сообщений или документов и обеспечивает недопустимость отрицания авторства подписанных данных. DSA широко применяется в различных областях, включая цифровые сертификаты, электронные транзакции и обмен информацией, где важна аутентификация и защита от изменения данных.

ECDSA не является алгоритмом шифрования в строгом смысле. Вместо этого, он используется для создания и проверки электронных цифровых подписей с помощью криптографии на эллиптических кривых. Табл. 1 Он предназначен для обеспечения идентификации и целостности данных, путем создания подписи, которая может быть проверена другими участниками с использованием открытого ключа, связанного с подписью [4]. Это позволяет убедиться в том, что данные не были изменены после того, как они были подписаны, и что подпись была создана владельцем соответствующего закрытого ключа (рис. 1)

ТАБЛИЦА 1. Сравнительная характеристика основных алгоритмов асимметричного шифрования

Алгоритм	Ключ	Назначение	Криптостойкость
RSA	До 4096 бит	Шифрование и подпись	$2,7 \cdot 10^{28}$ для ключа 1300 бит
ELGAMAL	До 4096 бит	Шифрование и подпись	$2,7 \cdot 10^{28}$ для ключа 1300 бит
DSA	До 1024 бит	Подпись	
ECDSA	До 521 бит	Шифрование и подпись	Криптостойкость и скорость работы выше, чем у RSA

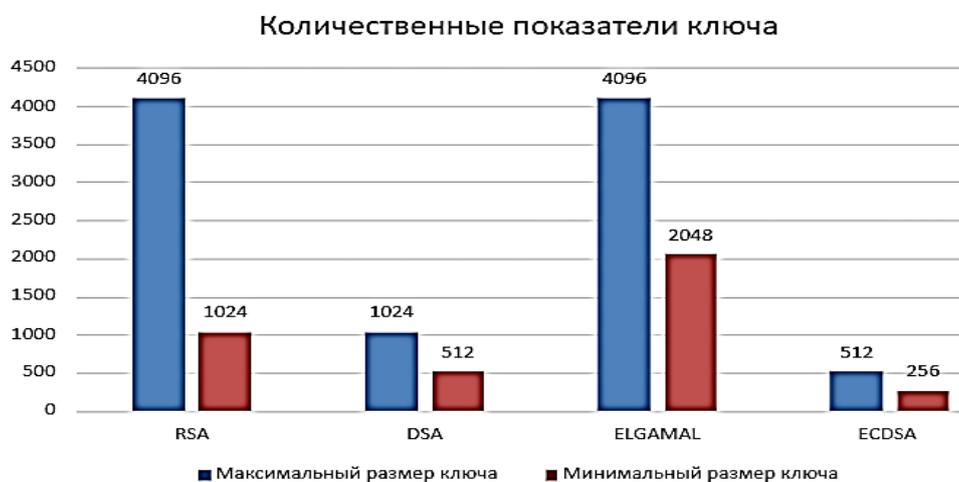


Рис. 1. Результаты исследования величины ключа

В ходе исследования величины ключа следует сказать, что DSA имеет достаточно сильный разброс в размере ключа, так как более малые значения свидетельствуют тому, что обрабатываемый ключ закрытый. Значения, начинающиеся от 1024 бит, соответствуют открытому ключу [5].

Алгоритм ELGAMAL примерно схож с RSA по количеству бит, но весьма различен по способностям расшифрования, и в отличие от RSA позволяет быстрее генерировать ключи без потери стойкости.

В табл. 2 ECDSA по сравнению со всеми предыдущими алгоритмами имеет большое преимущество в скорости, что требует меньше памяти для

обработки. Также весомым преимуществом является обеспечение значительно меньшей длины вывода при том же уровне безопасности. Например, 3072-битная подпись RSA обеспечивает тот же уровень безопасности, что и 256-битная подпись ECDSA [6].

ТАБЛИЦА 2. Основные характеристики сравнения

Алгоритм	Криптостойкость	Скорость шифрования	Скорость дешифрования	Простота реализации
RSA	средняя	средняя	высокая	очень высокая
ELGAMAL	высокая	высокая	средняя	очень низкая
DSA	Очень высокая	высокая	средняя	средняя
ECDSA	высокая	очень высокая	высокая	низкая

Таким образом, с точки зрения цифровой передачи данных наиболее предпочтительные в условиях максимальной эффективности и безопасности можно выделить алгоритм RSA и ECDSA.

Список используемых источников

1. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2015. 376 с.
2. Аль-Нами Б. А., Сидельников А. М. Анализ современных методов обнаружения и защиты от кибератак на базе машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 228–231.
3. Мао В. Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.
4. Аль-Нами Б. А., Афанасьев А. А., Михеев Г. Д. Актуальная информация о безопасности браузеров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 42–45.
5. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2009. 372 с.
6. Аль-Нами Б. А., Баранов А. М., Бурмак К. К. Методы использования двухфакторной аутентификации в современном мире. как обезопасить свои данные от злоумышленников // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 46–50.

Статья представлена научным руководителем, кандидатом технических наук, старшим преподавателем кафедры ИКД Аль-Нами Б. А.

УДК 621.316.91
ГРНТИ 50.43.15

УСТРОЙСТВО ЗАЩИТЫ ЭЛЕКТРОННОЙ АППАРАТУРЫ АСУ НА БАЗЕ СОВРЕМЕННЫХ ПРОГРАММИРУЕМЫХ МИКРОСХЕМ

А. В. Ваганов, А. С. Марчаков

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

В статье рассматривается устройство защиты электронной аппаратуры автоматизированной системы управления от негативного воздействия нестабильности питающего напряжения, различных импульсных помех, а также некорректных режимов ее включения и работы. Обоснована актуальность разработки подобного класса устройств, а также рассмотрены основные преимущества и недостатки аналогичных систем и методов защиты автоматизированных систем управления на базе современных программируемых микросхем. Представлена структурная схема системы защиты и обоснован выбор современной элементной базы для ее реализации, основанной на программируемых дискретных интегральных схемах. Осуществлен выбор математического аппарата для расчета отдельных блоков системы. Приведены результаты моделирования.

защитное устройство, импульсные помехи, микроконтроллер, электропитание, АЧХ, структурная схема

Электронная аппаратура в автоматизированной системе управления (АСУ) играет значимую роль в обеспечении ее функционирования. Нестабильность питающего напряжения, различные помехи и перенапряжения в электросети питания могут вызвать сбои и повреждения электронных компонентов, поскольку аппаратура чрезвычайно чувствительна к нестабильности питающего напряжения [1]. Поэтому разработка защитного устройства, способного обеспечить надежную защиту от различных электрических воздействий, является актуальной задачей.

На сегодняшний момент существуют следующие основные системы защиты электронного оборудования АСУ.

Защита от перенапряжений. Система защиты от перенапряжений предназначена для обеспечения безопасности электронного оборудования путем предотвращения повреждений, вызванных резким увеличением напряжения в электрической сети [2]. В ее состав входят различные устройства, такие как сетевые фильтры, стабилизаторы напряжения, разрядники, источники бесперебойного питания (ИБП), трансформаторы с защитой от перенапряжений, а также устройства защиты от импульсных перенапряжений, включающие в себя варисторы и TVS-диоды.

Защита от короткого замыкания и перегрузок. Короткое замыкание и перегрузки приводят к возникновению большого тока и перегрузке электрической сети, что в свою очередь ведет к серьезным повреждениям электронного оборудования, включая перегрев проводов, повреждение электрических компонентов и плат электронных устройств [3]. Система способна оперативно обнаруживать подобные проблемы и принимать необходимые меры для предотвращения ущерба. В ее состав входят различные устройства, такие как предохранительные устройства, защитные реле, ограничители тока, датчики и детекторы, резервные источники питания, а также программируемые микросхемы.

Защита от электромагнитных помех. Система защиты от электромагнитных помех разработана с целью уберечь электронное оборудование от воздействия электромагнитных помех, которые могут появляться от других электронных устройств или внешних источников. Она содержит использование экранирования, фильтров электромагнитных помех шунтирующих и других устройств, которые могут подавлять и снижать уровень помех.

Преимуществом рассмотренных выше систем является их относительно невысокая цена и то, что каждая система защиты может быть разработана и установлена для решения конкретных задач и предотвращения определенных видов угроз.

Главным недостатком рассмотренных выше систем защиты электронного оборудования АСУ является то, что эти системы являются разрозненными и не могут обеспечить комплексную защиту. Вторым недостатком систем является вероятность ложных срабатываний защитных устройств.

Для устранения вышеперечисленных недостатков предлагается защитное устройство электронной аппаратуры АСУ (рис. 1), которое одновременно защищает автоматизированную систему управления от выхода из строя, от некорректной работы электропитания, от различных помех и перенапряжений.



Рис. 1. Структурная схема устройства защиты аппаратуры АСУ

Проанализируем подробно структурную схему. На структурной схеме ИБП – это источник бесперебойного питания, ЭП – электронный предохранитель, АЦП – аналогово-цифровой преобразователь. Устройство питается от внешнего кабеля питания, который является источником энергии для всех устройств, обеспечивая необходимое напряжение и ток для их работы. На кабель воздействуют различные внешние помехи, электрические разряды, электромагнитные помехи, молнии, которые, в свою очередь, вызывают перенапряжения в сети.

Молния представляет серьезную угрозу для кабеля питания и всей системы, создавая импульсные перенапряжения. Поэтому в системе применяется газоразрядный разрядник. Он предназначен для защиты системы от перенапряжений и импульсных помех, которые могут поступать по сетевому кабелю питания. Газоразрядные разрядники функционируют на основе принципа газового разряда. Они включают в себя пространство между электродами, заполненное газом. Газ при достижении определенного напряжения автоматически генерирует искру, направляя излишнее электричество в землю.

Параллельно разряднику, подключен сетевой фильтр питания. Сетевой фильтр представляет собой устройство, предназначенное для фильтрации электрических помех, поступающих из электрической сети. В устройстве фильтр выполняет следующие функции: подавление электромагнитных помех и повышение качества электропитания.

Блок питания необходим для обеспечения стабильного и надежного питания всей автоматизированной системы управления. Он преобразует входное напряжение 220 Вольт в необходимые для работы устройств напряжения и токи. Благодаря блоку питания система получает постоянное электрическое питание, что обеспечивает нормальное функционирование всех компонентов системы.

В системе управления установлен источник бесперебойного питания (ИБП), который функционирует параллельно с основным блоком электропитания. Основная цель ИБП заключается в обеспечении непрерывного электропитания системы в случае сбоя блока питания или отключения электричества. При отключении блока питания ИБП автоматически переключается на потребление энергии аккумуляторной батареи.

Электронные потребители АСУ подключены к блоку питания через электронные предохранители, которые служат для защиты от перегрузок и коротких замыканий. В данной системе электронный предохранитель обеспечивает быстрое отключение питания, обеспечивая надежную защиту исполнительного устройства автоматизированной системы управления (АСУ) от негативных воздействий.

В системе микроконтроллер играет роль центрального управляющего устройства. Микроконтроллер непрерывно отслеживает параметры системы, такие как напряжение и ток. В случае преувеличения показателей принимает решение отключить систему от внешней сети питания.

Алгоритм работы устройства защиты электронной аппаратуры АСУ представлен на рис. 2.

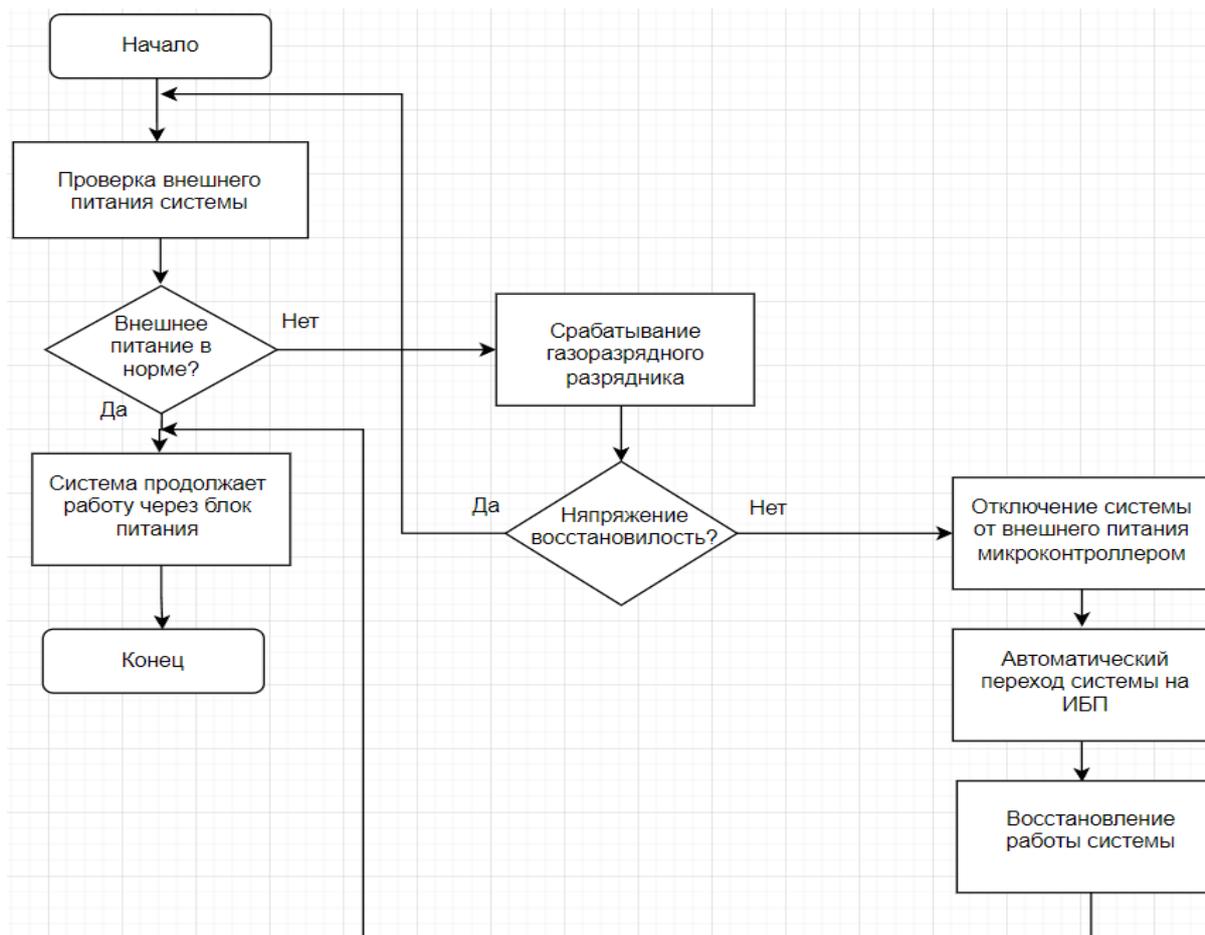


Рис. 2. Алгоритм работы защитного устройства электронной аппаратуры АСУ

Наблюдение за состоянием внешней сети электропитания производится с помощью микроконтроллера. Если напряжение соответствует нормальному значению (около 220 вольт), тогда система работает через штатный блок питания АСУ. При возникновении мощной импульсной помехи или перепада напряжения на внешнем кабеле питания, первичной реакцией устройства защиты является активация газоразрядного разрядника. В случае если микроконтроллер заметит нестабильность питающего напряжения, то он производит отключение системы от штатной системы питания и переключается на аккумуляторную батарею ИБП.

Исследование работы вторичной схемы сетевого фильтра питания произведено в программе схемотехнического проектирования Micro-Cap 12.

Программа обеспечивает обширный набор инструментов для анализа и моделирования электрических цепей, включая различные сигналы, а также предоставляет удобство при проведении различных видов анализа.

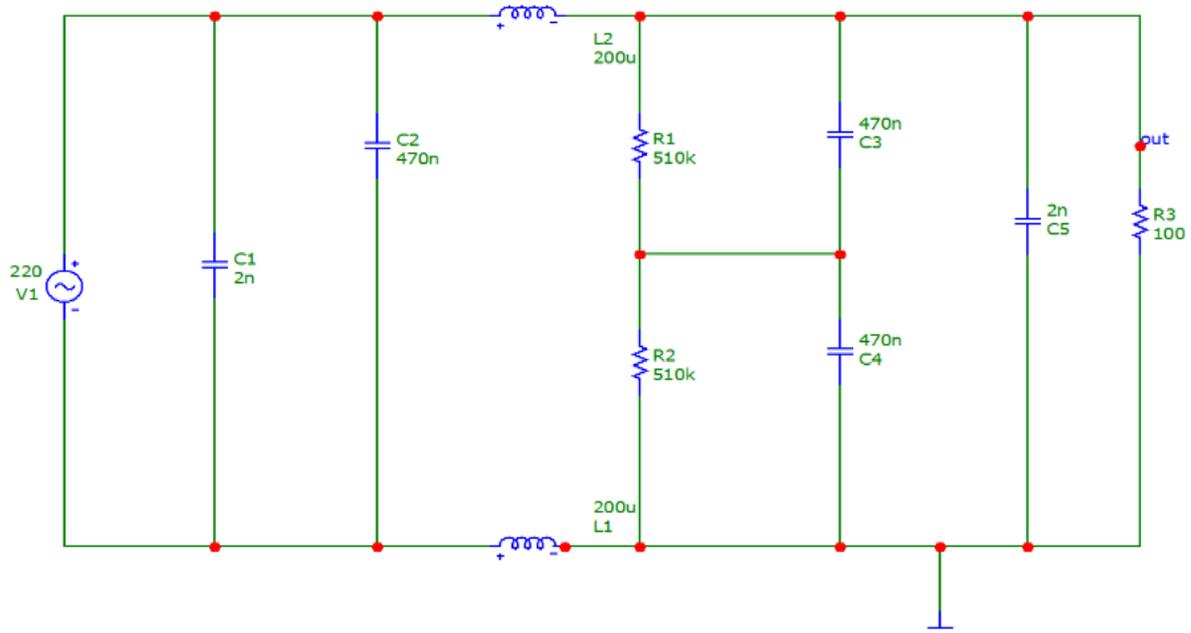


Рис. 3. Схема сетевого фильтра питания в среде Micro-Cap 12.

В результате произведен частотный анализ необходимой схемы.

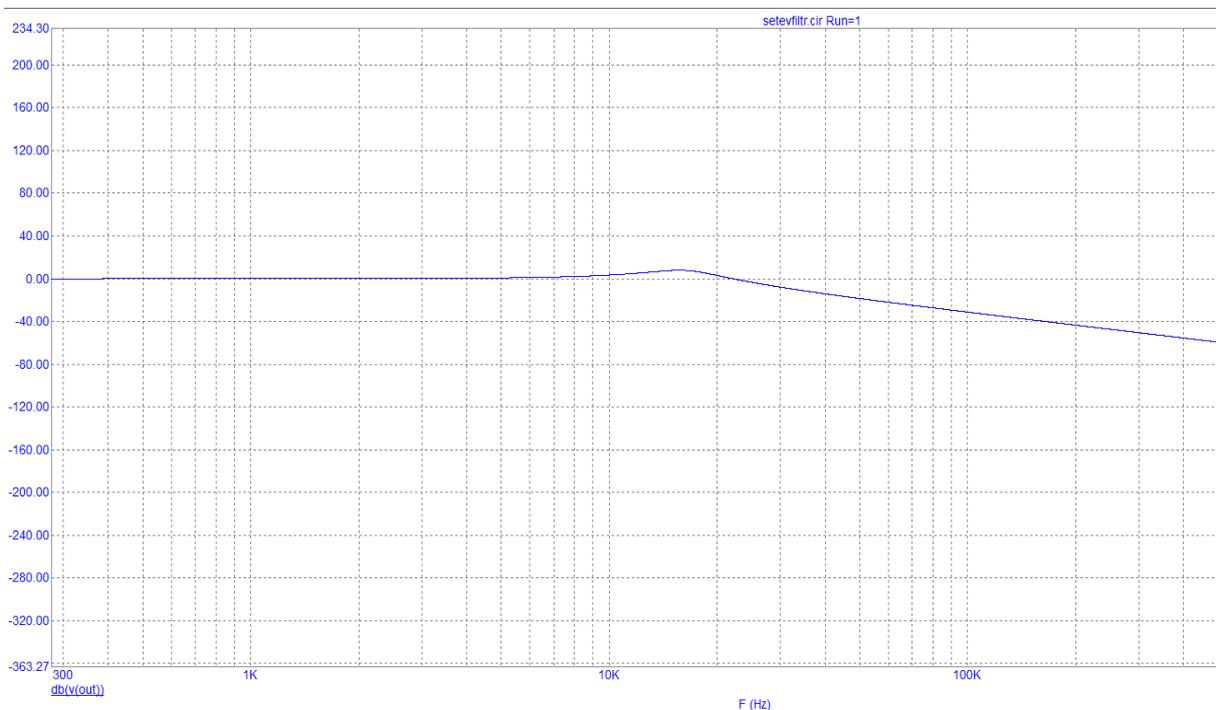


Рис. 4. АЧХ сетевого фильтра питания.

Как следует из рисунка 4, фильтр пропускает сигналы менее 10 кГц, а на более высокой частоте происходит спад АЧХ, что указывает на эффективное подавление сигналов на высоких частотах.

Таким образом, внедрение данного устройства поможет повысить устойчивость и надежность электронной аппаратуры АСУ, что в свою очередь позволит повысить производительность и эффективность управления процессами производства на современном предприятии.

Список используемых источников

1. Помехи в электросети: классификация, источники и способы защиты. URL: <https://detectorland.ru/pomehi-v-elektroseti-klassifikatsiya-istochniki-i-sposoby-zaschity/#content> (дата обращения: 27.03.2024)
2. Схема сетевого фильтра для подавления электромагнитных помех. URL: https://vrayaem.ru/circuits_podavlenie_pomeh.html (дата обращения: 28.03.2024)
3. Черепанов В. П., Посысаев Е. И. Защита радиоэлектронной аппаратуры от электрических перегрузок. Москва: РадиоСофт, 2010. 216 с.

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

УДК 004.946
ГРНТИ 28.17.33

АРХИТЕКТУРА ПРОГРАММНО-АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБРАБОТКИ И ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В ФОРМАТЕ GEOJSON

Г. В. Верховая, Е. О. Козлова

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

Представлены результаты разработки архитектуры программно-алгоритмического обеспечения для выполнения оверлейных операций над объектами, представленными в формате GeoJSON, и визуализации результатов. В результате проведенных исследований выделено множество основных оверлейных операций и определены реализующие эти операции алгоритмы. Приложение имеет сервис-ориентированную архитектуру. Бизнес-логика реализована в виде микросервиса, а система визуализации – в виде микрофронтенда. Отличительной особенностью предложенной архитектуры является возможность глубокой интеграции программного обеспечения в любые геоинформационные приложения с микросервисной архитектурой.

оверлейные операции, векторные и растровые модели, архитектура микросервиса, методы выполнения оверлейных операций, GeoJSON

При решении задач, требующих учета геоинформационных аспектов, требуется выполнение оверлейных операций над объектами, представленными в формате GeoJSON [1]. Учитывая тенденцию создания геоинформационных систем и инфраструктуры пространственных данных, реализованных в виде геопорталов, необходимы микросервисы реализующие отдельные операции пространственного анализа. К таким задачам относятся и оверлейные операции, заключающиеся в наложении друг на друга двух или более слоев, результатом которой является графическая композиция (оверлей) исходных слоев, либо новый слой, включающий в себя множество пространственно распределенных объектов, находящихся в исходных слоях. Микросервис, выполняющий оверлейные операции необходим для интеграции систем многоаспектного моделирования в геоинформационные системы, реализованные в виде геопорталов [2-3].

Существует два основных подхода к выполнению оверлейных операций – на векторных и растровых моделях географических объектов. На рис. 1. показан оверлей векторных слоев, при котором новые полигоны создаются посредством пересечения полигонов, расположенных на исходных

слоях геоинформационной системы. Новые полигоны находятся в результирующем слое, полученном в результате выполнения оверлейной операции. Аналогичные оверлейные операции используются и для случая растровой модели.

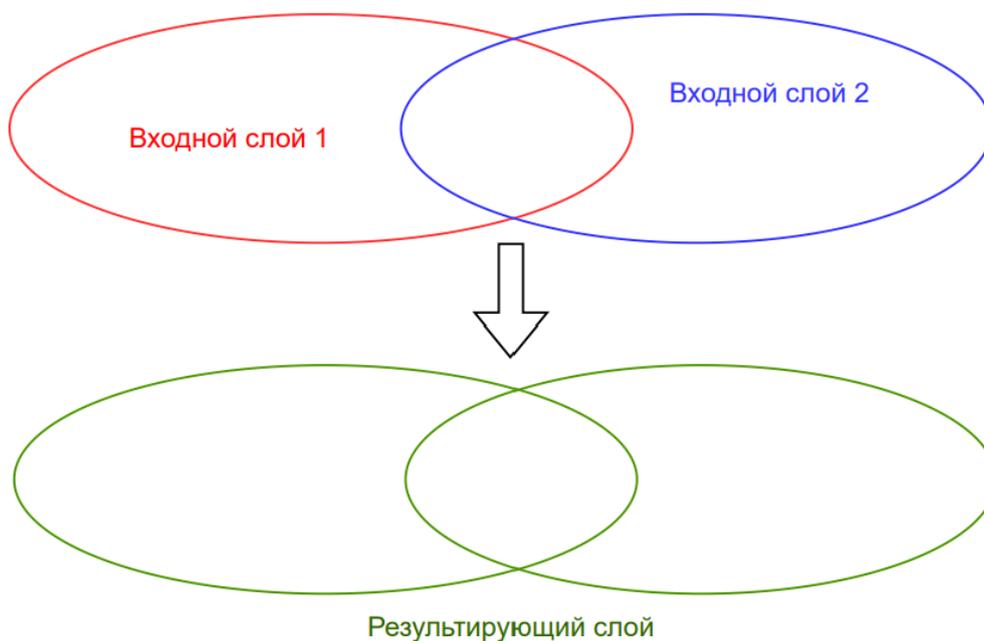


Рис. 1. Наложение векторных слоев

Основными оверлейными операциями, выполняемыми микросервисом будут:

1. Объединение (Union) слоев, которая соответствует OR (ИЛИ), результатом выполнения которых будет слой, содержащий все элементы входных слоев.

2. Пересечение (Intersection), соответствующая логическому оператору AND (И), которая формирует выходной слой, содержащий векторную модель, включающей точки, являющиеся общими для векторных моделей исходных слоев.

3. Операция включения (Inclusion), формирующая выходной слой, который содержит векторную модель второго слоя, перекрываемую векторной моделью первого входного слоя.

4. Операция исключения (Exclusion), формирующая выходной слой, содержащий векторную модель первого входного слоя, из которой вычтена векторная модель второго входного слоя.

5. Операция исключения (Exclusion) – рис. 6, определяет часть входного слоя, которая не содержится в оверлейном слое.

Учитывая широкое распространение формата GeoJSON, принято решение использовать входные данные в данном формате. Кроме того, JSON является основным форматом данных для передачи информации между микросервисами и в архитектуре RESTful. Микросервис, реализующий оверлейные операции, принимает на вход два слоя в формате GeoJSON и название оверлейной операции, и возвращает результирующий слой в том же формате (рис. 2). Полученный результат передается в слой визуализации, который имеет унифицированный API, реализуемый под определенным геопорталом (Google Maps, Яндекс Карты и т.д.). Общая архитектура представлена на рис. 3.

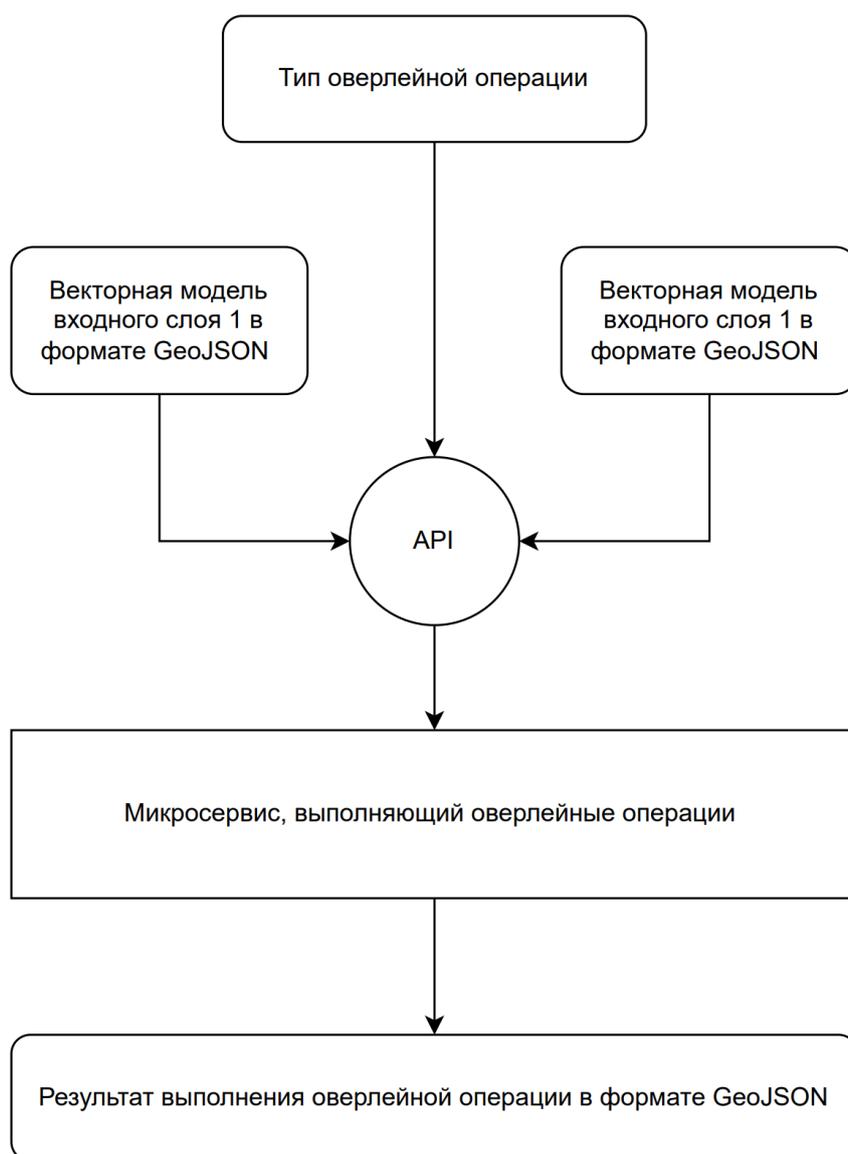


Рис. 2. Микросервис, реализующий оверлейные операции

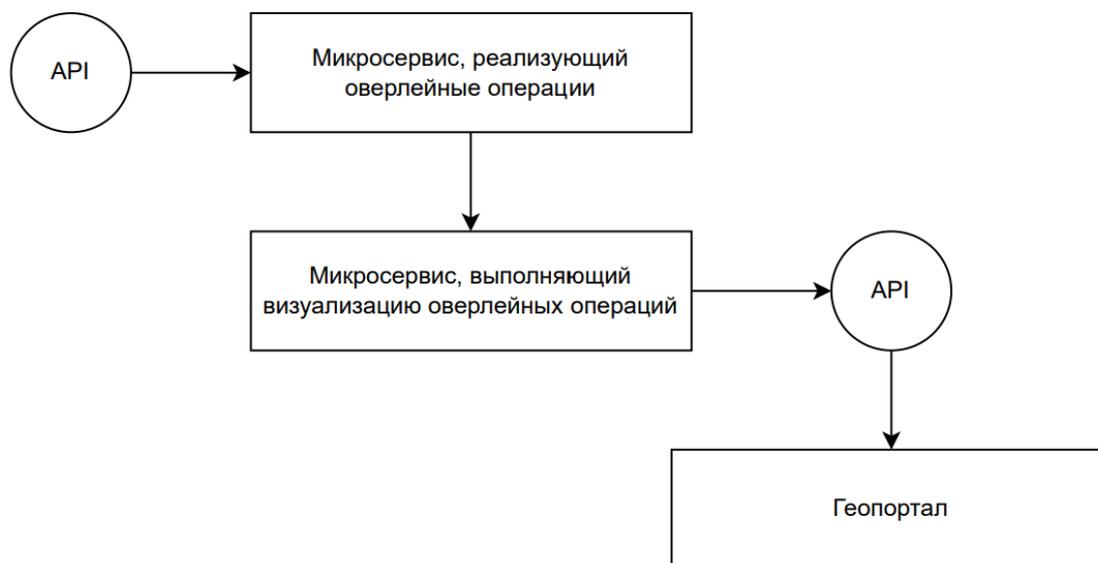


Рис. 3. Архитектура программно-алгоритмического обеспечения для обработки и визуализации информации, представленной в формате GeoJSON

Предлагаемая организация программного обеспечения обладает следующими достоинствами:

- микросервисная архитектура;
- интероперабельность;
- возможность использования в любых геоинформационных системах;
- минимально необходимый и достаточный функционал обработки и визуализации геоинформации, представленной в формате GeoJSON.

Список используемых источников

1. Верхова Г. В., Акимов С. В. Метод объединения гетерогенных геопространственных данных на основе многоаспектных моделей // Телекоммуникации. 2021. № 3. С. 34–40.
2. Ларюков С. А., Кочергин А. М. Геопортал с использованием технологий облачной обработки и хранения данных // Информатика и прикладная математика. 2019. № 25. С. 60–65.
3. Табота А. С. Проектирование геопортала регионов с использованием серверных платформ с постоянным (открытым) доступом // Славянский форум. 2019. № 2 (24). С. 228–232.

УДК 004.946
ГРНТИ 28.17.33

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ ДВОЙНИКОВ ПРОСТРАНСТВЕННО-РАСПРЕДЕЛЕННЫХ КИБЕРФИЗИЧЕСКИХ ПРОИЗВОДСТВЕННЫХ СИСТЕМ

Г. В. Верхова, В. А. Летучий

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

Представлены результаты исследований в области формирования пространственно-распределенных киберфизических производственных систем на базе цифровых двойников. Проанализированы ключевые отличия цифровых двойников пространственно-распределенных объектов от традиционных цифровых двойников производственного оборудования, в которых не учитываются геоинформационные аспекты. Рассмотрены возможные сценария развития цифровых двойников пространственно-распределенных киберфизических производственных систем и их роль в формировании единой геоинформационной киберсреды.

цифровой двойник, структура, анализ, логико-математическое описание, киберфизическая система, система

Цифровой двойник представляет собой виртуальное отображение реального объекта, процесса или системы в цифровой форме [1]. Его структурированное представление включает разнообразные элементы, такие как организация данных, процессы обновления и согласования, а также интерфейсы для доступа и взаимодействия. Структура данных цифрового двойника зависит от типа объекта и может содержать различные параметры, характеристики и атрибуты [2]. Например, для цифрового двойника физического объекта, такого как автомобиль, данные могут включать информацию о марке, модели, годе выпуска, текущем состоянии двигателя, уровне топлива и другие аспекты. Для процессов или систем, таких как производственный процесс, структура данных может описывать текущее состояние каждого этапа производства, параметры оборудования, состояние технологического процесса и т.д.

Цифровые двойники пространственно распределенных киберфизических систем должны отвечать ряду требований. Цифровой двойник должен способствовать отслеживанию изменений в реальном объекте или системе и корректировать свои данные соответствующим образом, что достигается с помощью специализированных алгоритмов синхронизации, которые включают получение данных с датчиков, обработку сигналов, фиксацию истории изменения цифрового двойника, отражающего физический объект или процесс [3].

Совмещение нескольких цифровых двойников способствует формированию более полного и сложного представления о реальном объекте или системе. Например, в промышленности различные цифровые двойники оборудования и процессов могут быть объединены для создания общей цифровой модели всего производственного процесса. Цифровые двойники объектов, распределенных в пространстве, могут использоваться для моделирования и управления системами, находящимися в разных местах. Например, цифровые двойники могут быть созданы для управления сетью распределенных энергетических систем или управления транспортной сетью в различных географических областях, что достигается с помощью алгоритмов сетевой связи и синхронизации данных между распределенными узлами.

Киберфизическая система (CPS) представляет собой концепцию управления информационными потоками, в которой вычислительные ресурсы интегрируются в физические процессы производства. В рамках такой системы датчики, вычислительные устройства и информационные системы объединены в единую сеть. Основой CPS является компьютерная модель, встроенная в систему управления, представляющая цифровой или виртуальный дубликат физического актива, которая обеспечивает его эффективное функционирование. Киберфизическая среда может быть представлена в виде мультиагентной системы (MAS):

$$MAS = \langle A, E, R, ORG \rangle \quad (1)$$

где A – множество агентов; E – коммуникационная среда; R – множество связей между агентами; ORG – определение MAS, как изображения, представляющего собой сходные между собой регулярные конфигурации, объединенные в множество, на котором определены классы эквивалентности.

Цифровые двойники киберфизической системы представляют собой мощный инструмент для моделирования, мониторинга и управления различными объектами и процесса через их виртуальные дубликаты, что позволяет улучшить эффективность, безопасность и надежность работы различных процессов и систем. Цифровой двойник может быть представлен в следующем виде:

$$D = \langle P, L, S, Perf, T, Sp \rangle \quad (2)$$

где P – объекты физического мира; L – объекты виртуального мира; S – сенсоры; $Perf$ – алгоритмы функционирования; T – тип цифрового двойника, Sp – геоинформационные аспекты.

В рамках производственной системы используется несколько цифровых двойников, которые являются подсистемами единого цифрового двойника данной производственной системы. Цифровой двойник пространственно-распределенной системы подразумевает множество цифровых двойников подсистем, находящихся в различных частях географического пространства, связанных друг с другом с помощью сетевых технологий. Таким образом, цифровой двойник пространственно-распределенной системы может быть представлен следующим образом:

$$S = \{ \langle D_{\text{объед}}, Ar_n \rangle \mid i \in [1, n], n \in [1, n] \}, \quad (3)$$

где S – множество цифровых двойников пространственно-распределенных объектов; $D_{\text{объед}}$ – объединенный цифровой двойник; Ar – идентификатор местонахождения элементов киберфизической производственной системы.

В настоящий момент все высокотехнологичные компании активно внедряют цифровые двойники в свои производственные процессы, включая обработку данных, направленную на оптимизацию производства. Данные цифровые двойники позволяют смоделировать и оптимизировать производственные системы на протяжении всего жизненного цикла продукта. Применение цифровых двойников обеспечивают ускоренное развитие экономики, обеспечивая эффективную поддержку продукции, а также способствуют становлению и развитию постиндустриального общества [3]. При этом внедрение новых технологий также требует адаптации традиционных жизненных циклов продуктов для поддержки системы сервисов.

Внедрение цифровых двойников на предприятиях происходит поэтапно. На краткосрочной перспективе они используются для оптимизации процесса использования данных и контроля активов предприятия. В среднесрочной перспективе – повышают управленческую и эксплуатационную эффективность, и общую производственную культуру. В долгосрочной перспективе цифровые двойники способствуют внедрению инноваций и сокращению затрат на производство и обслуживание оборудования.

Список используемых источников

1. Дженкинс Г. Цифровые двойники и их применение в управлении киберфизическими системами // Вестник Института информатики и вычислительной техники 2019. № 10(2). С. 64–73.
2. Ли Ю., Чен Д. Архитектура цифрового двойника и ее применение в киберфизических системах // Компьютерные медиа и программная инженерия. 2028. № 5(2). С. 46–52.
3. Верхова Г. В., Акимов С. В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // В сборнике: Волновая электроника и инфокоммуникационные системы. Сборник статей XXIV Международной научной конференции. Санкт-Петербург, 2021. С. 34–39.

УДК 004.738
ГРНТИ 50.41.23

МЕТОДЫ ФОРМИРОВАНИЯ ДОПУСТИМЫХ ЗОН РАЗМЕЩЕНИЯ ТЕХНИЧЕСКИХ ОБЪЕКТОВ НА ЦИФРОВОЙ МОДЕЛИ МЕСТНОСТИ

Г. В. Верхова, А. А. Пермяков

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

Задача оптимизации размещения технических объектов на местности с помощью поискового алгоритма требует формализованного задания допустимых зон размещения, которые определяются типом и параметрами местности, наличием необходимой инфраструктуры и инженерных коммуникаций. Современные геоинформационные системы позволяют решать задачи размещения объектов в диалоговом режиме, но использование для этих целей поисковых алгоритмов в таких системах затруднительно, так как в большинстве из них отсутствуют развитые средства, позволяющие автоматизировать данный процесс. В статье представлены результаты исследования методов формирования допустимых зон размещения технических объектов на цифровой модели местности и их реализация в современных геоинформационных системах, а также предложен подход к формированию таких зон.

зоны размещения, ГИС, технический объект, цифровая модель местности, оптимизация размещения пространственных объектов

Определение зон размещения технических объектов является ключевым этапом в процессе планирования и разработки инфраструктурных проектов. Данный этап требует выполнения анализа параметров местности и существующей инфраструктуры с целью определения допустимых зон, которые будут соответствовать требованиям проекта и выбранных локаций. Анализ параметров местности включает в себя комплексное изучение природно-техногенных геосистем, включая особенности рельефа, гидрографии, почвенного покрова, климатических условий, а также других факторов, которые могут повлиять на выбор места размещения технических объектов. Инфраструктурные параметры, в свою очередь, определяют наличие и состояние дорожно-транспортной сети, электро- и водоснабжения, канализации и других инженерных коммуникаций, которые необходимы для функционирования объектов [1]. При определении границ и параметров зон размещения технических объектов применяются различные методы и технологии: пространственного анализа, геофизики, системного анализа, машинного обучения и искусственного интеллекта [2-3].

В настоящий момент для определения зон размещения технических объектов используются геоинформационные системы (ГИС), в основу кото-

рых положены цифровые карты или цифровые модели рельефа, не позволяющие выполнить всесторонний анализ территории, на которой планируется размещения технических объектов [4-5]. Большинство современных ГИС не имеют развитых механизмов, позволяющих автоматизировать процесс задания допустимых зон размещения технических объектов, после чего воспользоваться поисковым оптимизационным алгоритмом [6].

Допустимые зоны размещения технических объектов могут быть формализовано с использованием языка теории множеств, путем формализованного задания свойств локаций и множества технических объектам, предполагаемых к размещению. Основными объектами в современных ГИС являются точка, линия, полигон и мультиполигон, которые могут быть легко заданы на языке теории множеств. Также на языке теории множеств могут быть заданы свойства территорий, которые допускают размещение заданных типов технических объектов [7].

Описание всех точек полигона на языке теории множеств является важным аспектом при работе с геоинформационными системами и анализе пространственных данных. Полигон, как замкнутая область, состоит из бесконечного числа точек, которые вместе образуют его контур и внутреннюю область. Определение точки внутри полигона является одной из наиболее часто используемых задач в пространственном анализе, которая может быть решена с помощью алгоритма трассировщика луча (рис.1). Данный алгоритм исследует каждую грань полигона и проверяет, сколько раз луч из точки пересекает границу полигона. Если количество пересечений нечетное, то точка находится внутри полигона, в противном случае она считается снаружи.

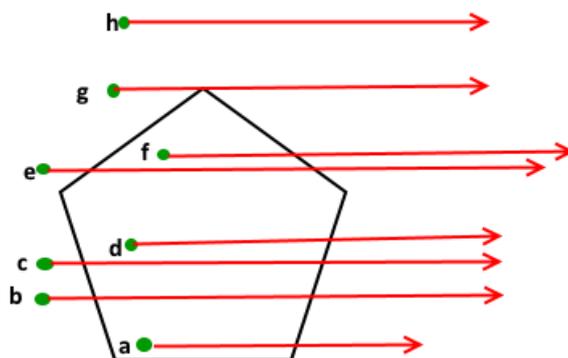


Рис.1. Визуализация алгоритма трассировщика луча

Множество всех точек внутри полигона может быть определено как множество точек, соответствующих алгоритму трассировщика луча (1):

$$VPol = \{ P \mid P \text{ находится внутри полигона } Pol \} \quad (1)$$

А множество всех точек полигона определено как объединение точек внутри полигона и его вершин (2).

$$Polig = Pol \cup VPol \quad (2)$$

Каждый из этих типов объектов играет свою роль в формировании допустимых зон размещения технических объектов. Точки могут указывать на потенциальные места размещения мелких объектов, например, столбов или приборов. Линии могут определять маршруты или транспортные пути, вдоль которых возможно размещение объектов, а также ограничивать зоны, в которых размещение нежелательно. Полигоны же позволяют определять области, где размещение объектов допустимо или недопустимо, например, водоохранная зона, застройка или зона охраняемого ландшафта.

Дороги играют ключевую роль в формировании допустимых зон размещения технических объектов на цифровой модели местности. Дорожная инфраструктура определяет доступность участков местности для размещения технических объектов, поэтому важно, чтобы полигон, на котором возможно размещение технического объекта, был соединен с дорогой, но в то же время, он не должен включать в себя точки на самой дороге, так как технический объект размещен на ней быть не может.

Определение всех точек на дороге можно осуществить путем разбиения дороги на отрезки из двух точек и последующего анализа каждого отрезка для определения всех точек на этом отрезке с использованием длины вектора (3):

$$\begin{aligned} MPoi &= \left\{ \langle x, y \rangle \mid x = x_1 + \frac{d * (x_2 - x_1)}{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}, \right. \\ & \quad y = y_1 + \frac{d * (y_2 - y_1)}{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}, \\ & \quad \left. d \in [0; \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}] \right\}. \end{aligned} \quad (3)$$

Множество всех точек дороги будет представлять из себя последовательное множество таких отрезков:

$$D = (MPoi_1, MPoi_2, \dots, MPoi_n). \quad (4)$$

Следовательно, все дороги на местности будут представлены мультилинией:

$$MD = \{D_1, D_2, \dots, D_n\}. \quad (5)$$

Полигоны, к которым доступен подъезд представляют из себя множество всех полигонов, пересекающихся с дорогой:

$$O = \{ Polig | Polig \cap D \}. \quad (6)$$

Тогда множество всех возможных точек для размещения технического объекта может быть описано формулой:

$$A = M \cap O \cap \bar{D}, \quad (7)$$

где M – множество всех точек плоскости, O – множество точек полигонов, к которым доступен подъезд, D – множество точек дорог.

Выражения (1-7) позволяют выполнить формализацию представления областей, на которых могут быть размещены технические объекты. Следующим шагом является использование задание целевой функции и выбор поискового алгоритма размещения объектов на местности. Исследования могут быть продолжены в направлении автоматического выбора областей допустимых зон размещения технических объектов на основе цифровых карт, цифровых моделях рельефа местности и спутниковых снимков.

Список используемых источников

1. Чернов И. В. Концепция геоинформационного обеспечения / Чернов И. В., Г. К. Осипов. // Информация и космос. 2022. № 3. С. 120–124.
2. Александров Ю. С. О новых подходах в технологиях создания электронных (цифровых) карт / Ю. С. Александров, А. Н. Сердюков, В. А. Леонтьев, С. П. Присяжнюк // Информация и космос. 2022. № 4. С. 152–157.
3. Левадный Ю. В. Комплекс геоинформационного обеспечения / Ю. В. Левадный, И. В. Чернов, Г. К. Осипов // Информация и космос. 2023. № 1. С. 120–125.
4. Чернов И. В. Обобщенная функциональная модель систем геоинформационного обеспечения / И. В. Чернов, Г. К. Осипов // Информация и космос. 2023. № 2. С. 78–83.
5. Верховая Г. В., Акимов С. В. Метод объединения гетерогенных геопространственных данных на основе многоаспектных моделей // Телекоммуникации. 2021. № 3. С. 34–40.
6. Александров Ю. С. Электронные карты повышенной точности – новый вид геопространственной информации / Ю. С. Александров, С. П. Присяжнюк // Информация и космос. 2021. № 4. С. 140–143.
7. Янкелевич С. С. К вопросу создания инфраструктуры геопространственных знаний / С. С. Янкелевич // Информация и космос. 2023. № 2. С. 114–120.

УДК 004.946
ГРНТИ 28.17.33**ПРОГРАММНО-АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ
ДЛЯ УПРАВЛЕНИЯ ПРОСТРАНСТВЕННЫМИ ОТНОШЕНИЯМИ
МЕЖДУ ГЕОГРАФИЧЕСКИМИ ОБЪЕКТАМИ
НА БАЗЕ ТЕМПОРАЛЬНЫХ ГРАФОВ****Г. В. Верхова, И. Ю. Попов**

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

При решении широкого класса задач с помощью геоинформационных технологий требуется учет топологических отношений между пространственно–распределенными объектами, однако в современных геоинформационных системах поддержка топологического моделирования реализована на уровне, недостаточном для современного состояния развития информационных технологий. В статье представлены результаты разработки программно-алгоритмического обеспечения для управления пространственными отношениями между географическими объектами на базе темпоральных графов. В рассматриваемом программном обеспечении реализованы основные операции на темпоральных графах. Данный вид программного обеспечения может быть использовано в перспективных геоинформационных системах, базирующихся на базе знаний.

темпоральные графы, геоинформационные системы, топологические отношения

Решение ряда современных задач, среди которых маршрутизация, анализ сетей, планирование городского развития и экологическое моделирование, требуют учета географических аспектов [1]. Для эффективного решения этих задач широко применяются геоинформационные системы и сервисы, которые автоматизируют сбор и обработку геоданных. Существует проблема в области моделирования топологических отношений в рамках объектно-ориентированной парадигмы. Ограничение в методах и средствах моделирования топологических отношений в геоинформационных системах может значительно снижать точность и эффективность анализа пространственных данных. Недостаточное развитие этих методов приводит к ряду трудностей в процессе принятия решений на основе геоданных при планировании и управлении городскими территориями, транспортной инфраструктурой, экологическими системами и другими сферами, где географические аспекты играют ключевую роль.

Целью данной статьи является разработка программно-алгоритмического обеспечения для управления пространственными отношениями между географическими объектами на базе темпоральных графов. Практическая значимость заключается в том, что предложенная модель топологи-

ческих отношений позволяет явным образом задать топологические отношения между географически распределенными объектами с учетом темпоральных аспектов в рамках объектно-ориентированной парадигмы.

Топология в ГИС отражает пространственные отношения между различными географическими объектами, которые могут быть представлены точками, линиями и полигонами. Топологические отношения позволяют определять, каким образом объекты расположены друг относительно друга на местности, контролировать их геометрическое изменение и положение, проводить анализ на основе их пространственных связей [2].

Топология в ГИС играет ключевую роль, обеспечивая:

- определение пространственных отношений между объектами, таких как соседство, пересечение и прочие пространственные связи;
- выявление и исправление ошибок в геометрии объектов, таких как самопересечения и разрывы;
- проведение разнообразных видов пространственного анализа, включая поиск ближайших объектов, объектов в заданной области, а также расстояний между объектами;
- повышение эффективности выполнения пространственных запросов за счет сокращения числа анализируемых объектов;
- контроль и поддержание в ГИС топологических связей между объектами для соблюдения топологических правил и сохранения данных в согласованном виде;
- решение сложных пространственных задач, учитывающих топологические отношения между объектами, такие как поиск пути вдоль дороги или определение областей видимости;
- поддержку редактирования данных, автоматическое обновление связей и отношений при изменении геометрии объектов, позволяющих сохранить целостность данных.

В геоинформационных системах важно учитывать временные изменения. Идея подхода учета темпорального аспекта в пространственных отношениях представлена на рис. 1. Здесь с помощью темпорального графа представлено объединение двух пространственных объектов «Объект_В» и «Объект_А» в новый объект «Объект_{АВ}», учитывая то, что изначально два ранее упомянутых объекта существовали отдельно друг от друга. На модели исходные ребра выделены бирюзовым цветом, а «Объект_В» имел топологическую связь с объектом «Объект_С», поэтому происходит создание новой топологической связи «L_{АВ-С}», данное ребро выделено красным цветом. Ребра, которые отражают темпоральные связи нового объекта «Объект_{АВ}» с родительскими объектами «Объект_А» и «Объект_В», выделены зеленым цветом. Архивные связи и объекты выделены оранжевым цветом. Данный под-

ход полностью отвечает парадигмы объектно-ориентированного моделирования топологических отношений, так как каждый объект и каждая связь между объектами являются отдельными сущностями.

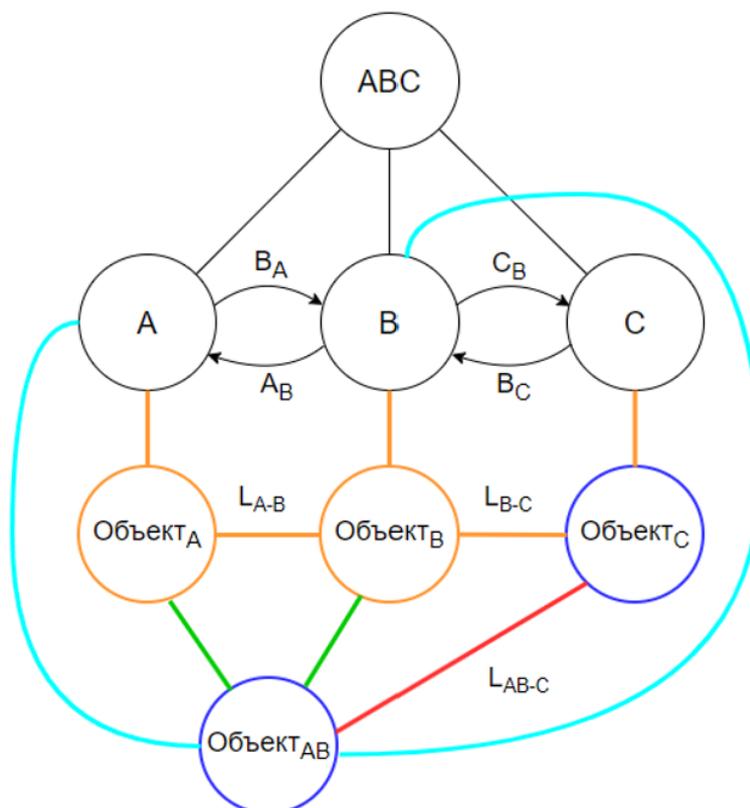


Рис. 1. Объектно-ориентированная модель топологических отношений

В графах топологические отношения часто представляются числами для удобства их анализа. В матрице смежности графа соприкосновение может быть обозначено единицей, пересечение – двойкой, содержание – тройкой, вложение – четверкой, а близость – пятеркой [3]. Для объединения текущей матрицы смежности с темпоральным графом используется формула:

$$g_{i,j}^t = \begin{cases} g_{i,j}^{t-1} + g_{i,j}^t, & \text{если } \exists i, j \text{ в } t \text{ и } \exists i, j \text{ в } t - 1 \\ g_{i,j}^t, & \text{если } \exists i, j \text{ в } t \text{ и } \nexists i, j \text{ в } t - 1 \\ 6, & \text{если } \nexists i, j \text{ в } t \text{ и } \exists i, j \text{ в } t - 1 \end{cases}, \quad (1)$$

где $g_{i,j}^{t-1}$ – тип связи в предыдущий момент времени; $g_{i,j}^t$ – тип связи в текущий момент времени; $i, j \in \{1 \dots n\}$, n – количество объектов на карте.

Если объект не существует на карте, то в формуле (1) ему будет присвоено значение «6» [4].

Пусть G_1 – матрица смежности в момент времени t_1 , G_2 – матрица смежности в момент времени t_2 , то итоговая матрица темпорального графа при сложении будет иметь следующий вид:

$$G_t = G_1 + G_2, \quad (2)$$

Матрица смежности статического графа G_t состоит из добавленных и существующих объектов.

На рис. 2 представлены объекты в момент времени t_1 и t_2 . В момент времени t_2 произошло добавление объекта 4, что повлекло за собой изменение матрицы смежности статического графа в момент времени t_2 . Для каждого момента времени составлены матрицы смежности статического графа и матрица смежности темпорального графа, в котором показано, что в момент времени t_1 объект 4 не существовал, а в момент времени t_2 был добавлен.

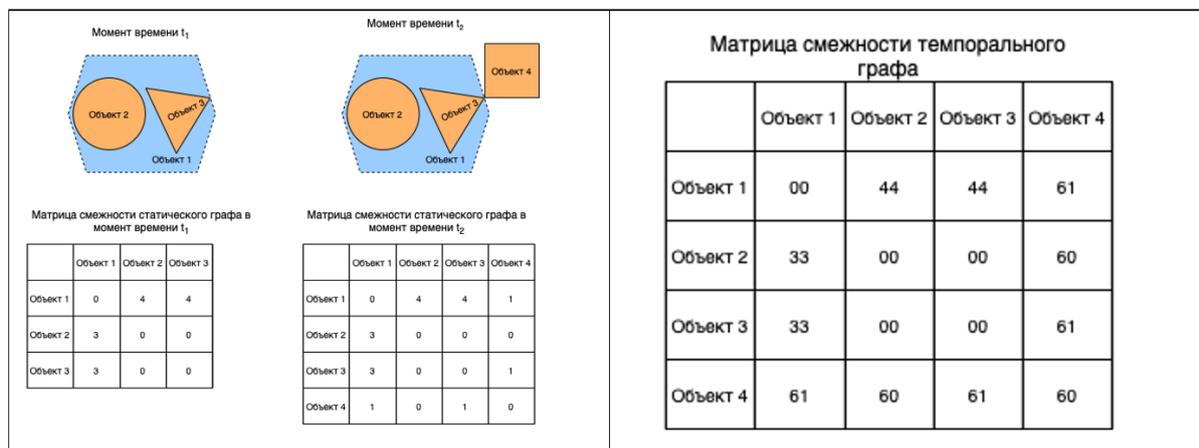


Рис. 2. Пример сложения матриц смежности темпорального и статического

В процессе выполняемых исследований был разработан прототип программного обеспечения, выполненный в виде веб-приложения, включающий в себя тестовый вариант пользовательского интерфейса, демонстрирующего работу алгоритма по управлению пространственными отношениями между географическими объектами. На рис. 3 показано изменение границы между корпусами дома на момент времени t_2 , после выполнения объединения двух корпусов.



Рис. 3 Тестовый пользовательский интерфейс

Список используемой источников

1. Верхова Г. В., Акимов С. В. Метод объединения гетерогенных геопространственных данных на основе многоаспектных моделей // Телекоммуникации. 2021. № 3. С. 34–40.
2. Vassilis Kostakos. Tempotal Graphs // Physica A: Statistical Mechanics and its Applications. 2009. №. 6. PP. 1007–1023.
3. Берштейн, Л. С. Использование темпоральных графов, как моделей сложных систем / Л. С. Берштейн А. В. Боженюк // Известия Южного федерального университета. Технические науки. 2010. № 4. Т. 105. С. 198–203.
4. Ereemeev S. V., Andrianov D. E., Komkov V. A. Comparison of Urban Areas Based on Database of Topological Relationships in Geoinformational Systems, Pattern Recognition and Image Analysis. 2015. Vol. 25. № 2. PP. 314–320.

УДК 004.738
ГРНТИ 50.41.23

МЕТОД ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ИНТЕРОПЕРАБЕЛЬНЫХ КИБЕРСРЕДАХ

Г. В. Верхова, А. Ю. Суетин

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

Предложен метод реализации информационного взаимодействия в рамках единой киберсреды, сформированной из локальных интероперабельных киберсред. Предложенный метод отличается организацией информационного взаимодействия с помощью агентов трех типов. Представлены модели формирования агентов для реализации информационного взаимодействия между локальными киберсредами. Рассмотрены примеры возможной реализации агентного подхода на уровне синхронизации баз данных.

киберсреда, виртуальная организация, виртуальное предприятие, интероперабельная киберсреда

Киберфизическая среда представляет собой совокупность технических и программных средств, обеспечивающих активное взаимодействие людей, социальных групп и киберфизических систем [1–2]. Киберфизическая среда создается на базе децентрализованного цифрового двойника реального мира с использованием мультиагентных технологий. В рамках киберсреды функционируют взаимодействующие между собой аппаратные и программные средства, обеспечивая в реальном масштабе времени решение задач по управлению автоматизированными производственными системами.

Проектирование цифровой инфраструктуры предприятия должно учитывать взаимодействие между физическими и цифровыми активами, а также между людьми, участвующими в производственном процессе. Каждый цифровой актив должен быть способен устанавливать связи и взаимодействовать с другими цифровыми активами, аналогично тому, как это происходит на реальном физическом предприятии. Взаимодействие всех участников производственного процесса в рамках киберфизической среды реализуется с помощью агентов. Программно-аппаратное обеспечение киберсреды автоматизированных производственных систем должно создавать с использованием магистрально-модульного принципа построения [3]. На рис. 1 представлены возможные типы связей, которые могут устанавливать агенты друг с другом [4].

Учитывая возможные типы связей между агентами, киберсреду, основанную на агентном подходе, можно представить в виде следующего выражения:

$$CE = \langle P, B, M, P2P, B2B, M2M, P2B, P2M, B2M \rangle \quad (1)$$

где P – физическое лицо, B – коллектив физических лиц, включая организационные единицы и организации (юридические лица), M – физический актив, $P2P$ – связь «физическое лицо – физическое лицо», $B2B$ – связь «коллектив – коллектив», $M2M$ – связь «физический актив – физический актив», $P2B$ – связь «физическое лицо – коллектив», $P2M$ – связь «физическое лицо – физический актив», $B2M$ – связь «коллектив – физический актив».

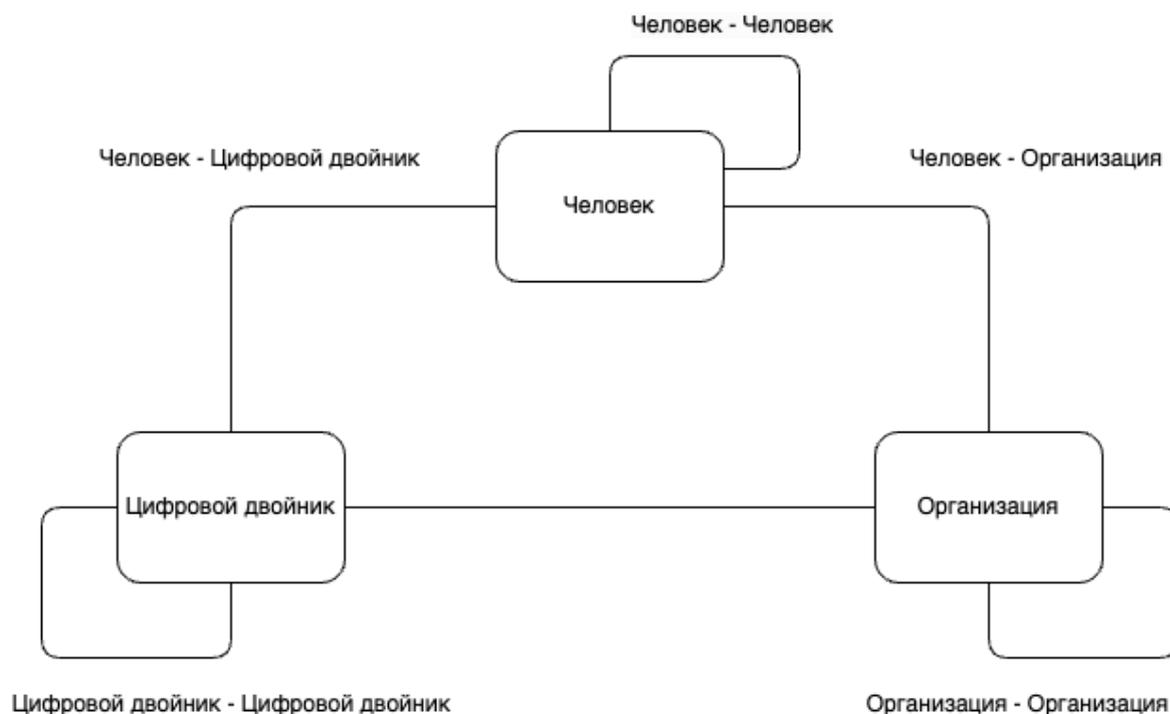


Рис. 1. Типы связи для агентов

Агент, являющийся представителем некоего актива, способного устанавливать связи с другими агентами, может быть представлен в виде следующем виде:

$$A = \langle Atr, Act, R, S, Ch \rangle, \quad (2)$$

где $Atr = \langle Atr1, Atr2, \dots, Atrn \rangle$ – множество свойств и характеристик, $Act = \langle Act1, Act2, \dots, Actn \rangle$ – множество все возможных действий, которые может совершить агент, $R = \langle R1, R2, \dots, Rn \rangle$ – множество всех связей с другими агентами, $S = \langle S1, S2, \dots, Sn \rangle$ – множество состояний агента во

время выполнения действий, $Ch = \langle Ch1, Ch2, \dots, Chn \rangle$ – множество, содержащие способы и средства коммуникации между агентами так-как агент может быть представлен физическим устройством.

Модель формирования связей между агентами, зарегистрированными в различных киберсредах, может быть представлена в виде следующего выражения:

$$A = \langle A1, A2, Type, T1, T2, State, I, ID1, ID2 \rangle \quad (3)$$

где A_1, A_2 – агенты, между которыми устанавливается информационная связь, $Type$ – тип связи, $T1, T2$ – время установления и время завершения действия связи, $State$ – состояние связи, I – дополнительная информация, $ID1, ID2$ – идентификаторы киберсреды, в которых зарегистрированы участники, между которыми устанавливается связь.

В современном информационном пространстве обеспечение интероперабельности между киберсредами является одной из основных проблем, возникающих при построении цифрового пространства производственных систем. Решение данной проблемы может быть достигнуто с помощью двух основных методов: унификация функционального взаимодействие через API и репликация баз данных. Механизм взаимодействия через API представляет собой гибкую методiku, позволяющую киберсредам обмениваться данными и ресурсами. Использование API обеспечивает возможность стандартизации интерфейсов, что способствует более эффективной интеграции различных систем. Такой метод позволяет обеспечить агентам независимость от конкретной среды и обеспечивает возможность оперировать информацией в любой из них.

Метод, основанный на репликации баз данных, предполагает создание синхронизированных копий (реплик) баз данных и их распределение между различными киберсредами [5]. При данном методе основной целью является обеспечение полной синхронизации таблиц, представляющих информацию об агентах в каждой из сред, что позволяет гарантировать доступность и актуальность информации о каждом агенте независимо от его местоположения или регистрации в киберпространстве.

Оба метода имеют свои достоинства и недостатки, и выбор между ними зависит от конкретных потребностей и особенностей решаемой задачи. Вне зависимости от выбранного метода, обеспечение интероперабельности между киберсредами является ключевым аспектом, обеспечивающим эффективное функционирование информационной инфраструктуры и повышение уровня автоматизации и координации в современном цифровом мире.

На рис. 2 представлен процесс формирования интеграционной модели агента, которая обладает минимально необходимым набором параметров

для создания реплики агента в другой киберсреде. На рис. 3 представлено итоговое состояние киберсред после создания реплик агентов. В современной цифровой инфраструктуре имеет смысл рассматривать двухуровневую стратегию обеспечения согласованности данных между различными киберсредами. Первый уровень предполагает использование обычной репликации для информации, которая не требует строгой гарантии отсутствия изменений со стороны каждого агента. На данном уровне акцент делается на обеспечении полной эквивалентности реплик в различных локальных киберсредах. Обычная репликация баз данных позволяет эффективно распространять данные между узлами системы, обеспечивая их доступность и согласованность. Таким образом, данный уровень служит основой для обмена информацией между участниками в процессе управления общими ресурсами без строгого контроля за изменением данных каждым из них.

В некоторых случаях требуется более высокий уровень доверия и контроля над согласованностью данных. Для этой цели предлагается второй уровень стратегии, основанный на использовании технологии блокчейн, которая обеспечивает строгий контроль над эквивалентностью реплик данных путем распределенного и надежного хранения информации, неконтролируемое изменение которой невозможно без согласия большинства участников.

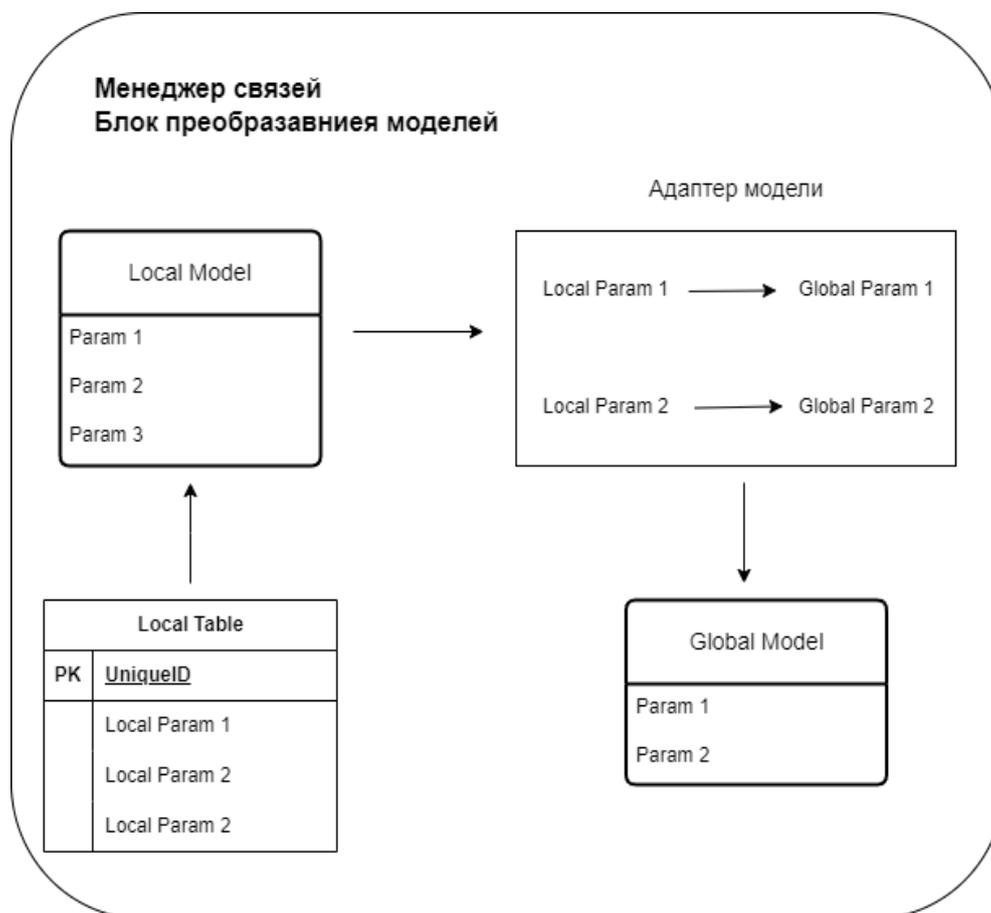


Рис. 2. Формирование интеграционной модели агента

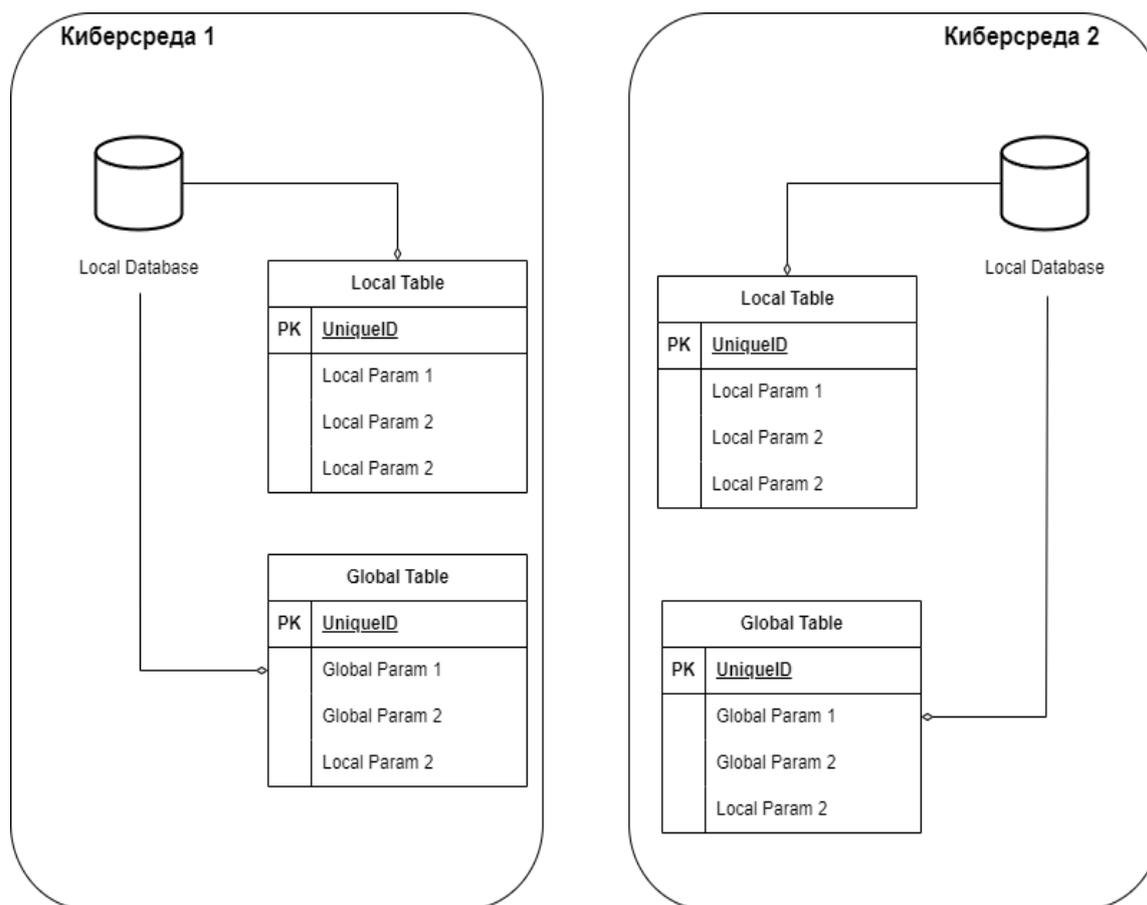


Рис. 3. Итоговое состояние киберсред после интеграции агентов

Предложенный метод создает два слоя обработки данных: основанный на обычной репликации, используемый для информации с невысоким уровнем доверия и требований к согласованности, а также слой, использующий технологию блокчейн, предназначенный для обеспечения высокой степени надежности и доверия к данным. Данный метод позволяет эффективно удовлетворять потребностям и ограничениям в области обработки данных в современных киберсредах автоматизированных производственных систем.

Список используемых источников

1. Seyed H., Jörg H. Design of Cyber-Physical Systems: An Interdisciplinary Approach, 2020.
2. Gabor K., Insup L., Sokolsky O. Cyber-Physical Systems: A Computational Perspective, 2015.
3. Кходер Х., Верхова Г.В., Акимов С.В. Модульная технология проектирования гибких сложных систем // Т-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 86–90.
4. Верхова Г. В., Акимов С. В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // В сборнике: Волновая электроника и инфокоммуникационные системы. Сборник статей XXIV Международной научной конференции. Санкт-Петербург, 2021. С. 34–39.
5. Schönig H. PostgreSQL Replication – Second Edition, 2015.

УДК 004.9
ГРНТИ 20.53.01

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ИНЖЕНЕРНОГО ПРОФИЛЯ В ТЕЛЕКОММУНИКАЦИОННЫХ ВУЗАХ

Е. С. Владимирова¹, Е. С. Крюкова²

¹ Севастопольский государственный университет

² Военная академия связи им. Маршала Советского Союза С.М. Буденного

В статье говорится о стремительном развитии, активном внедрении и использовании в процессе подготовки специалистов инженерного профиля современных информационных технологий. Это позволяет сделать электронные образовательные ресурсы более доступными для широкой аудитории пользователей, способствует повышению интенсивности и эффективности учебного процесса.

электронная информационная образовательная среда вуза, электронная библиотека, контент, информационные технологии, дистанционное обучение, доступность электронных образовательных ресурсов, обучающиеся, профессорско-преподавательский состав

В настоящее время в высших учебных заведениях России активно развивается электронная информационно-образовательная среда (ЭИОС). В процесс обучения широко внедряется использование различных цифровых технологий, информационно-поисковых, информационно-справочных систем.

Электронная информационно-образовательная среда – совокупность организационных, технических, технологических и методических условий разработки, поиска, сбора, хранения, обработки, предоставления и распространения информационных ресурсов в электронно-цифровой форме при реализации образовательной организацией и освоении обучающимися основных и дополнительных профессиональных образовательных программ [1]. Иными словами, ЭИОС подразумевает использование в образовательной деятельности различных информационных технологий как для организации учебного процесса в вузе, так и для осуществления его мониторинга и контроля.

Основным достоинством применения в процессе преподавания различных информационных технологий является индивидуальный неограничен-

ный доступ к ЭИОС вуза из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории вуза, так и вне его.

Внедрение и использование современных информационных технологий актуально и для подготовки специалистов инженерного профиля в телекоммуникационных вузах. К таким перспективным технологиям относятся автоматизированные информационно-справочные, информационно-поисковые системы: электронная библиотека (ЭБ) обеспечивает доступ обучающихся к электронным образовательным ресурсам (ЭОР); электронный журнал (ЭЖ) предназначен для ведения и контроля успеваемости; электронная система тестирования служит для проверки качества усвоения материала занятий по различным дисциплинам, а также системы информационных ресурсов организации образовательной, научно-исследовательской и повседневной деятельности вуза в целях управления и мониторинга учебного процесса [1, 2].

Одним из ведущих телекоммуникационных вузов страны, осуществляющим подготовку высококвалифицированных специалистов инженерного профиля в интересах Министерства обороны (МО) Российской Федерации (РФ) является Военная академия связи. В учебном заведении стремительно развивается, активно используется и постоянно совершенствуется ЭИОС. Структура ЭИОС академии представлена следующими элементами: системой информационных ресурсов; системой организации образовательной деятельности вуза; системой научно-исследовательской деятельности; системой повседневной деятельности вуза и организационно-технической системой. Все перечисленные системообразующие элементы ЭИОС предназначены для управления образовательной деятельностью академии, организации взаимодействия между различными формами проведения занятий и реализации дистанционных технологий обучения [3].

С помощью этих систем осуществляется доступ участников образовательного процесса со всех автоматизированных рабочих мест (АРМ) к информационно-образовательной базе академии, а именно, к ЭОР, размещенным в ЭБ, виртуальным турам и тренажерам, расписанию занятий, системам тестирования, электронному журналу, сайтам кафедр и другим структурным подразделениям вуза, а также иным информационным ресурсам, находящимся в локальной сети образовательной организации. Доступ осуществляется с учетом разграничения прав различных категорий пользователей к информационным ресурсам академии. Перечисленные автоматизированные системы имеют модульную структуру, что обеспечивает простоту их использования как для обучающихся, так и для профессорско-преподавательского состава.

Основное достоинство подобных информационно-справочных, информационно-поисковых систем – предоставление широких возможностей различным категориям пользователей. Системы такого класса поддерживают обработку и хранение больших объемов информации; оперативный поиск необходимых сведений; размещение и уничтожение ЭОР, основу которых составляет всевозможный обучающий контент (презентации, материалы проведения занятий, учебные фильмы и аудио-лекции, а также электронные учебники, учебные пособия и тесты) и обмен файлами любых форматов между пользователями.

Одной из информационно-поисковых, информационно-справочных систем заслуживающих особого внимания является ЭБ. Это сложная автоматизированная система, предназначенная для управляемого доступа пользователей к ее контенту. Важными преимуществами ЭБ является то, что она позволяет широко внедрять новейшие технологии, обеспечивающие доступ к большому объему ЭОР на качественно новом уровне, а также то, что развертывание систем такого класса не требует значительных затрат времени и средств. Предполагается, что ЭБ является телекоммуникационным и информационным узлом, обеспечивая оперативный, удобный и управляемый доступ к информации, профессиональным базам данных, информационным справочным и поисковым системам, и иным информационным ресурсам [4].

Главными и значимыми достоинствами ЭБ являются доступность ЭОР, размещенных в ней, практически с любого АРМ, имеющего подключение к сети Интернет, а также возможность осуществления дистанционного обучения. В учебном процессе академии используются информационные ресурсы нескольких ЭБ: Единой ЭБ МО РФ, ЭБ академии и внешние ЭБ (например, ЭБ «Лань»). Ключевой составляющей ЭБ является ее контент, который представляет собой образовательный ресурс в цифровом виде. Он также включает в себя структуру, предметное содержание и метаданные о нем [5].

В ходе реализации образовательной деятельности особое внимание уделяется вопросам контроля усвоения учебного материала. Для решения данной задачи посредством тестирования в академии реализуются два подхода. Первый – это использование встроенной системы тестирования в электронный учебник. Данный вариант удобен для процедуры самоконтроля обучающихся в процессе самостоятельной работы. Второй – автономная система тестирования, которая позволяет осуществлять контроль знаний большого количества обучающихся с использованием базы вопросов по необходимой дисциплине. Данный подход удобен в ходе проведения практически всех видов учебных занятий либо промежуточной аттестации.

Одной из самых рутинных процедур планирования учебного процесса является составление расписания занятий на большое количество групп обучения. В него вовлечено большое количество подразделений академии, ко-

торые предоставляют необходимые исходные данные для составления расписания. В результате формируется расписание учебных занятий для групп, для профессорско-преподавательского состава, имеется возможность загрузки расписания за конкретную кафедру, а также анализ занятости аудиторного фонда.

Задачу учета и анализа результатов успеваемости обучающихся академии успешно решает информационная система «Электронный журнал». Она позволяет одновременно осуществлять ввод, обрабатывать и проводить анализ большого количества данных об успеваемости обучающихся. Так, при необходимости имеется возможность формирования запросов за определенный период, например, по количеству неудовлетворительных оценок в учебных группах, проценту отсутствующих на занятиях, поиску отдельного обучающегося и результатов его успеваемости, а также сводные данные по успеваемости за группу, факультет, кафедру. Большие возможности этой информационной системы позволяют качественно осуществлять контроль результативности обучения в вузе.

Важными и обязательными элементами ЭИОС академии являются информационно-справочные системы – сайт академии и сайты ее структурных подразделений (кафедр). Здесь представлена основная информация об их деятельности: основные функции и задачи, личный состав, новости, ЭОР в разделе «библиотека» и другие полезные материалы.

Еще одна составляющая ЭИОС академии – информационная система «Антиплагиат». С помощью нее выпускные квалификационные работы обучающихся в соответствии с требованиями руководящих документов проверяются на наличие заимствований.

Научная работа является обязательным видом деятельности для исследовательского и педагогического состава академии. С целью эффективности планирования, учета и контроля выполнения основных мероприятий научной деятельности в ЭИОС включена информационная система «Портал научной работы».

Помимо развития ЭИОС вуза, одним из новых и активно внедряющихся в учебный процесс направлений развития и совершенствования информационных технологий, применяемых в образовательной деятельности, является использование виртуальных машин (ВМ) и виртуальных классов (ВК) [6]. На сегодняшний день в академии такая возможность реализована посредством виртуальной лаборатории PNETLAB – это программное обеспечение (ПО) с широкими возможностями подготовки специалистов инженерного профиля по общетехническим дисциплинам. С использованием PNETLAB появляется возможность организовать сетевую форму проведения занятий. Преподаватель может дистанционно контролировать работу обучающихся, проводить индивидуальные консультации, не отвлекая дру-

гих обучающихся, а также оценить результаты работ в ВК. PNETLAB представляет собой свободно распространяемое ПО, обладающее всеми необходимыми средствами для подготовки сетевых инженеров. Его применение дает возможность создавать сложнейшие виртуальные лаборатории, с использованием готовых конфигураций сетевых устройств и операционных систем, с большой вариативностью. При этом для каждого обучающегося лаборатория может эмулироваться индивидуально. Сформировать такие лабораторные стенды для каждого обучающегося на физическом оборудовании практически нереально. Использование узлов с различными операционными системами (Windows, Linux и др.) предоставляет возможность применения различного программного обеспечения (Matlab, Mathcad, Компас-3D и др.). Все это способствует качественной организации образовательного процесса.

Использование виртуальных классов позволяет резко сократить время на подготовку персональных машин к учебному занятию. Нет необходимости администрировать 100 % машин обучающихся, достаточно подготовить одну виртуальную сетевую машину с необходимым ПО и создать учетные записи пользователей.

Таким образом, внедрение в учебный процесс сетевых ВК является первым шагом на пути создания единого информационно-образовательного пространства вуза, что еще недавно было перспективой развития ЭИОС. С помощью PNETLAB обучающийся полностью погружается в единое информационно-образовательное пространство и может использовать практически все элементы ЭИОС вуза.

В статье описан вариант использования современных информационных технологий в процессе подготовки специалистов инженерного профиля на примере одного из ведущих телекоммуникационных вузов МО РФ. Представлены достоинства применения информационно-справочных, информационно-поисковых систем в образовательной деятельности вуза. Описана актуальность и преимущества применения виртуальных технологий в учебном процессе. Дальнейшее развитие и внедрение различных информационных технологий в образовательную деятельность с учетом непрерывного роста науки, техники, общества, а вместе с тем и подходов к обучению является неизбежным и неоспоримым фактом.

Список используемых источников

1. Антопольский А. Б., Маркарова Т. С., Крюкова О. П., Харламов А. А. Электронные библиотеки в образовании // Под редакцией О. П. Крюковой, А. А. Харламова. М., 2009. 94 с.
2. ГОСТ Р 7.0.96-2016 Национальный Стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. М.: Стандартинформ, 2018. 11 с.

3. Ренсков А. А., Чирушкин К. А., Чирушкин А. Н. Опыт применения дистанционных технологий обучения в информационно-образовательной среде вуза. // Итоги науки и техники: Научно-технический сборник № 120. Труды академии. СПб.: ВАС, 2023. С. 493–498.

4. Временный регламент работы и взаимодействия органов военного управления, воинских частей и образовательных организаций Вооруженных Сил Российской Федерации в процессе функционирования открытой части Электронной библиотеки Министерства обороны Российской Федерации утвержденный начальником Генерального штаба Вооруженных Сил Российской Федерации 05 декабря 2016.

5. Паращук И. Б., Крюкова Е. С. Контент электронных образовательных ресурсов как инновационная среда подготовки военных и инженерно-технических кадров. // Военная безопасность России: взгляд в будущее: Материалы 8-й Международной межведомственной научно-практической конференции научного отделения № 10 РАН. Москва, 16 марта 2023 г.: в 3 т. // ФГБУ «РАРАН», ФГБОУ ВО «МГТУ им. Н.Э. Баумана», ФГКВОУ ВО «Военная академия ГШ ВС РФ». М.: Издательство МГТУ им. Н.Э. Баумана, 2023. Т. 2. 277 с. С. 182–187.

6. Чирушкин К. А., Пащенко В. В., Логинов В. А. Применение виртуальных технологий в образовательной деятельности Военной академии связи. // Итоги науки и техники: Научно-технический сборник № 122. Труды академии. СПб.: ВАС, 2023. С. 241–247.

УДК 004.8
ГРНТИ 28.23.37

СРЕДСТВА ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ НОВОСТНЫХ ТЕКСТОВ В ИНТЕЛЛЕКТУАЛЬНЫХ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ

И. А. Внуков, Ф. В. Филиппов

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

Описано современное состояние и перспективы развития интеллектуальных рекомендательных систем. Актуализирована интеграция моделей глубокого обучения в интеллектуальные рекомендательные системы. Исследованы различные архитектуры моделей глубокого обучения, включая полносвязные нейронные сети прямого распространения, одномерные сверточные нейронные сети, рекуррентные нейронные сети, а также архитектуру Transformer, в контексте их применения для классификации русскоязычных новостных текстов. Проведен сравнительный анализ с учетом различных гиперпараметров, направленных на оптимизацию точности и производительности моделей.

искусственные нейронные сети, глубокое обучение, интеллектуальные рекомендательные системы, классификация текстов.

В современном информационном мире, насыщенном огромным объемом данных, интеллектуальные рекомендательные системы (ИРС) играют ключевую роль в облегчении доступа пользователей к нужной информации. Одним из важных аспектов их функционирования является способность классифицировать и фильтровать контент, адаптируя его к индивидуальным потребностям и интересам. ИРС включают в себя способность точно определять тему и содержание текстов, что особенно важно в контексте новостных ресурсов, где быстрая и точная классификация текстов позволяет эффективно предлагать пользователю релевантную информацию.

В настоящее время существует большое количество средств глубокого обучения для решения различных задач обработки естественного языка, включая классификацию текста. Однако выбор конкретного подхода в значительной степени зависит от языковой системы и предметной области задачи [1]. Естественные языковые системы – не изоморфны, каждая из них отражает определенную культуру и контекст. Предметная область задачи определяет векторное пространство слов, потому что у каждой задачи своя

специфика семантических отношений. В связи с этим проведен сравнительный анализ различных архитектур искусственных нейронных сетей, обученных классифицировать русскоязычные новостные тексты, с целью выявления наиболее эффективных подходов, которые могут быть интегрированы в ИРС.

Для проведения сравнительного анализа собран набор данных, состоящий из 5100 новостных текстов, охватывающих различные новостные категории (классы). Всего в наборе данных представлено 12 классов. Данные разделены на обучающую, проверочную и тестовую выборки в следующих пропорциях: 3060 образцов для обучения моделей, 1020 для проверки и 1020 для тестирования. Такой подход к разделению данных позволяет эффективно оценить производительность моделей на каждом этапе их обучения.

Сравнительный анализ моделей произведен по следующим метрикам: точность (доля объектов, верно отнесенных к положительному классу относительно всех объектов, отнесенных к этому классу), полнота (доля объектов, верно отнесенных к положительному классу относительно всех объектов, которые фактически принадлежат к этому классу), F1-мера (гармоническое среднее между точностью и полнотой), а также AUC-ROC (вероятность того, что модель правильно классифицирует случайно выбранный положительный объект выше, чем случайно выбранный отрицательный объект) и AUC-PR (соотношение точности и полноты при различных пороговых значениях). Эти метрики позволяют получить представление о производительности моделей классификации и оценить их эффективность.

Перед обучением и эксплуатацией моделей необходимо провести векторизацию текста, поскольку модели глубокого обучения оперируют числовыми тензорами. Этот процесс включает стандартизацию текста (с удалением общеупотребительных слов с малой смысловой нагрузкой), его токенизацию и преобразование каждого токена в числовой вектор.

В данной статье рассмотрены следующие архитектуры моделей классификаторов, каждая из которых использует соответствующий способ кодирования текста:

- многослойный перцептрон (MLP) [2] с использованием бинарного (прямого) кодирования отдельных слов (униграмм);
- MLP с использованием униграмм и показателем TF-IDF [3] для оценки степени важности слов в контексте;
- MLP с использованием бинарного кодирования пар слов (биграмм);
- MLP с использованием биграмм и показателем TF-IDF;
- одномерная сверточная нейронная сеть (CNN) [4] с использованием векторных представлений слов для кодирования их смысловой нагрузки;
- рекуррентная нейронная сеть с долгой краткосрочной памятью (LSTM) [5] с использованием векторных представлений слов;

- рекуррентная нейронная сеть с управляемым рекуррентным блоком (GRU) [6] с использованием векторных представлений слов;
- Автокодировщик Transformer [7] с использованием векторных представлений слов.

MLP-модели обрабатывают текст в виде «мешков слов», остальные же – в виде последовательностей. Во время обучения все модели получают на вход пакет данных из 32 новостных текстов. После этого происходит векторизация текста с ограничением в 20000 токенов. В моделях последовательностей также добавлен слой, конвертирующий целые индексы в плотные векторы для создания векторных представлений.

На выходе каждой модели находится полносвязный слой из 12 нейронов, каждый из которых применяет сигмоидную функцию активации и соответствует определенному классу.

Для оптимизации настройки обучаемых параметров применены: L1 и L2 регуляризации, прореживание, алгоритм адаптивной оптимизации Adam, а в качестве функции потерь – бинарная кросс-энтропия [2].

Полносвязные сети MLP включают в себя 2 скрытых слоя с функцией активации ReLU: в первом слое 512 нейронов, а во втором – 256. Такая структура способная обрабатывать неупорядоченные множества токенов. При этом в качестве токена можно использовать не одно слово, а целые группы из соседних слов – N -граммы, где в токен входят от 1 до N слов. N -граммы позволяют вносить в «мешок» информацию о локальном порядке слов. Помимо этого, в представление можно добавить степень важности слова в данном контексте, оценивая его частоту встречаемости во всем наборе данных, с помощью TF-IDF нормализации.

Анализ табл. 1 подтверждает, что при решении задачи классификации новостных текстов однозначно важна информация о значимости токена (которую предоставляет TF-IDF). Также на улучшение точности модели влияет информация о локальном порядке слов.

При обработке последовательностей важно использовать вместо прямого бинарного кодирования векторное представление слов: во-первых, прямое кодирование создаёт большие разреженные векторы, что приводит к большому объёму входных данных и, как следствие, большому количеству вычислений, а во-вторых, прямое кодирование не отображает семантическую связь между словами, потому что абсолютно все векторы закодированных слов будут ортогональны друг другу [1]. Таким образом, векторные представления позволяют создать пространство плотных векторов, несущих в себе информацию о значении слов в данном контексте.

Одним из эффективных подходов к обработке последовательностей являются одномерные сверточные сети. Одномерная CNN включает в себя 2 скрытых слоя свёртки: с 64 фильтрами и размером окна свёртки равным 5 и с 128 фильтрами, а также с размером окна свёртки равным 3 соответственно;

после каждого слоя свёртки происходит пакетная нормализация, а затем применяется функция активации ReLU. За свёрточными слоями следует слой субдискретизации (pooling) с функцией глобального максимума.

ТАБЛИЦА 1. Сравнительный анализ моделей MLP

Оценка	MLP, униграммы	MLP, униграммы + TF-IDF	MLP, биграммы	MLP, биграммы + TF-IDF
Количество обучаемых параметров	2 569 164	2 569 164	2 569 164	2 569 164
Точность (Precision)	79,4 %	78,8 %	77,2 %	78 %
Полнота (Recall)	45,9 %	56,8 %	49,7 %	59,6 %
F1-мера	38,9 %	50,4 %	36,4 %	55,2 %
AUC-ROC	92,7 %	91,9 %	92,8 %	92,7 %
AUC-PR	72,7 %	73,3 %	73,1 %	75,3 %

Рекуррентные нейронные сети (RNN) имеют внутренний цикл, реализующий память о предыдущих состояниях сети. Это позволяет эффективно обрабатывать временные последовательности. Две наиболее успешные архитектуры рекуррентных слоев – это ячейки LSTM и GRU, которые решают проблему затухания градиента в классической версии RNN. Модель RNN с долгой краткосрочной памятью включает в себя 2 скрытых слоя из двунаправленных ячеек LSTM с 64 и 32 выходами соответственно. Аналогично, модель RNN с управляемым рекуррентным блоком включает в себя 2 скрытых слоя из двунаправленных ячеек GRU с 64 и 32 выходами.

В большинстве задач обработки естественного языка рекуррентные нейронные сети уступают архитектуре моделей Transformer. Transformer, в отличие от остальных моделей последовательностей, не зависит от порядка слов, но, при этом, учитывает информацию об их положении, что позволяет ему рассматривать разные части предложения. Для этого в представление слов внедрена информация о порядке с помощью позиционного кодирования. Кодировщик Transformer состоит из механизма внутреннего внимания (многоголовое внимание) с использованием двух голов, а также плотной проекции (двух полносвязных слоёв из 64 и 256 нейронов соответственно) с добавлением слоёв нормализации и остаточных связей. Сверх кодировщика установлен pooling слой с функцией глобального максимума.

Анализ табл. 2 показывает, что для задачи классификации новостных текстов среди моделей последовательностей архитектура автокодировщика Transformer лидирует в точности. Однако такая модель уступает модели

MLP, использующей биграммы и показатель TF-IDF, в F1-мере и в соотношении точности и полноты (AUC-PR). Более того, Transformer, как и все рассмотренные модели последовательностей, дольше обучается и требует в разы больше ресурсов, чем модели MLP. Всё это свидетельствует о том, что в контексте данной задачи информация о последовательности слов и их семантических связях не даёт оптимального прироста в точности моделей.

ТАБЛИЦА 2. Сравнительный анализ моделей последовательностей

Оценка	CNN	LSTM	GRU	Transformer
Количество обучаемых параметров	5 236 940	5 326 348	5 275 532	6 099 788
Точность (Precision)	82,3 %	78,1 %	73,4 %	75,7 %
Полнота (Recall)	29,5 %	44,6 %	40 %	49,8 %
F1-мера	53,2 %	34,8 %	32,4 %	43,8 %
AUC-ROC	88,4 %	90,7 %	88,5 %	93 %
AUC-PR	64,7 %	68,1 %	63,8 %	73 %

Таким образом, для задачи классификации новостных текстов в рамках ИРС лучшим решением является использование модели MLP с прямым кодированием биграмм и показателем TF-IDF.

Список используемых источников

1. Шолле Ф. Глубокое обучение на Python. 2-е международное издание. СПб.: Питер, 2023. С. 384–448. ISBN: 978-5-4461-1909-7.
2. Филиппов Ф. В. Нейросетевые технологии: учебное пособие. СПбГУТ. СПб., 2020.
3. Jones K. S. A statistical interpretation of term specificity and its application in retrieval // Journal of Documentation. MCB University Press. 2004. № 60(5). PP. 493–502.
4. Lecun Y., Boser B., Denker J. S., Henderson D., Howard R. E., Hubbard W., Jackel L. D. Backpropagation applied to handwritten zip code recognition. // Neural Computation, 1989. № 1(4). PP. 541–551.
5. Hochreiter S., Schmidhuber J. Long short-term memory // Neural Computation, 1997. № 9(8). PP. 1735–1780. PMID 9377276.
6. Cho K., van Merriënboer B., Gulcehre C., Bougares F., Schwenk H., Bengio Y. Learning phrase representations using RNN encoder-decoder for statistical machine translation. // Conference on Empirical Methods in Natural Language Processing. 2014.
7. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser L., Polosukhin I. Attention Is All You Need // NeurIPS. 2017. PP. 5998–6008.

УДК 004.056
ГРНТИ 81.93.29

КОМПЛЕКСНАЯ МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМАХ IoT

А. Г. Вовик

Московский технический университет связи и информатики

Решение проблемы управления информационной безопасностью в IoT-системах на сегодняшний день является важнейшим условием обеспечения информационной безопасности и поддержания требуемого уровня защищенности информации в информационных системах. При этом возможности управления информационной безопасностью ограничены отсутствием общепринятых численных метрик, основных составляющих процесса. Для обеспечения возможности получения численной оценки разработана комплексная математическая модель процесса управления информационной безопасностью в системах IoT, объединяющая методы: нечеткого моделирования, аналитические, структуризации и экспертных оценок.

управление информационной безопасностью, математическое моделирование, численная оценка защищенности информации, система Интернета Вещей.

Введение

Задача получения непрерывной оценки защищенности информационных систем в условиях стремительно развивающихся угроз и роста количества инцидентов ИБ является крайне важной для обеспечения национальных интересов Российской Федерации [1], [2].

Возможность непрерывного мониторинга уровня защищенности информации является одной из функций системы управления информационной безопасностью (УИБ).

Основные вопросы содержания понятия «управление информационной безопасностью» изложены в серии стандартов ГОСТ Р 2700х [3]. Вопросы оценки защищенности информации отражены в «Методике оценки угроз безопасности информации» [4]. В приведенных документах показатель защищенности информации в системе определен как «риск информационной безопасности». Как видно из рис. 1, предлагаемый государственными стандартами подход предполагает количественную оценку риска, проверку допустимости такого уровня риска, но не регламентирует ни критерии оценки, ни единицы измерения.

Важно отметить, что при организации процесса управления информационной безопасностью ИС, в соответствии с нормативными документами, не учитываются особенности относительно новых типов ИС, таких как системы Интернет вещей, киберфизические системы и др.

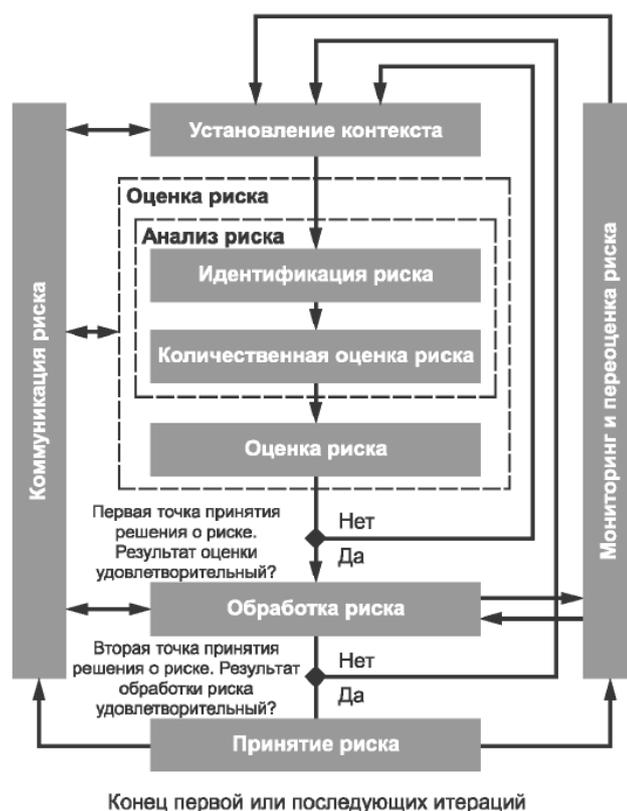


Рис.1. Процесс менеджмента риска ИБ [3]

Релевантные работы

Вопросам управления ИБ IoT-систем посвящено большое количество научно-исследовательских работ. В статье [5] проведен анализ подхода к аналитической оценке безопасности на основе формата CVSS. В результате, выявлены недостатки, оказывающие существенно-негативное влияние на оценку защищенности и возможность такой оценки.

Работы [6], [7], [8] посвящены попыткам получения численной оценки защищенности информации методами машинного обучения. Общая проблема такого подхода заключается в технической сложности получения репрезентативных выборок для обучения моделей.

Несмотря на большое количество отечественных и зарубежных работ, посвященных оценке защищенности информации, сегодня не существует общепринятого подхода, объединяющего оценку показателей защищенности, оценку уровня угроз и оценку возможностей СЗИ [9].

Подход к моделированию процесса управления информационной безопасностью

В основе предлагаемого подхода [10] к моделированию лежит аналогия с моделью управления с обратной связью из теории автоматического управления, показанная на рис. 2.

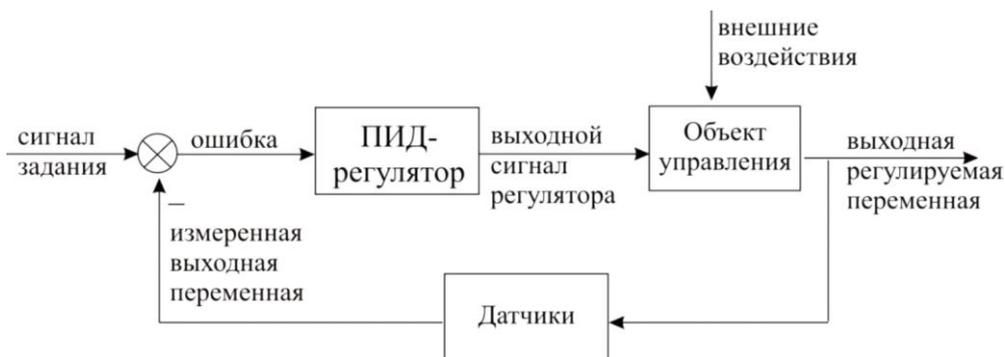


Рис. 2. Модель управления с обратной связью [11]

Интерпретация этой модели для процесса управления информационной безопасностью показана на рис. 3.

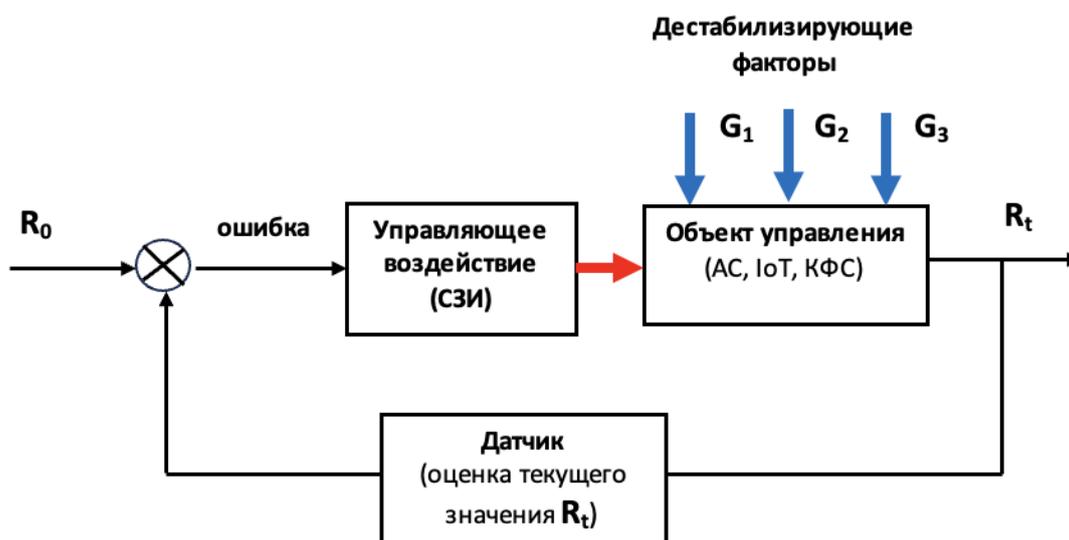


Рис. 3. Модель управления информационной безопасностью

В предложенной интерпретации:

R_t – значение показателя защищенности информации в системе;

R_0 – требуемое значение показателя уровня защищенности информации в системе;

G_1 – уровень актуальных угроз в защищаемой системе;

G_2 – изменения в структуре защищаемой системы в соответствии с потребностями бизнеса;

G_3 – изменения в политике безопасности организации;

СЗИ – конкретная конфигурация системы защиты информации, рассматриваемая в модели в качестве управляющего воздействия.

Объектом управления является информационная система, которая может быть как АС, IoT-система или киберфизическая система.

При условиях что конфигурация защищаемой системы и политики безопасности организации не изменяются, модель имеет вид, показанный на рис. 4.

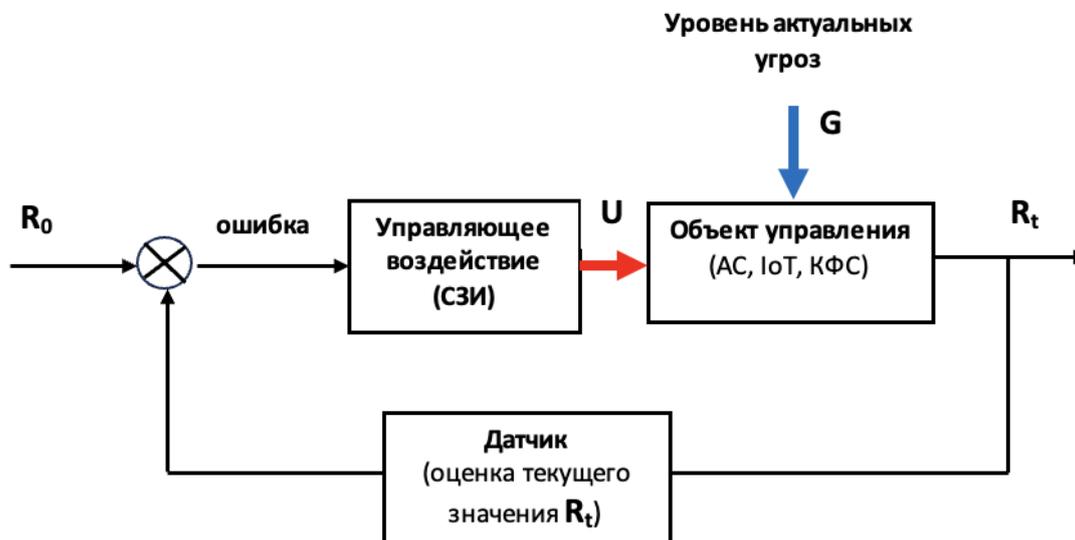


Рис. 4. Модель процесса управления информационной безопасностью для относительно стабильного периода

В таком случае единственным действующим воздействием остается уровень актуальных угроз в защищаемой системе.

При этом, основная проблема предложенного подхода заключается в невозможности измерения переменных модели, поскольку они являются качественными величинами, для которых не определены физическая величина, единицы измерения и инструмент измерения.

В результате преобразования, модель управления сведена к оптимизационной модели, представленной на рис. 5.

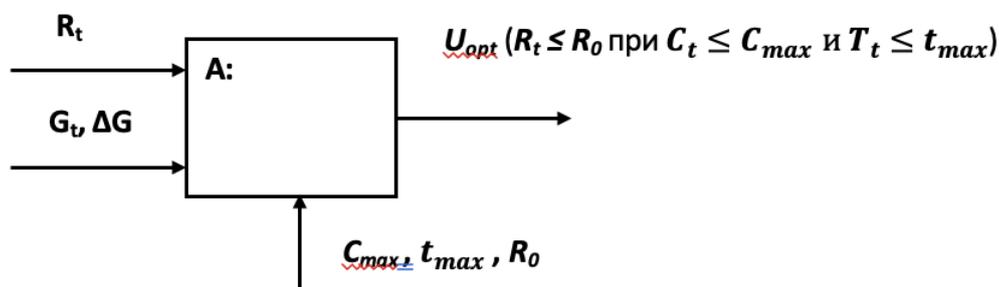


Рис. 5. Оптимизационная модель управления информационной безопасностью

В качестве входных переменных рассматривается текущий уровень защищенности информации в системе и изменение уровня угроз, а в качестве

выходной переменной определено управляющее воздействие, эквивалентное конфигурации СЗИ.

При этом наложены ограничения на выходную переменную в виде допустимой стоимости реализации контрмеры и времени на переход к новой конфигурации СЗИ.

Комплексная математическая модель процесса управления информационной безопасностью в системах IoT

На рис. 6 представлена структура модели процесса управления информационной безопасностью в системах IoT.

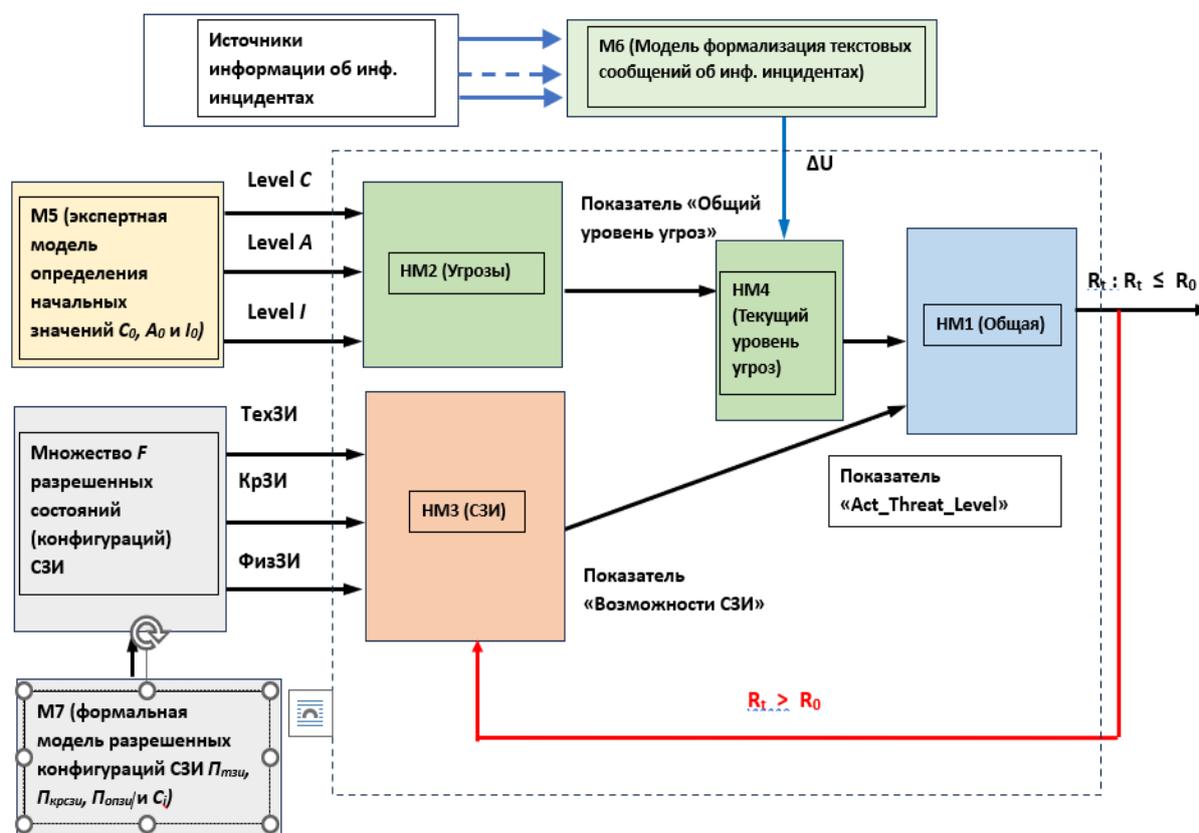


Рис. 6. Структура комплексной модели процесса управления информационной безопасностью в системах IoT

Модель управления состоит из следующих блоков:

- ядром является совокупность нечетких моделей **HM1-HM4**, общей выходной переменной для которых является уровень защищенности информации в системе Интернета вещей;
- для определения начальных значений уровня угроз целостности доступности и конфиденциальности используется **экспертная модель M5** на базе метода экспертных оценок и процедур типа дельфи;

• для получения информации о появлении новых актуальных угроз используется модель **М6 формализации текстовых сообщений об инф. инцидентах** из различных источников;

• **М7** представляет собой **формальную модель возможных конфигураций СЗИ**.

Результаты моделирования нечетких моделей НМ1 и НМ2 представлены в работах [10], [12].

Модель **НМ3** предназначена для оценки показателей возможности технических, криптографических и физических СЗИ.

Модель **НМ4** предназначена для корректировки уровня актуальных угроз с учетом информации об инцидентах ИБ из различных источников.

Заключение

В результате проведенного исследования предложен подход к формальному моделированию процесса управления информационной безопасностью в системах, использующих технологии Интернета вещей и разработанная комплексная модель, имеющая нечеткое ядро.

Разработанная модель позволяет численно оценивать уровень защищенности информации в защищаемой системе IoT, с учетом постоянного изменения уровня актуальных угроз ИБ и обеспечивать соответствие текущего уровня защищенности требуемому уровню путем изменения конфигурации системы защиты информации.

Реализация предложенной модели в виде методики управления информационной безопасностью в конкретной информационной системе IoT очевидно повысит эффективность управления по критерию оперативности и непрерывности управления по времени.

Дальнейшее развитие предложенного подхода позволит синтезировать автоматизированные, а, в перспективе, и автоматические системы управления информационной безопасностью систем Интернета вещей.

Список используемых источников

1. Дойникова Е. В., Федорченко А. В., Котенко И. В., Новикова Е. С. Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021. № 1 (41).

2. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29.03.2019 г. № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации»

3. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». М.: Стандартинформ, 2011.

4. Методический документ «Методика оценки угроз безопасности информации». Утвержден ФСТЭК России 5 февраля 2021 г.

5. Doynikova E., Chechulin A., Kotenko I. Analytical attack modeling and security assessment based on the common vulnerability scoring system, 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia. 2017. PP. 53–61, DOI: 10.23919/FRUCT.2017.8071292
6. Соломатин А. К. Исследование эффективности применения алгоритмов машинного обучения для анализа защищённости автоматизированных систем // Молодежь и наука – 2021. 2021. С. 74–82.
7. Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // Системная инженерия и информационные технологии. 2023. Т. 5. №. 4(13). С. 50–76.
8. Маликов А. В., Авраменко В. С., Саенко И. Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. 2019. №. 6(103). С. 32–42.
9. Федорченко Е. В., Новикова Е. С., Котенко И. В. и др. Система измерения защищенности информации и персональных данных для устройств интернета вещей // Вопросы кибербезопасности. 2022. № 5(51). С. 28–46. DOI: 10.21681/2311-3456-2022-5-28-46. EDN: МКАНHS
10. Вовик А. Г. О возможности численных метрик в управлении информационной безопасностью / А. Г. Вовик, А. И. Ларин // Научные исследования в космических исследованиях Земли. 2022. Т. 14. № 6. С. 12–19. DOI: 10.36724/2409-5419-2022-14-6-12-19. EDN BRHJMS
11. Веремей Е. И. Линейные системы с обратной связью. СПб.: Лань, 2013. Т. 448.
12. Вовик А. Г. Подход к формализации оценки угроз информационной безопасности методом нечеткого моделирования / А. Г. Вовик, А. И. Ларин // Научные исследования в космических исследованиях Земли. 2023. Т. 15. № 3. С. 30–37. DOI: 10.36724/2409-5419-2023-15-3-30-37. EDN LBUTQJ

Статья представлена научным руководителем, доцентом кафедры «Интеллектуальные системы в управлении и автоматизации» МТУСИ, кандидатом технических наук, А. И. Лариным.

УДК 004.89
ГРНТИ 28.23.37

РАСШИРЕНИЕ ОБУЧАЮЩЕГО НАБОРА СИНТЕТИЧЕСКИМИ ДАННЫМИ ПРИ ПОДСТРОЙКЕ ВЕСОВ МОДЕЛЕЙ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ

Д. В. Волошинов, Г. А. Урванцев, К. Т. Шарипова

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

В настоящей статье исследуется потенциал расширения обучающего набора с использованием синтетических данных при подстройке весов моделей генерации изображений. Описаны методы создания синтетических данных и изучена возможность их эффективного использования. Приведён анализ результатов экспериментов, предложены практические подходы к их интеграции, а также предложены перспективы дальнейших исследований в области подстройки весов моделей генерации изображений.

современные технологии, нейронные сети, машинное обучение, генерация изображений, Stable Diffusion, графический контент, алгоритмы подстройки весов, LoRA, этническое разнообразие

Современные технологии глубокого обучения значительно расширили возможности синтеза изображений, предоставляя новые инструменты для создания высококачественных визуальных материалов. Примеры таких инструментов – MidJourney, DALL-E [1], Kandinsky, Шедеврум и Stable Diffusion.

Stable Diffusion – модель глубокого обучения, создающая изображения по текстовой подсказке [2]. Она имеет открытый исходный код, позволяющий расширять функционал инструмента, чем активно занимается обширное сообщество пользователей. Кроме того, возможно производить тонкую подстройку весов модели (Finetuning) для получения более устойчивых результатов, стилизации или генерации ранее неизвестных объектов реального мира – концептов, в том числе людей.

Технология LoRA (Low-Rank Adaptation) – один из алгоритмов тонкой подстройки весов [3]. Он предоставляет хороший баланс между размером файла модели и качеством обучения. Более того, LoRA воздействует на наиболее важные веса модели, что повышает ее эффективность и качество результатов. Используя эту технологию, можно воссоздать изображения реально существующих людей или объектов, которые не были включены в обучающий набор модели генерации изображений.

Использование технологии LoRA для Stable Diffusion представляет огромный потенциал для создания персонализированных фотографий, иллюстраций, визуального контента для маркетинга и рекламы. Более того,

использование генеративного контента уменьшает количество ручной работы и открывает перспективы для автоматизации процессов создания контента в различных сферах деятельности. Кроме того, системные требования подобных инструментов на уровне средних персональных компьютеров, что позволяет использовать эту технологию в бизнес-среде или потребительском секторе, тем самым закрывая потребность в качественном и недорогом в производстве контенте [4].

Ранее было выявлено, что данный метод подстройки весов позволяет с высокой точностью воссоздать образ человека с сохранением черт лица [5]. Однако, в контексте этнически сложных черт лица использование обучающего набора, состоящего из реальных фотографий объекта, может не обеспечить достаточной точности воспроизведения (рис. 1) [6].



Рис. 1. а) Обучающий набор изображений для алгоритма LoRA,
б) Синтез изображений с использованием полученной LoRA

В связи с этим, предложен новый подход к использованию технологии LoRA, использовать в качестве обучающего набора синтезированные изображения исходного объекта, а не реальные фотографии. Для создания изображений будет использоваться Stable Diffusion и ряд дополнительных методов повышения качества выходных изображений. На рис. 2 представлена схема алгоритма подстройки весов методом LoRA с учетом предложенных изменений. Для синтеза фотографий человека, схожего с исходным объектом, будет использоваться модель LoRA, обученная на фотографиях объекта. Генерация изображений производится в разрешении 1024 на 1024 пикселя, вместо стандартных 512 на 512 пикселей.

Для предотвращения возникновения артефактов, таких как искаженные пальцы или появление двух или более лиц на изображении, применяется технология Kohya HiRes Fix [7]. Этот метод изменяет порядок генерации изображения – масштабируется шум, созданный в базовом разрешении модели вместо создания шума нестандартного разрешения, такой подход обеспечивает генерацию реалистичных изображений без артефактов.

Дополнительно производится обработка лиц на полученных изображениях. Для повышения точности детализации применяется расширение Adetailer [8], которое автоматически создает маску необходимых областей изображения и проводит генерацию только внутри этой маски. В данном контексте создается маска лица, в пределах которой осуществляется повторная генерация изображения.

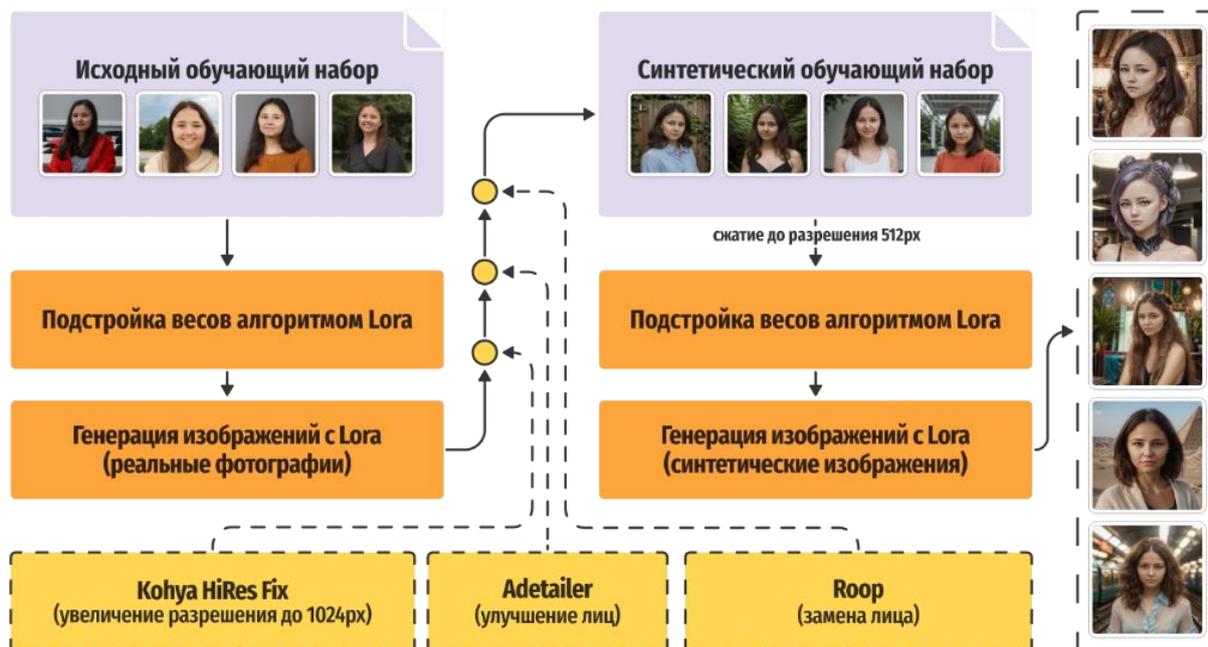


Рис. 2. Новый алгоритм обучения модели по алгоритму LoRA

К полученным изображениям применяется технология Roop [9], позволяющая заменить лицо человека на изображениях. Для формирования модели Roop используются реальные фотографии из исходного набора для обучения LoRA. Это способствует увеличению сходства сгенерированных изображений людей с исходным объектом.

Для обеспечения оптимального качества обучения LoRA необходимо использовать изображения такого разрешения, которое использовалось при обучении модели Stable Diffusion, поэтому синтезированные изображения сжимаются до 512 на 512 пикселей.

Последовательность синтеза изображений данным методом представлена на рис. 3. Синтезированы 200 изображений объекта в различных образах и контекстах, после чего выбраны 30 наиболее качественных, которые лучше всего сохранили черты исходного объекта. Полученные изображения использованы для обучения новой модели LoRA.



Рис. 3. Процесс синтеза изображения для обучающего набора

Модель LoRA, обученная на новом наборе изображений, демонстрирует возможность синтезировать исходный объект с гораздо большей точностью (рис. 4). Важно отметить, что длина текстовой подсказки, необходимой для получения приемлемого результата, значительно сократилась. Это позволит повысить вариативность генерируемых изображений, так как длина текстовой подсказки при генерации ограничена.

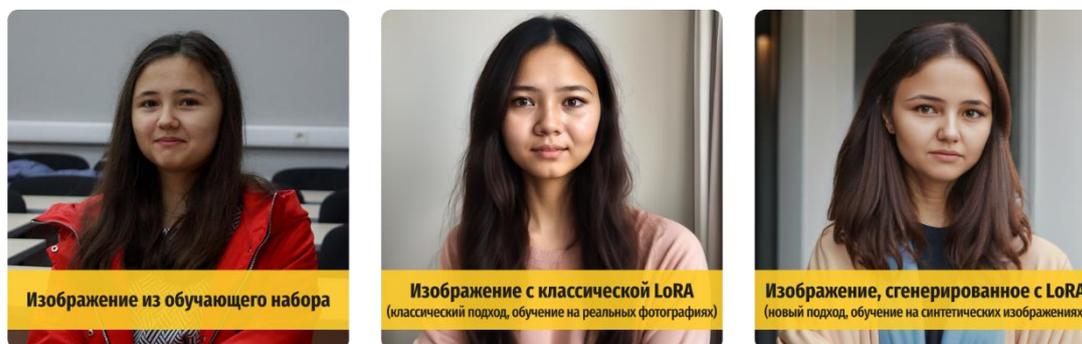


Рис. 4. Сравнение изображений сгенерированных с LoRA обученных на настоящих и синтетических данных

Использование синтетических данных в качестве обучающего набора для технологии LoRA позволяет лучше передать черты лица исходного объекта, по сравнению со стандартным алгоритмом обучения на фотографиях объекта. Однако, часть генерируемых изображений все еще содержат искаженные черты лица или неверное представление телосложения объекта. Примеры генерации представлены на рис.5. Для дальнейшего повышения качества обучения требуется более тщательно выбирать изображения, формирующие синтетический набор обучающих данных.



Рис. 5. Примеры генераций с новой версией LoRA

В дальнейших исследованиях возможно внедрение технологий предсказания пользовательской оценки для отбора качественных синтезированных изображений и технологий распознавания лиц для выбора изображений

с наибольшим сходством с исходным объектом. Эти технологии могут значительно сократить время формирования обучающего набора и в перспективе сделать его автоматическим.

Кроме того, при использовании этих технологий можно получить количественные оценки качества изображений и степени сходства с исходным объектом. Это позволит подтвердить состоятельность использования синтетических данных в обучающем наборе и оценить эффективность разработанных методов.

Список используемых источников

1. Jordan N. A.I. software called DALL-E turns your words into pictures // Официальный сайт CNBC URL: <https://www.cnbc.com/2022/06/18/ai-software-called-dall-e-turns-your-words-into-pictures> (дата обращения: 14.03.2024)
2. Rombach R., Blattmann A., Lorenz D., Esser P., Ommer B. High-Resolution Image Synthesis with Latent Diffusion Models // arXiv.org, 2021. Дата обновления: 13.04.2022. URL: <https://arxiv.org/abs/2112.10752> (дата обращения: 14.03.2024)
3. Gu Y., Wang X. Mix-of-Show: Decentralized Low-Rank Adaptation for Multi-Concept Customization of Diffusion Models // arXiv.org, 2023. Дата обновления: 10.11.2023. URL: <https://arxiv.org/abs/2305.18292> (дата обращения: 14.03.2024)
4. Пастревич Д. Роль визуального контента в развитии бренда // Бизнес и дизайн ревю. 2022. № 4 (28). С. 72–78.
5. Волошинов Д., Урванцев Г. Анализ перспектив применения изображений, сгенерированных посредством нейросети Stable Diffusion при формировании личного бренда // Материалы конференции ПКМ. 2022. С. 1192–1196
6. Волошинов Д., Урванцев Г. Проблемы воспроизводимости этнически сложных концептов при подстройке весов модели диффузионной нейронной сети Stable Diffusion // Сборник лучших докладов ПКМ. 2023. Т. 2. С. 394–399.
7. Официальный репозиторий Kohya Hires Fix // github.com. URL: <https://github.com/wcde/sd-webui-kohya-hiresfix> (дата обращения: 11.02.2024)
8. Официальный репозиторий Adetailer // github.com. URL: <https://github.com/Bing-su/adetailer> (дата обращения: 11.02.2024)
9. Официальный репозиторий Roop // github.com. URL: <https://github.com/s0md3v/roop> (дата обращения: 11.02.2024)

УДК 627.512
ГРНТИ 38.47.51

АЛГОРИТМИЧЕСКИЕ И ПРОГРАММНЫЕ РЕШЕНИЯ ПРОГНОЗИРОВАНИЯ ЗОН ЗАТОПЛЕНИЯ МЕСТНОСТИ

П. А. Волынкин

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

В эпоху активизации как природных, так и техногенных кризисов особо актуальной становится задача прогнозирования зон затопления местностей. В связи с этим ставится задача машинного моделирования процесса затопления с учетом множества факторов. В статье рассматриваются алгоритмические и программные решения прогнозирования зон затопления местности с учетом особенностей рельефа местности.

затопление, рельеф, моделирование, прогнозирование

В настоящее время активизируются кризисные процессы, связанные с затоплением земной поверхности. К причинам подобного рода ситуаций следует отнести как естественно-природные (весенние половодья, последствия ливневых осадков и т.п. [1]), так и техногенные [2], к числу которых можно отнести прорывы плотин и защитных сооружений водоемов, водохранилищ.

В связи с этим ставится несколько родов задач:

Задача № 1: Расчет зоны затопления при паводке или дождевых осадках. Для этой задачи исходными данными для моделирования становятся: скорость и время поступления воды, рельеф местности в районе затопления, характер почв в районе затопления, температура и влажность атмосферы.

Задача № 2: Расчет зоны затопления при точечном прорыве водохранилища. Для данной задачи исходными данными являются: объем или скорость и время поступления воды, рельеф местности в районе затопления, характер почв в районе затопления, температура, влажность атмосферы.

Задача № 3: Расчет зоны затопления при прорыве водохранилища и известных уровнях воды в точках местности. Исходными данными для третьей задачи становятся: объем и глубина водохранилища перед плотиной, ширина разрушенного участка, расстояние от плотины до объекта, уровень воды в районе объекта, рельеф местности в районе затопления, характер почв в районе затопления.

Во всех трех задачах требуется определить как высоту уровня воды в каждой точке участка затопления, так и построить зону затопления.

В данной статье рассмотрено решение второй и третьей задач, как наиболее сложных.

Алгоритм решения задачи № 2:

– Задание точки прорыва

- Задание начального радиуса области затопления
- Численный расчет высоты цилиндра (уровень воды) заданного объема воды. Нижняя часть цилиндра – рельеф.
- Если высота цилиндра выше любой точки на внешней границе цилиндра, то увеличение радиуса цилиндра
- Завершение процесса, когда уровень воды сравняется с высотой самой низкой точки рельефа по периметру цилиндра.

Для реализации данного алгоритма были выбраны следующие средства разработки и ресурсы:

1. Средства разработки плагинов и модулей:
 - Среда разработки: QT Creator
 - Язык программирования: C++
2. Средства разработки виджетов: QML (на основе JavaScript)

Типы карт-слоев:

- Подложка (world.mbtiles)
- Карта с рельефом (*.tif, *.mtw)

Пример работы программы для задачи № 2 представлен на рис. 1.

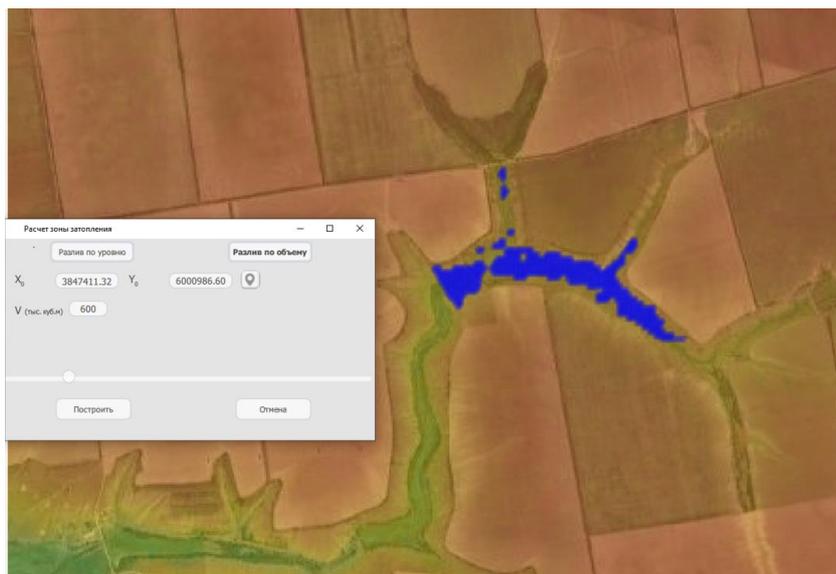


Рис. 1. Прогнозирование зоны затопления для задачи № 2

Алгоритм решения задачи № 3:

- Задание координат начальной (1) и конечной (2) точек движения потока затопления от более высокой точки к более низкой.
- Задание относительной высоты затопления в точках 1 и 2.
- Построение трассы (разбиением на дискретные элементы) между точками 1 и 2
- Цикл по элементам трассы сверху вниз.
- На каждой итерации (уровне трассы) построение ортогонали (перпендикуляра) к трассе.

– На начальной ортогонали поиск (итерации) участков рельефа, связанных по уровню затопления с затопленным элементом трассы и между собой (почва пока считается непроницаемой). Поиск останавливается на элементе ортогонали с высотой рельефа выше уровня затопления.

– На последующих ортогоналях поиск затопленных элементов ортогонали проводится не только от элемента трассы, но и от затопленных элементов предыдущей (более высокой) ортогонали.

На рис. 2 приведена иллюстрация вышеописанного алгоритма:

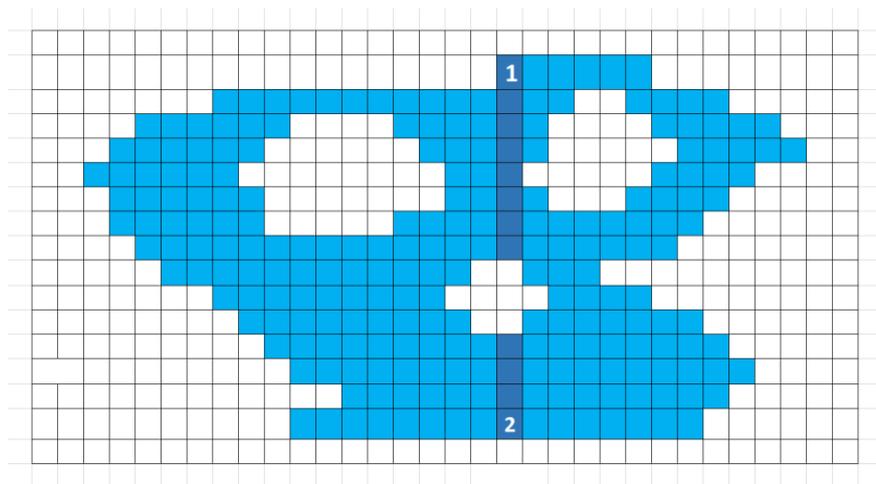


Рис. 2. Пример иллюстрации алгоритма для задачи № 3

Пример реализации вышеописанного алгоритма решения задачи №3 представлен на рис.3, где синим цветом отображена зона затопления.

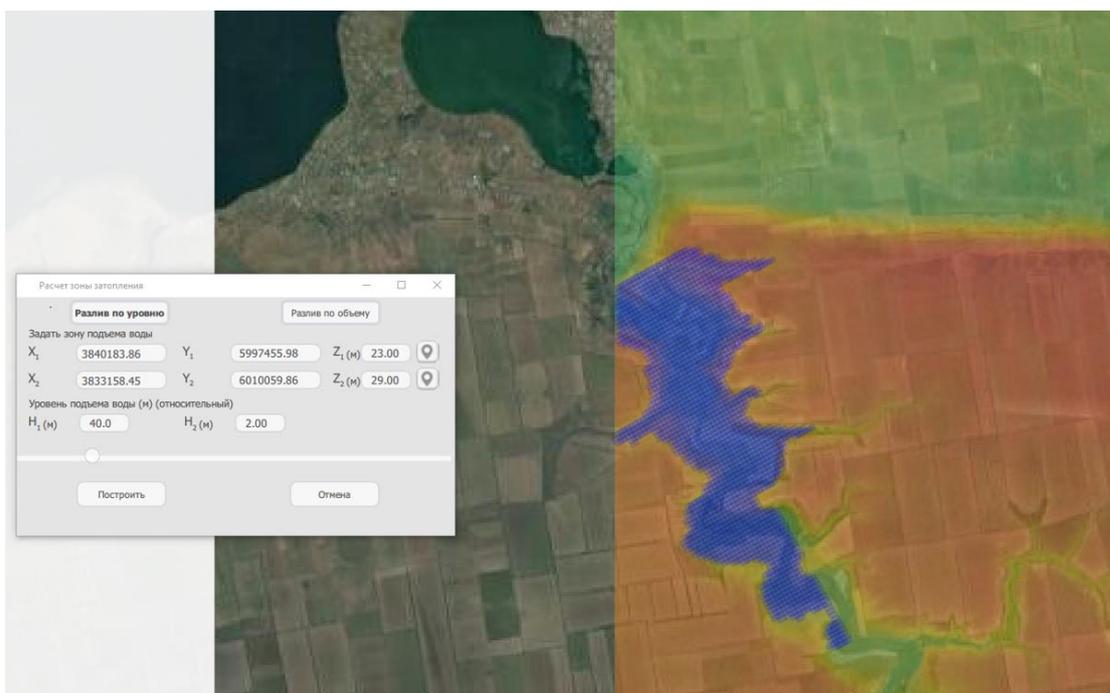


Рис. 3. Прогнозирование зоны разлива для задачи № 3

На данном этапе работ при прогнозировании зон разлива не учитывались почвенные и атмосферные факторы. Учет этих факторов запланирован на ближайших этапах работы над поставленными задачами.

Список используемых источников

1. Баринов А. В., Седнев В. А., Шевчук А. Б., Харисов Г. Х., Кошечая Е. И. Опасные природные процессы. М.: Академия Государственной противопожарной службы, 2009.
2. Векслер А. Б., Ивашинов Д. А., Стефанишин Д. В. Надежность, социальная и экологическая безопасность гидротехнических объектов: оценка риска и принятие решений. СПб.: Изд-во ОАО «ВНИИГ им. Б.Е. Веденеева», 2002. 591 с.

УДК 004.056.6
ГРНТИ 50.41.25

АНАЛИЗ ИЗМЕНЕНИЯ ПАРАМЕТРОВ ВИДЕОКОНТЕЙНЕРОВ ПОСЛЕ ВЛОЖЕНИЯ СТЕГОСООБЩЕНИЯ

П. А. Волынкин, М. К. Гильманова

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

*В эпоху активного развития информационных технологий передача и просмотр данных в видеоформате становится одним из самых распространенных видов трафика. Это делает их удобным вариантом для использования в качестве контейнера для стегосообщения. Полностью скрыть наличие внедренного сообщения нельзя, однако существует возможность минимизировать его заметность. Это достигается путем минимизации изменений размера файла. Для автоматизации внедрения стегосообщения в видеоконтейнер была использована программа *Masker 7.5*, а также приведены результаты внедрения для различных форматов файлов.*

*стеганография, видео, контейнер, *.avi, *.mov, *.mpg*

В настоящее время пользователи Интернета постоянно обмениваются друг с другом видеороликами. Поэтому маскировка стегосообщения в видеоконтейнер становится одним из самых простых способов скрытно передать сообщение. Чтобы обезопасить себя от получения вредоносных файлов, надо осторожно относиться к получаемому контенту. В данной статье рассмотрен один из общедоступных способов передать скрытое сообщение.

Примером программного обеспечения для внедрения сообщения в контейнер является Masker 7.5. Программа является условно бесплатной, предлагая десятидневный пробный период. Masker 7.5 предлагает все необходимые функции для внедрения и извлечения стегосообщения. В программе доступно 7 алгоритмов шифрования. В качестве контейнеров для внедрения скрытых сообщений Masker поддерживает большое разнообразие форматов, возможно использование изображений, и звуков, и видео.

В ходе изучения видов видеоконтейнеров был проведен эксперимент по внедрению двух файлов различных форматов и размеров. Были созданы два файла: «Стегосообщение.txt» размером 100 байт и «Другое Стегосообщение.docx» размером 11 КБ (рис. 1).

Для шифрования сообщений был выбран алгоритм BlowFish [1]. Это алгоритм 64-битного блочного шифра с ключом переменной длины. Был разработан известным специалистом в области криптографии и защиты информации Брюсом Шнайером в 1993 году [2].

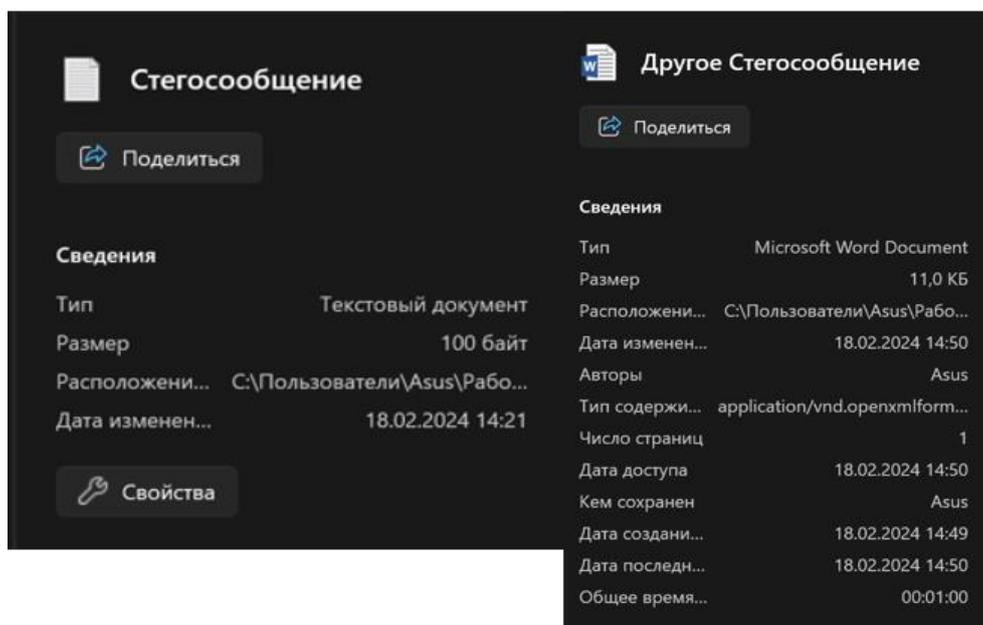


Рис. 1. Сведения о стегосообщениях

Для внедрения стегосообщений [3] были созданы 3 видеоконтейнера, представляющие собой один и тот же видеоролик, сохранённый в форматах .avi, .mov и .mpg.

Первым рассматриваемым контейнером является видеоролик в формате .avi. После внедрения в него стегосообщений при помощи программы Masker 7.5 (рис. 2) размер видеофайла увеличился на 13 КБ, что превышает сумму размеров стегосообщений на 10 %.

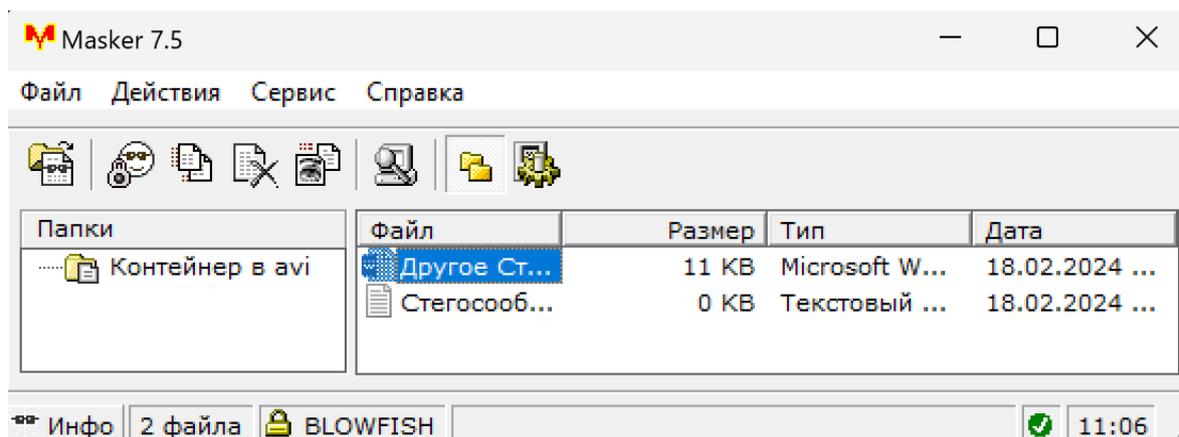


Рис. 2. Вид в Masker 7.5

При внедрении стегосообщений больших размеров это может существенно повлиять на изменение объема контейнера. Визуально видео не изменилось, кроме значительного изменения размера файла, отличий не обнаружено (рис. 3).

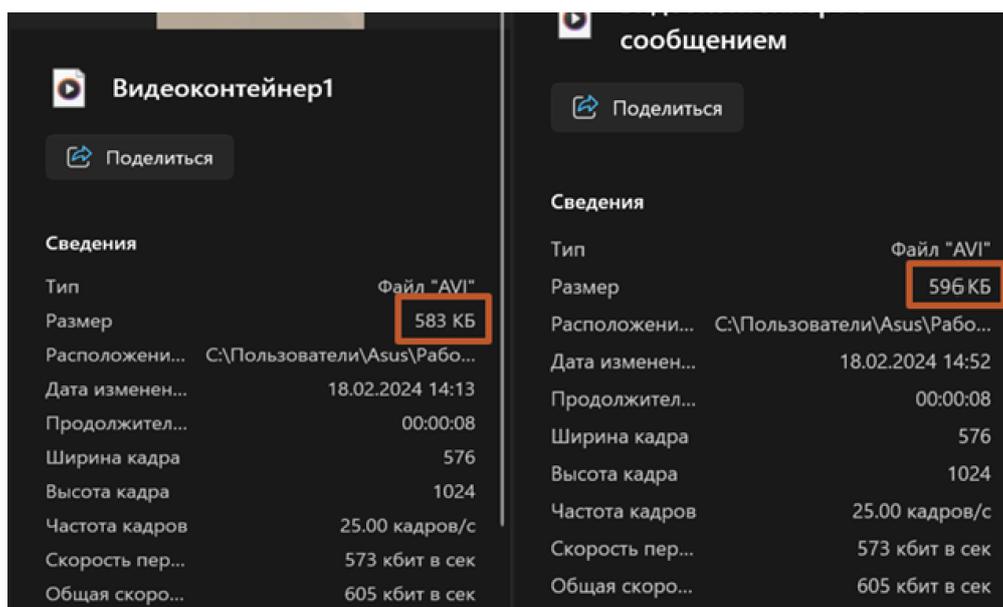


Рис. 3. Видеоконтейнер в формате .avi до и после внедрения стегосообщения

Следующим рассматриваемым контейнером является видео в формате *.mov*. После внедрения сообщения размер файла увеличился ровно на размер внедряемых стегосообщений, качество видео визуально не изменилось (рис. 4).

Последним рассматриваемым форматом видео стал *.mpg*. После внедрения сообщения размер файла увеличился ровно на размер внедряемого стегосообщения, однако значительно изменилось качество видеоролика. Скорость подачи кадров значительно увеличилась и визуально видео стали различаться (рис. 5).

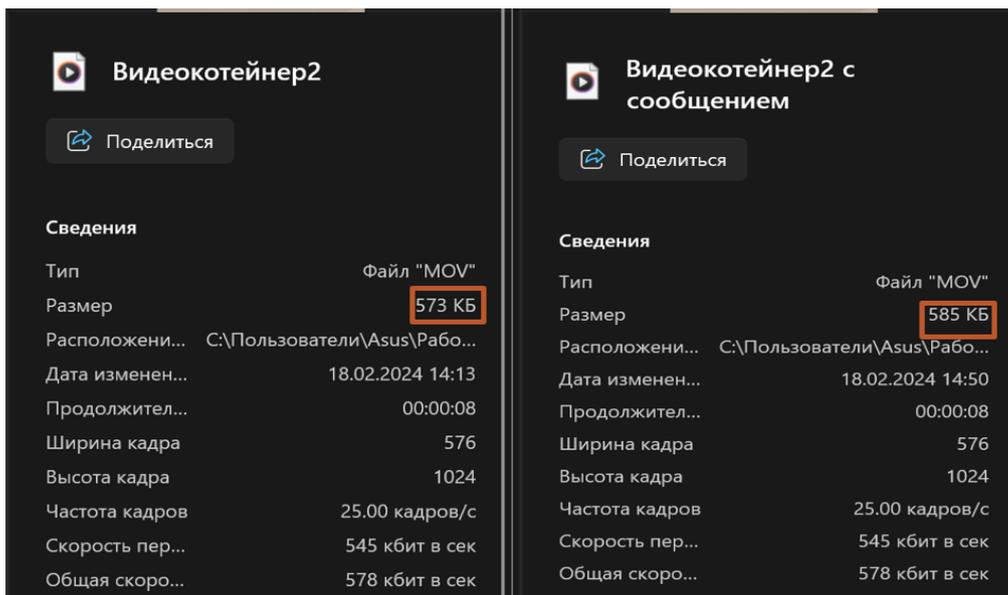


Рис. 4. Видеокотейнер в формате .mov до и после внедрения стегосообщения

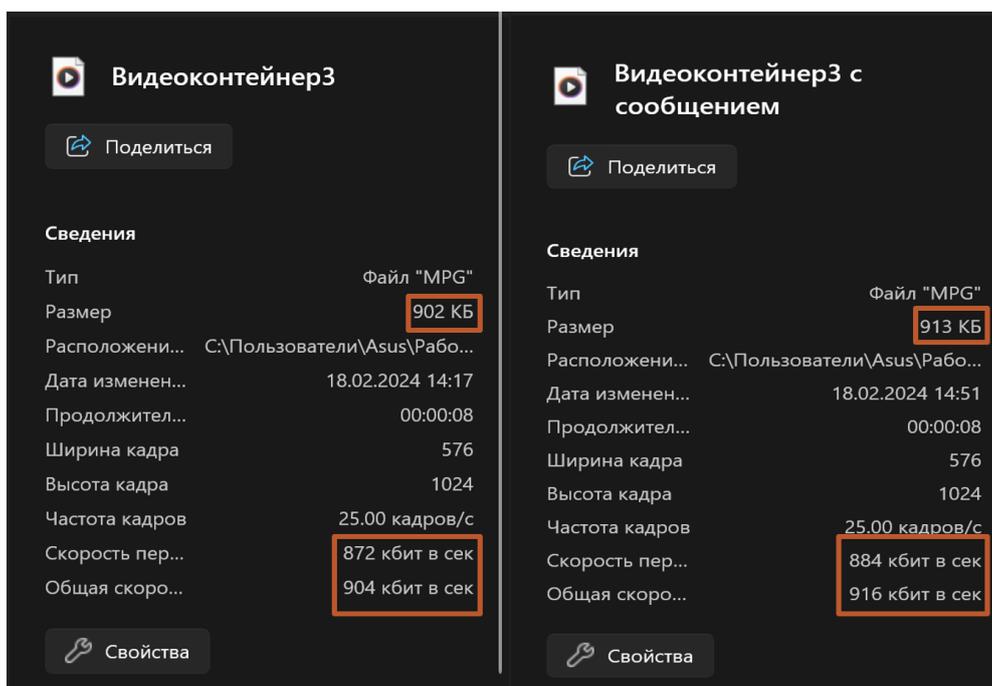


Рис. 5. Видеокотейнер в формате .mpg до и после внедрения стегосообщения

При сравнении видеоконтейнеров различных видеоформатов очевидно, что видеоконтейнер формата *.avi* сильнее изменяет размер после внедрения стегосообщения. Форматы *.mpg* и *.mov* меняют размер эквивалентно, однако *.mpg* после внедрения стегосообщения заметно изменил скорость потока кадров. При внедрении файла достаточно большого размера это существенно влияет на визуальное представление. Таким образом, с точки зрения информационной безопасности, следует обратить на это внимание и выбирать формат видео в соответствии со своими целями: *.mpg* –

при потребности обеспечить себе большую безопасность и .mov – чтобы как можно более скрытно передать сообщение.

Список используемых источников

1. Коржик В. И. и др. Цифровая стеганография и цифровые водяные знаки. 2017.
2. Habr. [сайт]. 2024. Текст электронный. <https://habr.com/ru/articles/140394/> (дата обращения: 27.02.2024)
3. Моденова О. В. Стеганография и стегоанализ в видеофайлах // Прикладная дискретная математика. Приложение. 2010. №. 3. С. 37–39.

УДК 004.384
ГРНТИ 45.01.05

СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ВЫБОР МИКРОКОНТРОЛЛЕРОВ ДЛЯ РЕАЛИЗАЦИИ ПРОГРАММНОГО МОДУЛЯ АВТОМАТИЧЕСКОЙ РЕГУЛИРОВКИ ВЫСОТЫ ПОЛЕТА БПЛА

П. А. Волынкин, В. Н. Кирсанова

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

В данной работе приведены результаты исследования различных видов микроконтроллеров, сфокусированное на выборе оптимального для разработки программного обеспечения автоматической регулировки высоты БПЛА. Проведен анализ нескольких типов микроконтроллеров, включая их технические характеристики, производительность и энергопотребление. Сравнительный анализ выявил основные преимущества и недостатки каждого типа микроконтроллера в контексте автоматической регулировки высоты полета БПЛА. На основе полученных данных сделан обоснованный выбор микроконтроллера, который наилучшим образом соответствует требованиям для разработки программного обеспечения автоматической регулировки высоты.

микроконтроллер, сравнение, программирование, БПЛА

При разработке программного модуля автоматической регулировки высоты полета беспилотного летательного аппарата (БПЛА) критическое значение имеет выбор подходящего микроконтроллера. В данном докладе будут рассмотрены несколько моделей от известных производителей микроконтроллеров и проведен сравнительный анализ их характеристик, чтобы сделать обоснованный выбор для нашего проекта.

Были выбраны модели микроконтроллеров или микроконтроллерных плат от зарубежных компаний Arduino, STMicroelectronics и Microchip. А также от российского производителя Миландр.

Рассмотрим микроконтроллеры следующих моделей:
Arduino UNO — это микроконтроллерная плата на базе микроконтроллера ATmega328P [1] (рис.1).

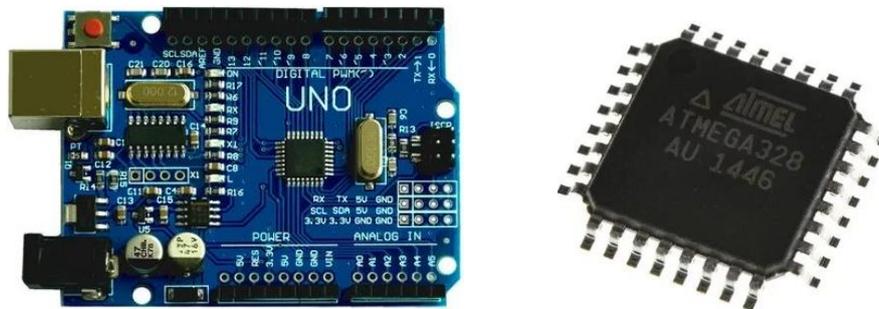


Рис. 1. Arduino Uno на базе ATmega328P

STM32F407VGT6 – 32-разрядный микроконтроллер на базе ядра Cortex-M4F с функцией DSP-вычислений, может быть установлен на плате STM32F4DISCOVERY [2] (рис. 2).



Рис. 2. Микроконтроллер STM32F407VGT6 на плате STM32F4DISCOVERY

PIC18F4550 – это 8-разрядный микроконтроллер с технологией nanoWatt и улучшенной флэш-памятью [3] (рис. 3).

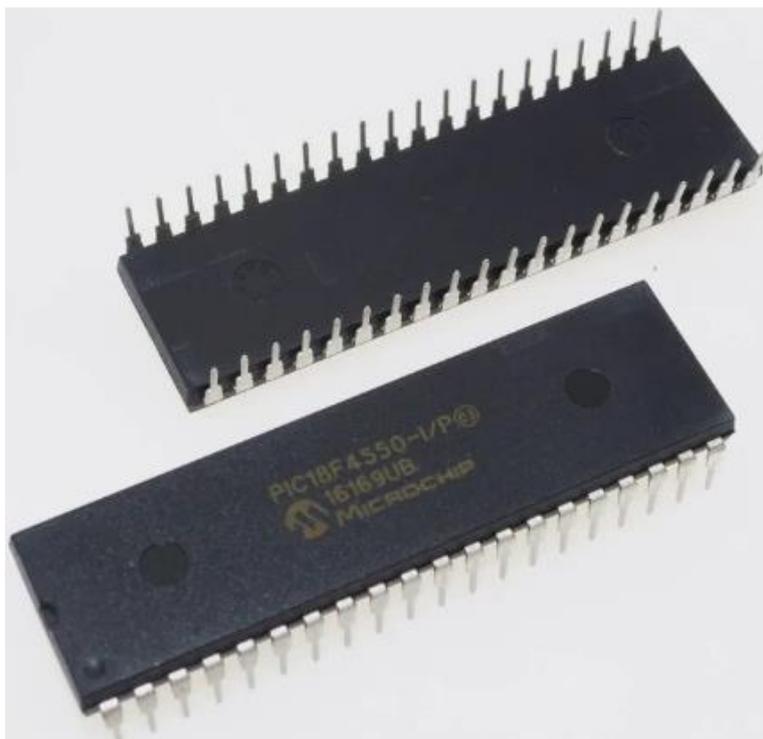


Рис. 3. Микроконтроллер PIC18F4550

K1986BE92QI – это серия 32-разрядных микроконтроллеров, построенных на ядре ARM Cortex-M3. Периферия данного микроконтроллера включает контроллер USB-интерфейса [4] (рис. 4).

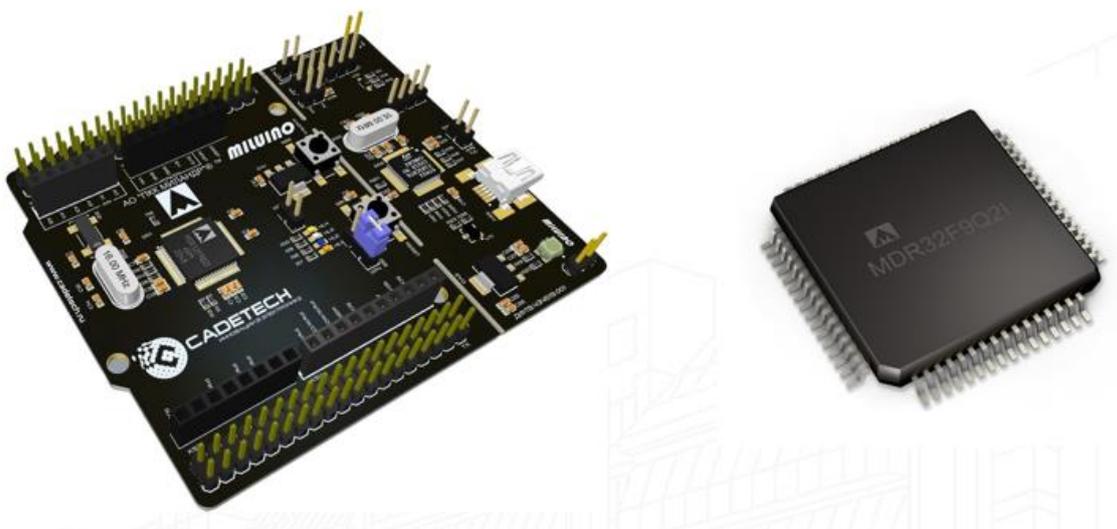


Рис. 4. Микроконтроллер K1986BE92QI

Вышеперечисленные модели обладают схожими характеристиками, которые приведены в таблице 1, однако эти характеристики являются оптимальными в рамках выполнения поставленной задачи.

ТАБЛИЦА 1. Технические характеристики микроконтроллеров

	ATmega328P	STM32F407VGT6	PIC18F4550	K1986BE92QI
Энергопотребление (в активном режиме), мА	До 50	100 - 200	100-200	100 - 120
Тактовая частота, МГц	16	До 168	До 48	80
Объем флэш-памяти	32 Кб	1 Мб	32 Кб	128 Кб
Рабочая температура, °С	От -40 до +85	От -40 до +85	от -40 до +125	От -40 до +85
Габариты платы	68.6 мм x 53.4 мм	70 мм x 41 мм	-	65 мм x 50 мм
Цена, руб	200-500	300-1000	1200-2800 (без платы)	1300 - 7000

Энергопотребление: Одним из первостепенных параметров является энергопотребление. Меньшее энергопотребление позволяет продлить время автономной работы БПЛА. В данном контексте микроконтроллеры Arduino Uno и K1986BE92QI выделяются, обеспечивая низкое энергопотребление и, следовательно, длительное время работы от батарейного питания.

Тактовая частота: чем выше тактовая частота, тем быстрее микроконтроллер способен выполнять вычисления и реагировать на изменения высоты для ее регулировки. Модель STM32F407VGT6 обладает высокой тактовой частотой до 168 МГц, что обеспечивает высокую производительность и быструю обработку данных.

Объем памяти: объем флэш-памяти важен для хранения программного кода. Микроконтроллер STM32F407VGT6 предлагает значительный объем внутренней флэш-памяти, что может быть полезно для хранения больших объемов данных и программного кода.

Диапазон рабочих температур: для работы в различных климатических условиях необходим широкий диапазон рабочих температур. В этом параметре все выбранные микроконтроллеры достаточно широко покрывают диапазон от -40°C до +85°C.

Габариты: для интеграции в корпус БПЛА важны компактные габариты микроконтроллерной платы. Микроконтроллер K1986BE92QI и STM32F407VGT6 обладают относительно небольшими размерами, обеспечивая удобство в интеграции и минимизацию размеров устройства.

Цена: цена является второстепенной характеристикой. В этом параметре самой доступной является плата Arduino.

В результате сравнительного анализа характеристик микроконтроллеров приходим к выводу, что для проекта наиболее подходящим будет микроконтроллер STM32F407VGT6. Он обладает высокой производительностью, большим объемом внутренней памяти и компактными габаритами, но уступает по энергопотреблению другим моделям.

Однако стоит отметить и модель K1986BE92QI [5]. Энергопотребление имеет достаточно большое значение в рамках выполнения задачи, так как от данного параметра зависит время работы БПЛА. В данном случае модель от компании Миландр является «золотой серединой» компенсируя недостаток тактовой частоты и памяти относительно низким энергопотреблением. Но в тоже время стоит учитывать и фактор доступности в рамках цены, в данном случае модель STM32F407VGT6 является более доступной для приобретения.

Дальнейшие планы работы включают в себя несколько этапов:

- необходимо проведение тестирования выбранного микроконтроллера для подтверждения его пригодности для конкретного проекта;
- разработка и тестирование программного модуля на выбранном микроконтроллере;
- интеграция программного модуля в реальное оборудование БПЛА и его тестирование в реальных условиях полета для уверенности в корректной работе и соответствии требованиям;
- оценка производительности и надежности программного модуля, а также его способности к адаптации к различным условиям полета;
- на основе результатов тестирования и обратной связи от пользователей будет осуществлено дальнейшее развитие и совершенствование программного модуля, включая добавление новых функций и улучшение существующих.

Список используемых источников

1. ATmega328/P // Microchip URL: <https://volfiq.ru/datasheets/ATMEGA328P.pdf> (дата обращения: 15.02.2024)
2. STM32F407VG // www.st.com URL: <https://www.st.com/en/microcontrollers-microprocessors/stm32f407vg.html> (дата обращения: 16.02.2024)
3. PIC18F2455/2550/4455/4550 Data Sheet // www.farnell.com URL: <https://www.farnell.com/datasheets/720550.pdf> (дата обращения: 16.02.2024).
4. K1986BE92QI // ic.milandr.ru URL: https://ic.milandr.ru/products/mikrokontrollery_i_protssory/32_razryadnye_mikrokontrollery/k1986ve92qi (дата обращения: 16.02.2024)
5. Переходим с STM32F103 на K1986BE92QI. Или первое знакомство с российским микроконтроллером // habr.com. URL: <https://habr.com/ru/articles/255199> (дата обращения: 17.02.2024)

УДК 004.415.23
ГРНТИ 20.53.25**ПРОЕКТИРОВАНИЕ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ
ЗАГРУЗКИ ТАЙЛОВ****П. А. Волынкин, И. А. Туманов**

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

Статья посвящена проектированию системы автоматизированной загрузки тайлов, предназначенной для актуализации электронных карт. Разработка акцентируется на создании удобного механизма обновления тайлов, что имеет важное значение для обеспечения актуальности и точности геопространственных данных. В ходе исследования также проводится сравнительный анализ существующих аналогичных систем, выявляя их сильные и слабые стороны. Описываются преимущества разрабатываемой системы в сравнении с другими решениями, предоставляя обоснование выбора конкретных решений.

автоматизированная загрузка тайлов, электронные карты, географические данные

В настоящее время электронные карты становятся все более популярными и востребованными. Однако, для обеспечения их актуальности и точности необходим механизм автоматизированной загрузки тайлов с общедоступных источников в Интернете.

Электронные карты создаются [1] путем сбора и анализа географических данных, которые затем отображаются на компьютерном экране или мобильном устройстве. Они часто организованы по принципу слоев (или уровней), где каждый слой представляет собой определенный набор данных или информации о конкретных аспектах местности (рис. 1).

Основные этапы построения электронных карт включают в себя сбор географических данных, их обработку и анализ, создание различных слоев для отображения разнообразной информации, а также рендеринг (отрисовку) карты для представления пользователю.

Тайлы [2] представляют собой небольшие изображения, которые составляют карту. Они обычно имеют квадратную форму и содержат небольшой участок местности. Чем ниже уровень, тем больше тайлов необходимо для полного покрытия области (рис. 2). Тайлы могут быть предварительно сгенерированными и храниться локально на устройстве или динамически загружаться из Интернета при необходимости, особенно при изменении масштаба карты.

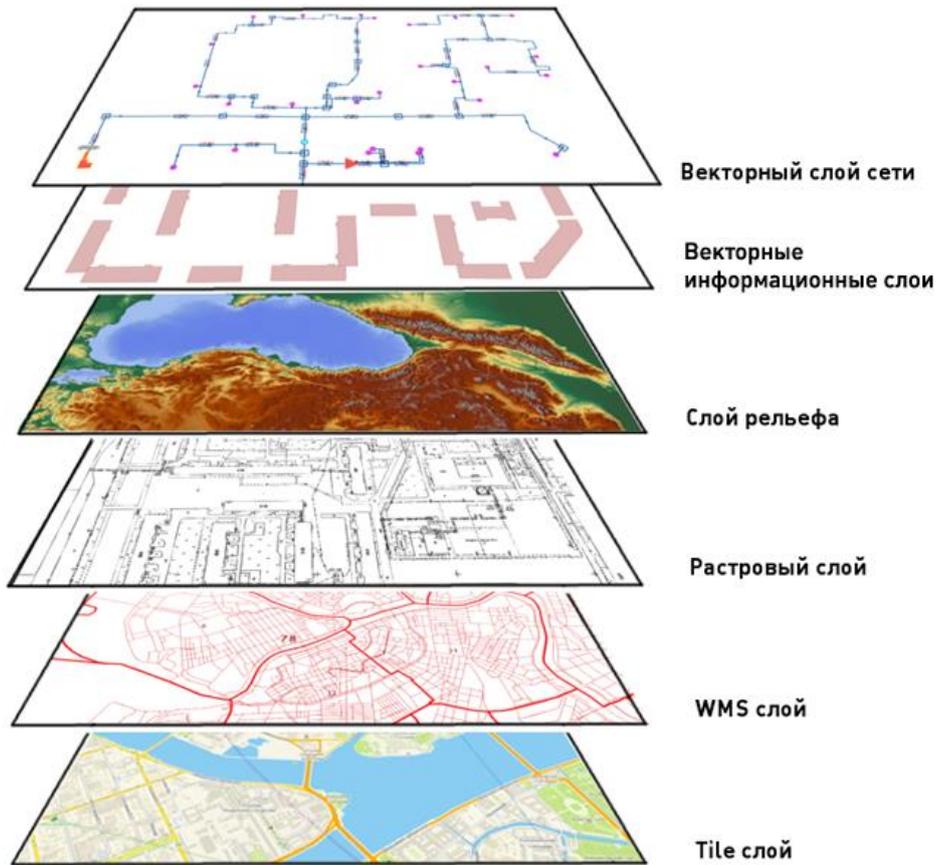


Рис. 1. Слои карты для геоинформационной системы

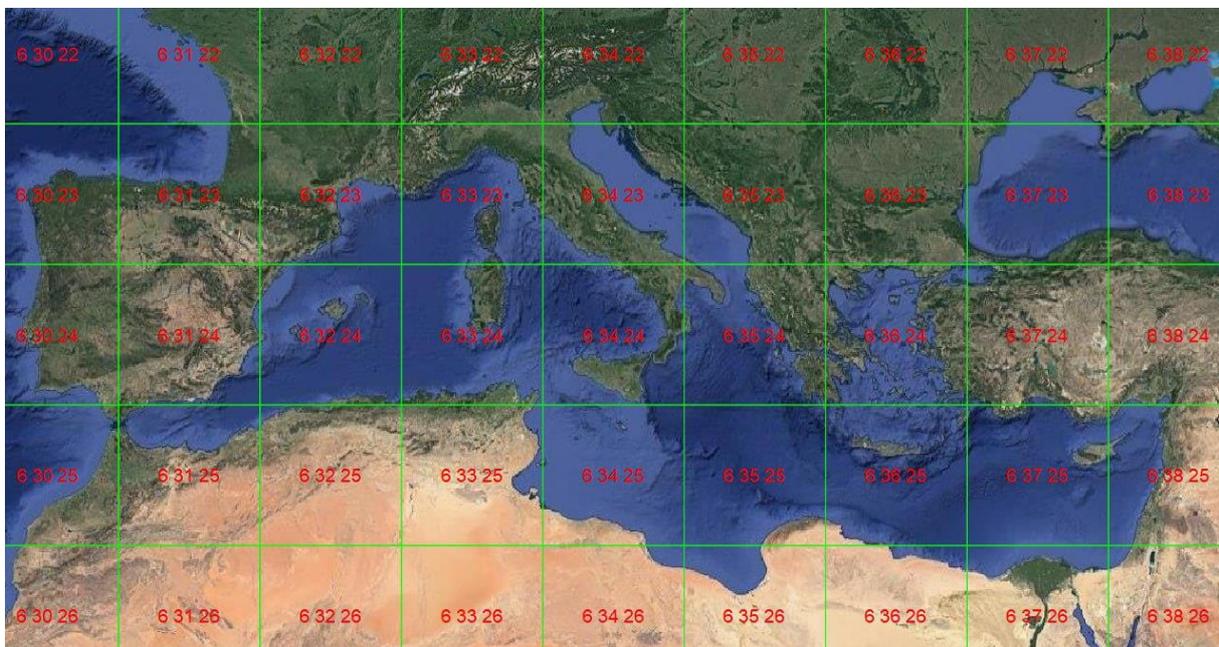


Рис. 2. Пример тайловой сетки

Каждый тайл обычно содержит информацию о конкретной части карты, включая географические объекты, текст, маршруты и другие элементы, которые отображаются на данном участке местности. Эти изображения собираются и отображаются вместе, чтобы пользователь мог просматривать и взаимодействовать с полной картой. Для облегчения сбора тайлов и проектируется данная система.

Проектируемая система представляет собой программное решение, которое будет позволять пользователям скачивать тайлы как единично, так и диапазонами, используя лишь уровень и параметры по x и по y . Она будет обладать функционалом клиент-сервер, где сервер будет выполнять ряд важных ролей: создание заданий для клиентов, выдача заданий, проверка работоспособности клиентов, а также прием загруженных изображений и их «сшивание» в единый файл формата MBTiles [3]. Формат MBTiles – это компактный способ хранения тайловых карт, где изображения тайлов сохраняются внутри единой SQLite базы данных. Этот формат обеспечивает эффективное хранение и доступ к тайлам, что делает его удобным выбором для офлайн-картографии и веб-приложений. Также будет возможен вариант без использования клиент-сервера, когда имеется только условный клиент, позволяющий пользователям скачивать тайлы самостоятельно.

Системы, предоставляющие возможность скачивания тайлов, включают такие примеры, как QGIS [4] и SASPlanet [5]. Однако отличительной особенностью этих систем является отсутствие автоматизированной возможности распределения заданий на несколько пользователей. Это означает, что задачи должны быть выполнены вручную, что может привести к человеческим ошибкам, таким как неправильное указание диапазона, потеря скачанных файлов или необходимость дополнительного объединения файлов в единый формат MBTiles. Одним из их преимуществ является возможность указания различных источников данных через ссылки на ресурсы.

В дальнейшем планируется развитие системы до степени, позволяющей проверять актуальность уже скачанных тайлов, чтобы избежать перекачивания тех, которые остались неизменными. Также планируется интеграция различных форматов хранения, таких как Bundle.

Проектируемая система представляет собой важный инструмент для обеспечения актуальности и точности электронных карт. Её автоматизированный подход к загрузке тайлов значительно упростит процесс составления карт, освободив пользователей от рутинных задач и снизив время их выполнения. Такой подход не только обеспечит удобство для пользователей, но и повысит эффективность в плане оптимизации загрузки и обработки данных, делая систему неотъемлемым инструментом для создания и поддержания электронных карт.

Список используемых источников

1. Давлетшина А. Д. Этапы и проблемы создания электронной карты // Молодой ученый. 2017. № 3(137). С. 191–193. URL: <https://moluch.ru/archive/137/38285> (дата обращения: 28.01.2024)

2. Цветков В. Я. Тайловое представление пространственной информации // Международный журнал прикладных и фундаментальных исследований. 2016. № 10-4. С. 670–671. URL: <https://applied-research.ru/ru/article/view?id=10417> (дата обращения: 21.01.2024)

3. MBTiles // mapbox URL: <https://docs.mapbox.com/help/glossary/mbtiles> (дата обращения: 19.01.2024)

4. QGIS – лучшая настольная ГИС с открытым исходным кодом // QGIS URL: <https://www.qgis.org/ru/site/about/index.html> (дата обращения: 19.01.2024)

5. GIS // SAS Planet URL: <https://sasplanet.geojamal.com/search/label/GIS> (дата обращения: 19.01.2024)

УДК 627.512
ГРНТИ 38.47.51

АЛГОРИТМ ПРОГНОЗИРОВАНИЯ ЗОНЫ РАЗЛИВА НЕФТЕПРОДУКТОВ

П. А. Волынкин, В. А. Чиняев

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

Утечки нефтепродуктов являются серьезной экологической проблемой, что требует разработки эффективных алгоритмов прогнозирования зон затоплений для предотвращения и минимизации последствий таких происшествий.

нефтепродукты, экология, алгоритмы

Существует несколько подходов к алгоритмам построения зон затопления местности.

1) Эмпирический подход, где проводится серия экспериментов, на основе полученных данных вычитывается зависимость, все оформляется в виде формул [1].

2) Теоретический подход, этот алгоритм основан на уравнениях Навье-Стокса [2] (1), которые описывают движение жидкости в пространстве и времени. При моделировании зон загрязнения алгоритм учитывает множество факторов, включая топографию местности, характеристики водотоков, препятствия на пути нефти, а также динамику изменения уровня нефти в зависимости от времени и изменений в окружающей среде.

$$\begin{cases} \frac{dvi}{dt} + vk * \frac{dvi}{dxk} = -\frac{1}{p} + V * \frac{d}{dxk} * \left(\frac{dvk}{dxk} + \frac{dvk}{dxi} \right) \\ \frac{dp}{dt} + \nabla(pv) = 0 \end{cases} \quad (1)$$

3) Использование геоинформационных систем, где подготавливаются данные (координаты мест с нефтью, ее концентрация), преобразовываются данные в матрицу и создание слоев (высоты, здания) [3]. Каждый слой с параметрами интерполируется с помощью метода обратных взвешенных расстояний (ОВР), однозначно предполагающего, что объекты, которые находятся поблизости, более подобны друг другу, чем объекты, удаленные друг от друга.

В рамках данных исследований был разработан оригинальный алгоритм компьютерного моделирования формирования зоны затопления рельефа местности при разливе нефтепродуктов.

Для данной задачи исходными данными являются: Объем или скорость и время поступления нефтепродуктов, рельеф местности в районе затопления, характер почв в районе затопления, температура, влажность атмосферы.

Алгоритм решения данной задачи можно описать следующим образом:

- Задание точки прорыва: координаты.
- Задание начального радиуса области затопления
- Численный расчет высоты цилиндра (уровень нефти) заданного объема воды. Нижняя часть цилиндра – рельеф.
- Если высота цилиндра выше любой точки на внешней границе цилиндра, то увеличение радиуса цилиндра
- Завершение процесса, когда уровень нефти сравняется с высотой самой низкой точки рельефа по периметру цилиндра.

Для реализации данного алгоритма были выбраны следующие средства разработки и ресурсы:

Средства разработки плагинов и модулей:

- Среда разработки: QT Creator
- Язык программирования: C++

Средства разработки виджетов: QML (на основе JavaScript)

Типы карт-слоев:

- Подложка (world.mbtiles)
- Карта с рельефом (*.tif, *.mtw)

Пример работы программы представлен на рис. 1.

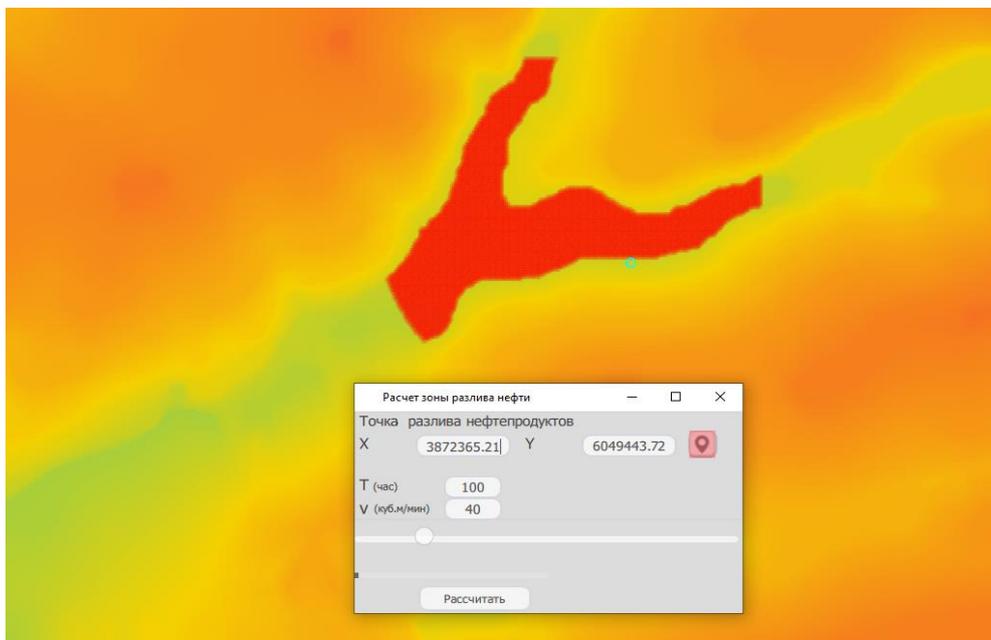


Рис. 1. Программная реализация алгоритма прогнозирования разлива нефтепродуктов

Список используемых источников

1. 4author.com. Эмпирические методы исследования. URL: <https://www.4author.com/ru/blog/story/empiricheskie-metody-isselovaniya> (дата обращения: 26.02.2024)
2. Solverbook.com. Уравнения Навье-Стокса. URL: <http://ru.solverbook.com/spravochnik/uravneniya-po-fizike/uravneniya-nave-stoksa> (дата обращения: 26.02.2024)
3. ArcGIS Resources. Введение в ArcGIS. URL: <https://resources.arcgis.com/ru/help/getting-started/articles/026n00000014000000.htm> (дата обращения: 26.02.2024)

УДК 004.9
ГРНТИ 38.47.51

АЛГОРИТМ ПОСТРОЕНИЯ ЗОН ВИДИМОСТИ ЛАНДШАФТОВ СО СЛОЖНЫМ РЕЛЬЕФОМ

П. А. Волынкин, А. А. Шумилова

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

Построение зон видимости ландшафтов со сложным рельефом необходимо для разных географических информационных систем, городского планирования, экологического мониторинга и других сфер. Алгоритмы, рассмотренные в данной работе, учитывают разные типы исходных данных. Каждый из алгоритмов имеет свои преимущества и недостатки. В зависимости от этих факторов и от ожидаемого результата, выбирается необходимый способ построения зон видимости. В результате работы некоторых алгоритмов представлены получившиеся зоны видимости.

зона видимости, построение зон видимости, алгоритм плавающего горизонта, алгоритм Z-буфера, триангуляция, двойная итерация

Создание зон видимости предоставляет создавать области на карте, которые бы показывали то, что может наблюдать человек или устройство из выбранной точки. Создание таких зон имеет большое значение в военном деле, в сельском и лесном хозяйствах, в навигации и планировании инфраструктуры городской среде.

Для подбора необходимого алгоритма стоит сначала определиться с тем, как проводить анализ пространства видимости. В основном, алгоритмы построения зон видимости различаются по анализу пространства видимости:

– в пространстве изображения (2D) – при данном методе находятся ближайшие точки сцены к наблюдателю и для каждого пикселя изображения отображаются только такие точки. Точность на уровне разрешения устройства и не требуется высокой точности вычислений.

– в пространстве объекта (3D) – идея данного алгоритма заключается в том, что происходит оперирование геометрическими примитивами и производится проверка пересечения объектов друг с другом, в результате получается список видимых объектов и их частей. Объекты из списка могут отображаться с любой точностью, но вычисления видимых частей – с высокой.

Основываясь на вышеупомянутой информации, будет рассмотрено несколько алгоритмов.

1. Алгоритм плавающего горизонта

В данном алгоритме чаще всего используется удаление невидимых линий трехмерного представления функций, которые описывают поверхность в виде $F(x, y, z) = 0$. Идея метода заключается в сведении трехмерной задачи к двумерной путем пересечения исходной поверхности последовательностью параллельных секущих плоскостей, имеющих постоянные значения координаты z [1].

Первоначально алгоритм упорядочивает плоскости, располагаемые на плоскостях $z = \text{const}$ по возрастанию расстояния до них от точки наблюдения. Затем для каждой плоскости, начиная с ближайшей к точке наблюдения, строится кривая, лежащая на ней, то есть для каждого значения координаты x в пространстве изображения определяется соответствующее значение y . Если на текущей плоскости при некотором заданном значении x соответствующее значение y на кривой больше значения y для всех предыдущих кривых при этом значении x , то текущая кривая видима в этой точке; в противном случае она невидима. На рис. 1 продемонстрирована часть работы алгоритма, где невидимые участки показаны пунктиром.

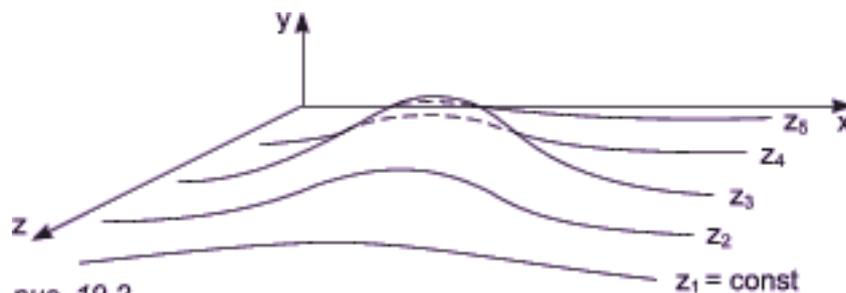


Рис. 1. Расположение кривых на плоскостях

2. Алгоритм Z-буфера (метод буфера глубины)

Данный алгоритм, как и предыдущий, основывается на анализе в пространстве изображения. В направлении линии видимости проводится ось z -координат, затем определяется, какие пиксели покрывают проекции объектов. Алгоритм хранит информацию об уже обработанных объектах в двух буферах: буфере кадра и z -буфере [2]. Буфер кадра содержит информацию о цвете объекта, отображаемого им на данный момент для каждого пикселя.

В z -буфере для каждого пикселя хранится z -координата видимого на данный момент объекта. Алгоритм работает таким образом, что, если z -координата объекта в этом пикселе меньше, чем z -координата, хранимая в z -буфере, тогда новый объект лежит перед видимым на данный момент. Тогда запишется цвет нового объекта в буфер кадра, а его координату – в z -буфер. В обратном случае новый объект не видим, и буферы останутся без изменений (рис. 2).

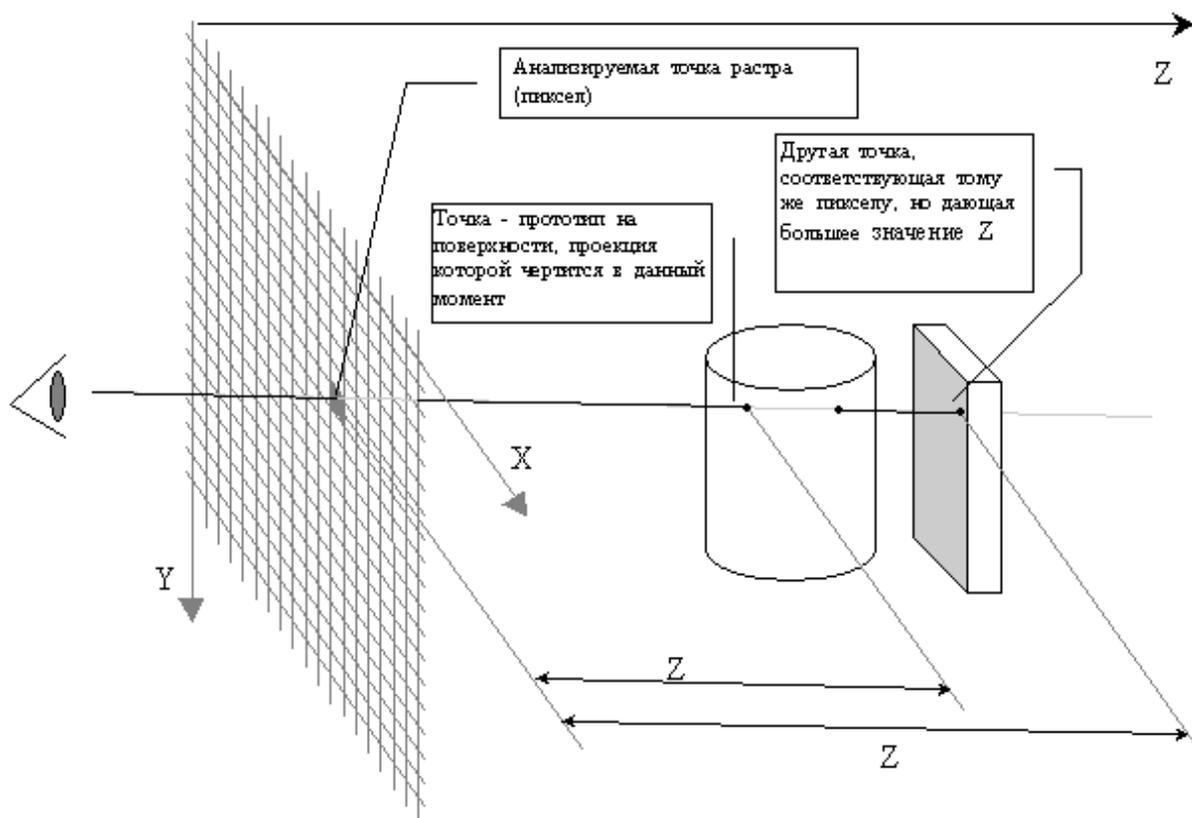


Рис. 2. Представление сути алгоритма в схематичном виде

3. Построение зон видимости с помощью триангуляции поверхности рельефа

В этом алгоритме построения зон видимости будут задействованы геометрические примитивы в виде треугольников, которые будут образовывать такие массивы, как: массив треугольников – описывающих поверхности всех объектов и поверхность рельефа; массив треугольников – описывающих поверхность исследуемого объекта; сторона квадрата, на которые будет разделена исследуемая территория [3] (Рис. 3).

Алгоритм построения зон видимости объекта будет следующим: исследуемая территория разбивается на некоторое число квадратов, квадраты, в свою очередь, представляют собой набор треугольников. Далее из центра выбранного треугольника проводится прямая в сторону наблюдаемого объекта и если этот отрезок будет пересечен поверхностью другого объекта, то

этот треугольник будет считаться невидимым. После проведения такой проверки всех треугольников для квадрата выставляется средняя оценка видимости, а после находится максимальная и минимальная оценка видимости квадратов всего объекта и создается итоговый интервал оценок. На рис. 4 представлен результат работы алгоритма. Наилучшая видимость объекта характерна для наиболее темных областей.

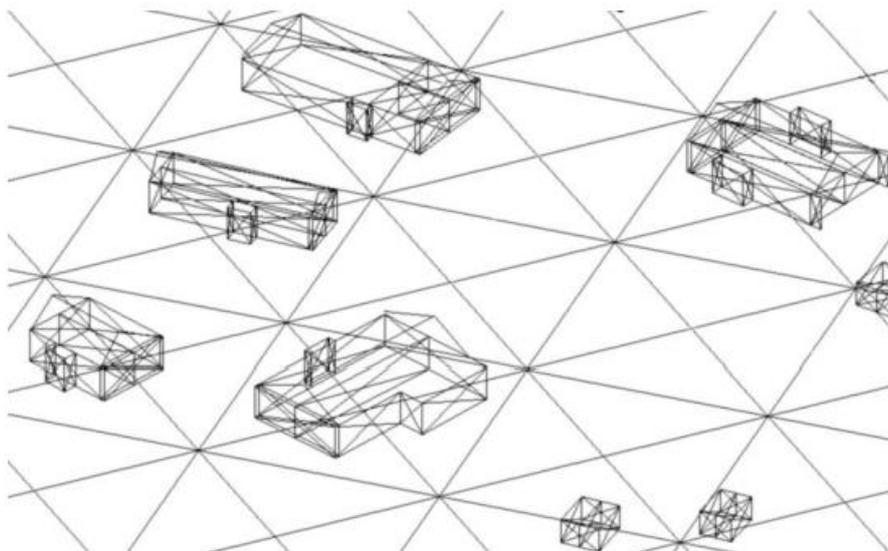


Рис. 3. Модель поселения

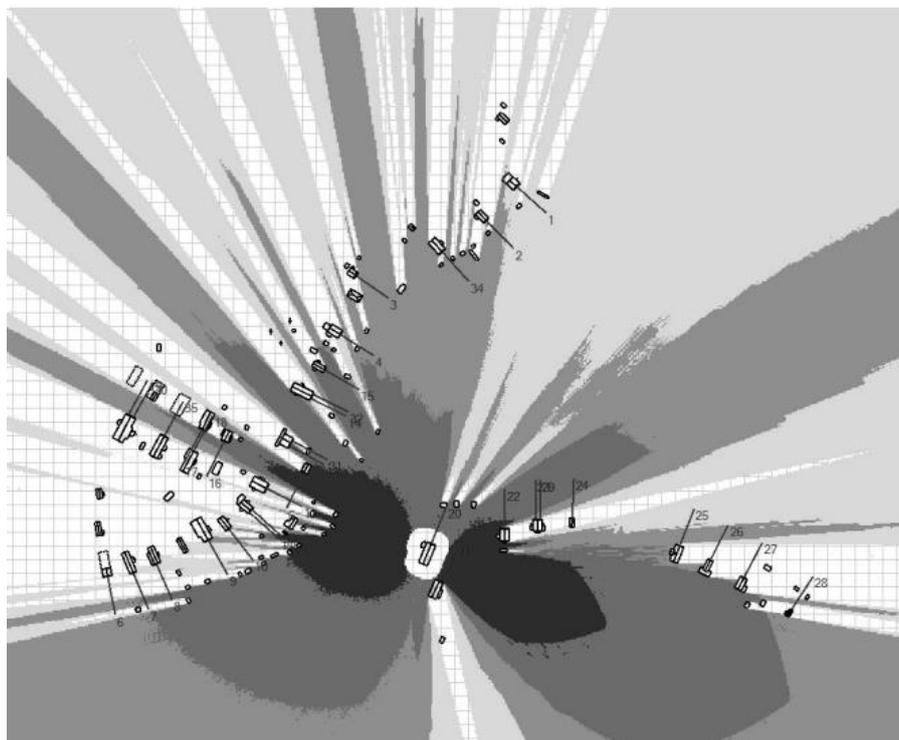


Рис. 4. Результат работы алгоритма

4. Алгоритм двойной итерации

Идея алгоритма создания зон видимостей на карте с рельефом заключается в том, что происходит «сканирование» карты в некотором радиусе с рельефом, для которого есть данные о высотах точек. «Сканирование» происходит таким образом, что из некоторой точки наблюдения, для которой также определены координаты (долгота, широта, высота), строятся линия видимости, благодаря которой можно определить видна ли та или иная точка рельефа в построенном направлении.

Видимость точек рельефа определяются путем сравнения значений высот точек, лежащих левее и правее от наблюдаемой. В случае, если ближайшая к наблюдателю точка будет ниже дальней, то можно сказать, что наблюдаемая точка видна, в противном случае – нет. Продолжая проводить подобные линии, можно получить видимые и скрытые от наблюдателя участки поверхности, что можно наблюдать на рис. 5.

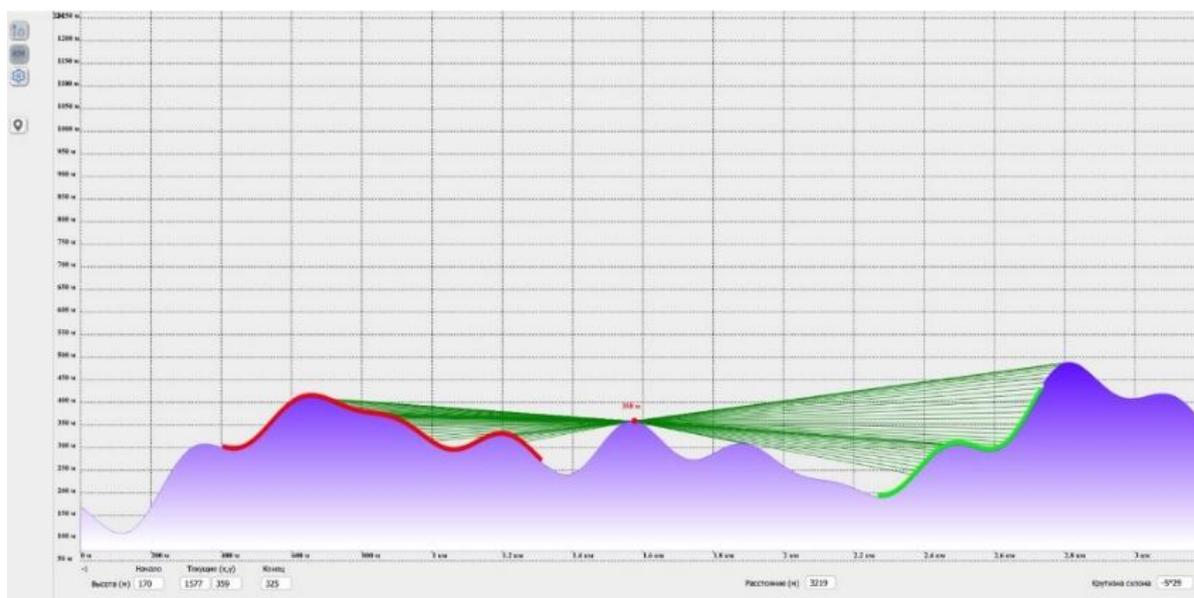


Рис. 5. Построение зон видимости

Далее процесс создания видимых областей повторяется со сдвигом на некоторый угол в выбранной области карты для заданного радиуса. Результат работы алгоритма представлен на рис. 6.

В результате данной работы рассмотрены некоторые методы и алгоритмы построения зон видимости с представлением результатов работы некоторых. Таким образом, в зависимости от необходимого способа анализа пространства и мощностей вычислительной техники должен проходить выбор в пользу того или иного алгоритма.

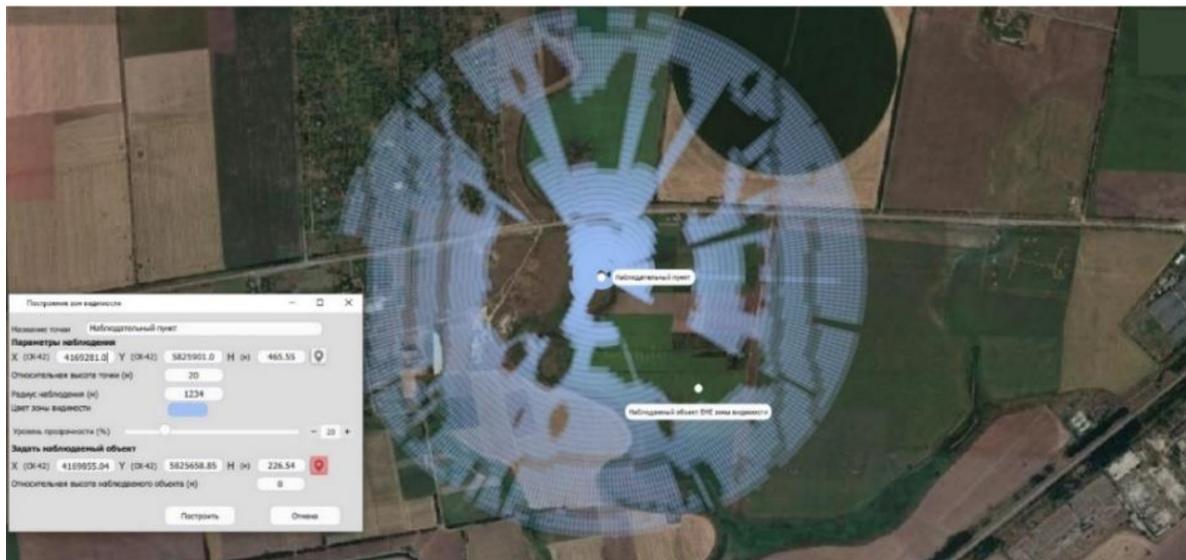


Рис. 6. Результат работы алгоритма

Список используемых источников

1. Мухин О. И. Компьютерная графика URL: <https://stratum.ac.ru/education/textbooks/kgrafic/author.html> (дата обращения: 27.02.2024)
2. де Берг М., ван Кревельд М., Овермарс М., Шварцкопф О. Вычислительная геометрия (2-е исправленное издание). Springer-Verlag, 2000. ISBN 3-540-65620-0 Глава 12: Разделение двоичного пространства. С. 259–267 URL: <https://neerc.ifmo.ru/wiki/index.php?title=BSP-%D0%B4%D0%B5%D1%80%D0%B5%D0%B2%D0%BE> (дата обращения: 27.02.2024)
3. Шлей М. Д. Алгоритм построения зон видимости объектов поселения // Вестник ЮУрГУ. Серия: Математическое моделирование и программирование. 2013. № 1. URL: <https://cyberleninka.ru/article/n/algorithm-postroeniya-zon-vidimosti-obektov-poseleniya> (дата обращения: 27.02.2024)

УДК 004.89:004.93'12
ГРНТИ 28.23.37

РАЗРАБОТКА СИСТЕМЫ ДЛЯ ПОИСКА МУЗЫКИ ПО РИТМУ

Э. Э. Гайбалиев, Ф. В. Филиппов

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

Представлена актуальность разработки и развития системы для поиска музыки по ритму. Выделены функциональные требования к поисковой музыкальной системе. Определен спектр технологий для разработки системы. Описан метод автоматического обнаружения и извлечения ритмической структуры в музыкальной композиции. Предложен алгоритм его реализации и применения. Обоснован выбор типа нейронной сети для реализации поиска музыки по ритму. Рассмотрен принцип обучения нейронной сети для решения поставленной задачи.

разработка информационной системы, распознавание музыки по ритму, поиск музыки.

Актуальность разработки системы для поиска музыки по ритму обусловлена несколькими факторами. Во-первых, с каждым годом количество музыкальных композиций увеличивается, и становится все сложнее найти подходящую музыку для определенного настроения или ситуации. Во-вторых, современные технологии позволяют анализировать музыкальные композиции на более глубоком уровне, что открывает новые возможности для поиска и классификации музыки. Разработка информационной системы для поиска музыки по ритму позволит пользователям быстро и эффективно находить композиции, соответствующие их предпочтениям и настроению. Это может быть особенно полезно для людей, которые занимаются спортом или танцами, так как они могут использовать систему для поиска музыки с определенным ритмом и темпом. Таким образом, разработка информационной системы для поиска музыки по ритму является актуальной задачей, которая может значительно улучшить опыт пользователей при поиске и прослушивании музыки.

Основной функцией системы является возможность найти музыку посредством введения ритма. Чтобы ввести ритм, необходимо нажать на кнопку поиска и настучать ритм клавишей «Пробел». После чего система обработает удары в числовой массив, где каждое число представляет собой временную метку, и выдаст 30 наиболее ритмически похожих песен.

Для реализации системы поиска музыки по ритму используется язык Python, т.к. он включает наибольшее число библиотек для создания нейронных сетей, а также для анализа звука и обработки видео.

Методом извлечения ритмической структуры из музыкальных композиций выбран бит-трекинг. Основной целью бит-трекинга является определение моментов начала и окончания каждого такта и темпа музыкальной композиции. Это позволяет создавать точную временную сетку и фиксировать временные метки каждого удара. Процесс бит-трекинга включает несколько этапов. Вначале анализируется аудиозапись с помощью алгоритмов, которые ищут ритмические характеристики, такие как ударные инструменты или другие яркие звуки, которые определяют акценты и ритм композиции. Затем алгоритмы обрабатывают эту информацию и определяют время начала и окончания каждого такта и темп музыкальной композиции. Преимуществом данного метода является то, что он достаточно прост и для его реализации не требуется больших вычислительных ресурсов. Однако потенциальным недостатком метода может быть его ограниченная способность обрабатывать сложные ритмические структуры.

Реализовать данный метод можно с помощью *librosa* – библиотеки Python, предоставляющей набор инструментов для анализа и синтеза аудио. Для выделения ритмических элементов из аудиосигнала обычно используется функция `beat.beat_track`, однако в данной работе использована функция `beat.plp`: она более предпочтительна, когда ожидается, что темп будет значительно меняться со временем, т.к. анализируется вся аудиозапись целиком, ведь пользователь может искать песню по любому ее фрагменту, то это довольно существенное преимущество.

Функция `beat.plp` используется для определения вероятности наличия ритмического элемента в данном временном интервале. Она анализирует огибающую силу начала в частотной области, чтобы найти локально стабильный темп для каждого кадра. Эти локальные периодичности используются для синтеза локальных полутонов, которые комбинируются таким образом, что пики совпадают с ритмически выраженными кадрами (например, событиями начала музыкальной временной сетки). Локальные максимумы пульсовой кривой можно принять за предполагаемые положения ударов [1]. Далее, для получения непосредственно ряда временных меток, использована функция `librosa.times_like`, на вход которой подается результат функции `beat.plp` и частота дискретизации.

На рис. 1 представлен результат работы функции `beat.plp`. Как видно на графике, функция улавливает довольно много шумов и звуков, которые обычный человек даже не заметит при прослушивании. Таким образом, запись временных меток для этих ударов может отрицательно повлиять на обучение нейронной сети и работу алгоритма поиска. Чтобы этого избежать, принято решение записывать только те удары, где вероятность наличия ритмического элемента во временном интервале выше 0.07.

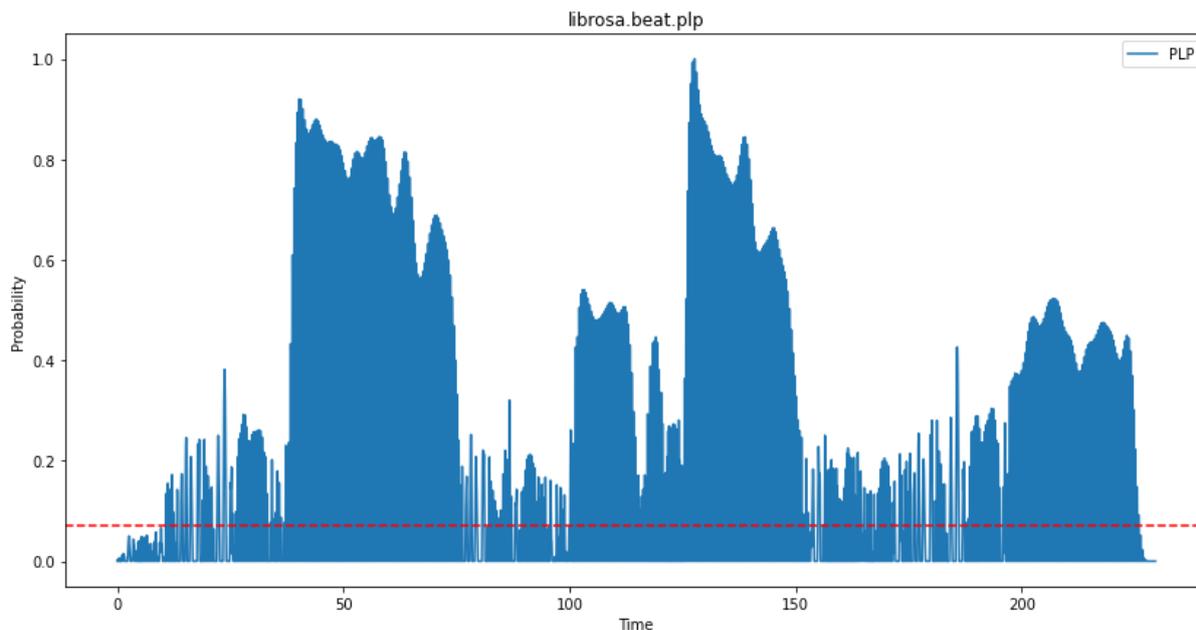


Рис. 1. Результат функции beat.plp

Для реализации алгоритма поиска выбрана рекуррентная нейронная сеть (RNN). RNN – тип нейронной сети, который особенно хорошо подходит для обработки последовательностей данных. В контексте поиска музыки по ритму, RNN может быть обучена на большом наборе данных музыкальных композиций, чтобы научиться распознавать и классифицировать различные ритмические паттерны. Затем, когда пользователь вводит новый образец ритма, RNN может быть использована для поиска наиболее похожих музыкальных композиций. В отличие от многослойных перцептронов, рекуррентные сети могут использовать свою внутреннюю память для обработки последовательностей произвольной длины. Поэтому сети RNN применимы в таких задачах, где нечто целостное разбито на части, например, распознавание рукописного текста или распознавание речи [2].

Однако обычные RNN имеют проблему с долговременной зависимостью, так как они могут забыть информацию из предыдущих шагов из-за проблемы исчезающего градиента. Поэтому в контексте данной работы выбрана LSTM (Long Short-Term Memory) – разновидность рекуррентной нейронной сети, которая была специально разработана для решения проблемы долговременной зависимости в последовательностях данных [3].

На вход нейронной сети подается не весь массив с временными метками. Перед этим каждая песня разбивается на 15-секундные отрезки. Предполагается, что средняя длина пользовательских ритмов с малой долей вероятности будет превышать данное значение, а слишком маленький отрезок может не отражать ритмический паттерн.

Система для поиска музыки по ритму имеет большой потенциал за счет высокой актуальности и малого количества похожих по функционалу систем. Главным преимуществом предложенного решения реализации алгоритма с помощью нейронной сети является его способность запомнить большое количество данных, что в контексте музыки имеет ключевое значение. В будущем можно также обучить модель на пользовательских данных, при достаточном их количестве, или изменить принцип извлечения ритмических структур из композиций, используя другие методы, например, спектральный анализ или динамическую битовую корреляцию.

Список используемых источников

1. McFee, B., Cai Y., McVicar M. Librosa documentation. California: librosa. 2021. 245 p. URL: <https://librosa.org/doc/main> (дата обращения 19.02.2024)
2. Гудфеллоу Я. Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвилль; перевод с английского А. А. Слинкина. 2-е изд. М.: ДМК Пресс, 2018. 652 с. ISBN 978-5-97060-618-6.
3. Прогнозирование временных рядов // Tensorflow. 2022. URL: https://www.tensorflow.org/tutorials/structured_data/time_series?hl=ru (дата обращения 19.02.2024)

УДК 004.056.52
ГРНТИ 20.01.04

DARKCOOL – АЛЬТЕРНАТИВНЫЙ ИНСТРУМЕНТ ДЛЯ ХАКИНГА

И. В. Гвоздков, А. И. Ликарь, М. Д. Поведайко

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

Постоянное расширение перечня программного обеспечения для пентеста значительно упрощает жизнь злоумышленникам. Гарантий, что указанное ПО будет применяться только в благих целях, нет, в результате чего возникает необходимость постоянного мониторинга ПО такого рода и ознакомления с ним.

защита; доступ к информации; противодействие взлому информационных систем

Развитие кибербезопасности включает в себя ряд мероприятий и технологий, направленных на защиту информационных систем от киберугроз. Они включают в себя разработку новых методов шифрования, создание более надежных антивирусов и защитных программ, обучение пользователей правилам безопасного поведения в сети, а также разработку законодательства, регулирующего кибербезопасность. Важным аспектом развития кибербезопасности является также постоянное обновление и улучшение существующих методов защиты, а также разработка специального программного обеспечения (ПО), чтобы противостоять постоянно меняющимся угрозам [1].

Параллельно развитию кибербезопасности развивается и хакерское искусство, назовем его так.

Развитие хакерского искусства включает в себя различные аспекты, как положительные, так и негативные. В контексте положительных аспектов развитие хакерского искусства может способствовать повышению уровня кибербезопасности путем выявления уязвимостей в информационных системах и помощи в разработке защитных мер, которые могут включать в себя исследование новых методов шифрования, анализ угроз и разработку инструментов для обнаружения и предотвращения кибератак.

Однако в данном виде деятельности превалирует негативная сторона, которая связана с угрозой для кибербезопасности. Некоторые хакеры могут использовать свои навыки для злонамеренных целей, таких как несанкционированный доступ к информационным системам, кража конфиденциальных данных, вымогательство и другие противоправные действия. Именно поэтому важно отличать развитие хакерского искусства в позитивном смысле, направленное на улучшение кибербезопасности, и злоупотреблением этими навыками для вредоносных целей [2].

В ходе эволюции вышеперечисленных «профессий» эволюционирует и ПО. В данной статье поговорим о DarkCool, достаточно простом ПО, но в тоже время функциональном [3]. Сравним DarkCool с Kali Linux, хотя это не совсем верное сравнение, т.к. мы будем сравнивать приложение с операционной системой, но сходства всё же у них есть.

Достоинства DarkCool:

1. Количество инструментов для тестирования на проникновение в DarkCool равно 177, а в Kali Linux – 600 (при этом не надо забывать, что это полноценная операционная система для пентеста). Спектр достаточно широк для приложения.

2. Обновления и поддержка в DarkCool, как и в Kali Linux, происходят регулярно. DarkCool имеет активное сообщество разработчиков, которые регулярно выпускают обновления и обеспечивают поддержку ПО.

3. Гибкость DarkCool в некотором роде проигрывает Kali Linux, но все же предлагает гибкую конфигурацию и возможность настройки под различные потребности тестирования на проникновение / хакинг.

4. Бесплатность DarkCool, что аналогично Kali Linux.

5. DarkCool, как и Kali Linux, поддерживает широкий спектр аппаратного обеспечения, что делает его доступным для установки на различные устройства.

6. Kali Linux, в отличие от DarkCool, имеет множество обучающих материалов и руководств, которые помогают пользователям изучить методы тестирования на проникновение и использование инструментов.

Несмотря на вышеперечисленные достоинства DarkCool также имеет некоторые недостатки, которые следует учитывать:

1. DarkCool, как и Kali, не подходит для ежедневного использования.

2. Уверены, что многие инструменты, как DarkCool, так и поставляемые с Kali Linux, могут быть под запретом в нашей стране из-за своего потенциального использования в незаконных целях.

3. Некоторые функции Kali Linux, а равно и DarkCool, могут требовать высокой производительности аппаратного обеспечения, что может быть проблемой для старых или слабых компьютеров.

Рассмотрим применение DarkCool на примере экстремистской и запрещенной социальной сети Facebook. Нет, взламывать ее мы не станем, на просторах Интернета и так существует большое количество обучающих видео по обходу алгоритмов идентификации, их названия приведены ниже:

1. Угадать пароль.

2. Попробовать старые пароли.

3. Запомнить меня.

4. Использовать кейлоггеры.

5. Забыть пароль.

6. Google Smart Lock.

Кажется, что ничего страшного не произошло. В данном примере произошло заспамливание страницы, но ее владелец никогда не установит источник, т.к., по сути, он им и является. Заспамленный экран приводить не станем. Печально, что в руках злоумышленников появился очередной инструмент по «отравлению жизни окружающих».

В данной программе помимо рассмотренного примера присутствуют достаточно серьезные инструменты, разбитые по следующим категориям:

1. EXPLOITER TOOLS.
2. CHECKER TOOLS.
3. SEARCHING GRAB TOOLS.
4. GRABBER TOOLS.
5. OTHER TOOLS.
6. RANDOM TOOLS.
7. BRUTEFORCE TOOLS.
8. DDOS ATTACK TOOLS.
9. WEBSHELL FINDER TOOLS.

Итого получается 177 позиций, как говорилось выше, собранных в 9 категориях.

В заключении необходимо сказать, что список хакерского ПО постоянно растет, а из названия приложения DarkCool совершенно непонятно его назначение, функционал и возможности. В результате этого вроде бы безопасная программа, как нам показалось на первый взгляд, с «дизайнерским назначением» и дословным переводом названия «Темно-холодный или прохладный», представляет собой достаточно серьезный инструмент осуществления противоправных действий. Поэтому сотрудникам, отвечающим за IT – безопасность, необходимо обращать внимание не только на названия запрашиваемых к установке и/или установленных программ, а также на системные требования, но и пристально анализировать функционал приложений, работающих на предприятии или организации.

Список использованных источников

1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны: практическое руководство / пер. с англ. Беликова Д. А. М.: ДМК Пресс, 2020. 326 с. ISBN 978-5-97060-709-1.

2. Белоус А. И., Солодуха В. А. Кибероружие и кибербезопасность. О сложных вещах простыми словами: монография. М.; Вологда: Инфра-Инженерия, 2020. 692 с. ISBN 978-5-9729-0486-0.

3. <https://github.com/DarkSkull777/DarkCool/blob/main/README.md> [дата обращения 01.02.2024].

УДК 004.932.2
ГРНТИ 20.19.29**ПОДХОД К МАРКИРОВАНИЮ ЭЛЕКТРОННЫХ
ДОКУМЕНТОВ, ВЫВОДИМЫХ НА ЭКРАН МОНИТОРА
ПОСРЕДСТВОМ НАЛОЖЕНИЯ НЕВИДИМОГО МАРКЕРА****П. Н. Горбачев, С. А. Копылов, М. М. Табунщикова**

Академия Федеральной службы охраны Российской Федерации

Высокая скорость обработки информации, удобное хранение и управление данными, возможность моделирования и анализа, многозадачность современных компьютеров – все это определяет быстрое развитие и распространение компьютерных технологий, автоматизацию работы с данными. Но помимо всех достоинств применения информационных технологий существует и основной недостаток в виде утечки данных. Для защиты от этого разрабатываются различные методы и средства. В данной статье представлен подход к маркированию экрана изображения, выводимого на экран монитора с целью предотвращения утечки данных, обусловленной фотографированием экрана или созданием снимка экрана с последующей отправкой сформированного изображения за пределы контролируемого периметра.

утечка информации, маркирование изображения, выводимого на экран монитора

В информационной сфере данные и информация обрабатывается на объектах информатизации и автоматизированных рабочих местах, что определяет задачу по защите прав владельцев интеллектуальной собственности и конфиденциальной информации от утечки одной из наиболее важных задач в области обеспечения информационной безопасности. По данным аналитического центра Infowatch, в 2023 году количество утечек информации в мире выросло в 2,4 раза, а скомпрометированных записей персональных данных в мире составило 18,3 млрд. В России «утекло» 705 миллионов записей персональных данных, что на 72 % больше, чем в 2022 г. Стоит отметить, что в отчетном периоде количество утечек государственной тайны также увеличилось вдвое. В ходе дальнейшего анализа статистических данных по утечкам конфиденциальной информации и информации ограниченного доступа установлено, что для успешной реализации большинства случаев утечек информации использовались методы, основанные на эксплуатации существующих уязвимостей (37 %), применение вредоносного программного обеспечения (45 %) и методы социальной инженерии.

Для защиты от утечки информации разрабатываются и применяются различные средства. Наиболее востребованной и популярной является технология DLP (Data Leak Prevention), которая осуществляет анализ циркулирующей информации и каналов передачи информации (электронная почта, веб, мессенджеры, FTP и прочее). Помимо циркулирующей информации и

каналов передачи данных, осуществляется анализ содержимого файловых хранилищ, а также локальные хранилища персональных ЭВМ пользователей (загрузка файлов на съемные носители, внесение изменений в документы, отправку их на печать и прочие события). Основным достоинством DLP-систем является возможность анализа всего объема обрабатываемой информации [1]. К существующим недостаткам относятся необходимость маркирования всей анализируемой информации (наличия информации о том, каким образом отличается информация ограниченного доступа от открытой информации).

Помимо технологии DLP, для защиты от утечки применяется технология управления цифровыми правами DRM (Digital Rights Management), которая осуществляет управления цифровой лицензией для файлов, позволяя работать с файлом только тем пользователям, у которых есть актуальная лицензия. Для защиты информации система DRM реализует шифрование файла, оставляя информацию о том, к какому сервису можно обратиться за ключом, позволяющим его расшифровать и отобразить пользователю. Пользователь, желающий просмотреть содержимое файла, запускает специализированное программное обеспечение, позволяющее обрабатывать файлы данного типа. В процессе взаимодействия из файла получается информация о местоположении сервера DRM. Сервер DRM проверяет, может ли пользователь работать с файлом, и если ответ положителен, то пересылает ключ в адрес специализированного программного обеспечения и осуществляется расшифровывание файла полученным ключом с последующим отображением его пользователю [2].

Описанные технологии позволяют обнаруживать маркированные данные и контролировать доступ к обрабатываемым файлам определенному кругу пользователей, но являются малоэффективными для противодействия утечки информации по каналу, обусловленному фотографированием или созданием снимка экрана монитора с выводимым на него документом ограниченного доступа или конфиденциальной информации. Для защиты от утечки по указанному каналу разработан подход к маркированию изображения, выводимого на экран монитора, посредством наложения полупрозрачного маркера (QR-кода) в те области изображения, в которых сохраняются характерные точки после применения фотографирования или получения снимка экрана монитора.

Разработанный подход к маркированию изображения, выводимого на экран монитора, состоит из следующих этапов:

1. Создание текущего снимка экрана монитора. На данном этапе посредством API функций операционной системы формируется снимок экрана монитора, содержащий выводимый документ.

2. Обнаружение областей встраивания маркера (QR-кода). Для реализации обнаружения проведена сравнительная оценка используемых детекторов ключевых точек для обнаружения текстовых областей изображения. В ходе проведенного анализа [3] установлено, что наиболее точное соответствие ключевых точек исходного и сфотографированного изображения получается посредством применения детектора ключевых точек FAST. Пример детектирования ключевых точек представлен на рис. 1.

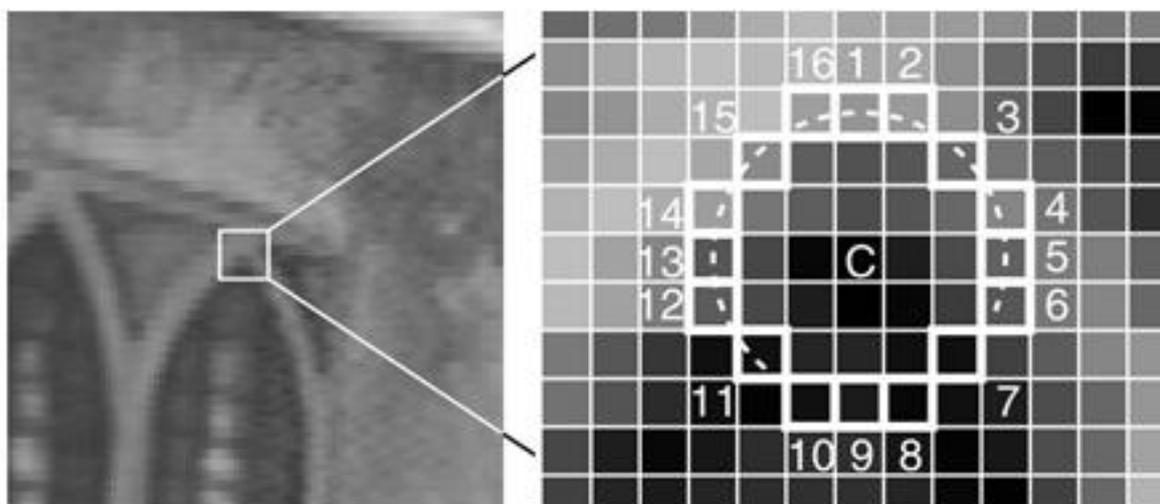


Рис. 1. Детектирование ключевых точек по алгоритму FAST

3. Формирование встраиваемого маркера (QR-кода). В качестве встраиваемого маркера обоснован выбор QR-кода, который представляет двумерный штрих-код, состоящий из черных квадратов, расположенных на белой квадратной сетке. QR-код имеет специальный механизм, увеличивающий надежность хранения закодированной в нем информации. Для кодов с самым высоким уровнем надежности могут быть испорчены или затерты до 30 % поверхности, но при этом информация будет сохранена и при необходимости корректно прочитана. Для исправления ошибок используется алгоритм Рида-Соломона, который заключается в том, что к шаблону QR-кода добавляются дополнительные модули, содержащие дубликаты встроенных данных. Таким образом, с их помощью сканеры будут по-прежнему распознавать QR-код, даже если его часть повреждена, отсутствует или закрыта [4]. Ввиду наличия стойкости встраиваемый QR-код может быть полупрозрачным или иметь прозрачность меньшую, чем встраиваемая область исходного изображения для снижения его незаметности.

4. Встраивание маркера (QR-кода) в обнаруженные области изображения, выводимого на экран монитора. Внедрение сформированного маркера осуществляется посредством внесения изменений в альфа-канал (прозрачность) изображения или посредством наложения полупрозрачного изображения маркера на исходное изображение. В случае работы с альфа-

каналом (прозрачностью) каждому пиксельному значению добавляется по крайней мере 1 оверлейный бит. Его установка позволяет программе визуализации выборочно игнорировать те пиксельные значения, у которых этот бит установлен. Другим способом встраивания маркера в канал прозрачности является наложения изображений за счет изменения прозрачности нижней и накладываемых картинок, в этом случае каждое пиксельное значение содержит не 1 оверлейный бит, а обычно 8. В результате наложения встраиваемого маркера формируется промаркированное изображение [5].

В результате работы алгоритма маркирования изображения электронного документа осуществляется внедрение идентификационной информации о степени конфиденциальности данных, идентификаторе пользователя или другая метаинформация, позволяющая однозначно идентифицировать как сам документ, так и его владельца. Выбор содержимого встраиваемого маркера (QR-кода) определяется в зависимости от решаемой задачи: обеспечение авторских прав пользователей, защиты от утечки или подтверждения авторства. Практическая реализация разработанного подхода к маркированию электронных документов, выводимых на экран монитора, позволит оценить стойкость разработанного маркера к осуществлению операций фотографирования или получения снимка экрана изображения, а также количественные значения точности извлечения встроенной в маркер информации после указанных преобразований. Практическая реализация и экспериментальная оценка являются направлением дальнейших исследований.

Список используемых источников

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. Киев: «МК-Пресс», 2006. 288 с., ил.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: СОЛОН-Пресс, 2017. 262 с.
3. Арестов А. А. Применение детекторов ключевых точек для обнаружения текстовых областей изображения / А. А. Арестов, С.А. Копылов. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ Актуальные проблемы инфотелекоммуникаций в науке и образовании, 2022. Т. 2. С. 30–35.
4. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling // IEEE Workshop of Nonlinear Signal and Image Processing, Greece, June 20–22, 1995. PP. 123–132.
5. Абасова А. М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение / М. А. Абасова. Известия ЮФУ. Технические Науки. 2014. С. 75–81.

УДК 004.273
ГРНТИ 20.15.05

ЗАБЫТЫЕ И НЕОЦЕНЕННЫЕ ЯЗЫКИ ПРОГРАММИРОВАНИЯ В УЧЕБНОМ ПРОЦЕССЕ КАК БАЗИС ПРОГРАММИРОВАНИЯ В УЧЕБНОМ ПРОЦЕССЕ

В. В. Громов

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

В докладе рассматриваются методика обучения студентов с помощью систем виртуальных машин при выполнении учебных заданий по дисциплине «Архитектура информационных систем» в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Приведенная методика основана на многолетнем опыте формирования и эксплуатации Федеральной информационной системы Госавтоинспекции с 1996 по 2013 г.г. Анализируются перспективы формирования навыков создания информационных систем студентов в условиях современного развития вычислительной техники.

системы виртуальных машин, программные системы, операционные системы

Статья подготовлена по материалам цикла лабораторных работ и лекций, которые были разработаны для дисциплины «Архитектура информационных систем» в период с 2019 по 2024 годы. В основу лабораторных работ указанной дисциплины положен язык Shell и системные утилиты, которые являются на протяжении последних 50 лет основополагающими в операционных системах семейства UNIX и Linux для конфигурации основных сервисов.

Больше 95 % студентов каждого курса работает в операционной системе Windows, остальные в macOS (большинство) и в редком исключении – Linux. Формально в рамках нескольких дисциплин, таких как:

- Архитектура информационных систем;
- Открытые операционные системы;
- Операционная система Linux.

Мы настоятельно рекомендуем студентам, чаще всего на третьем курсе СПбГУТ, обратить внимание на операционную систему семейства Linux.

В большинстве своем студенты не решаются отказаться от Windows и переходить на Linux.

Знакомство автора статьи с Linux состоялось в 1997 году, когда в рамках эксперимента был установлен Linux Caldera компании Tarantella на сервер Tricord-30.

Совсем другое отношение автора к UNIX системам. Первое знакомство с ОС Solaris корпорации SUN состоялось в 1996 году. С системой AIX корпорации IBM автор познакомился в 2010 году, позже – с операционной системой Mac OS X, которая сейчас переименована в macOS [1].

Естественно, во время опытных работ мы изучали такие UNIX системы как SCO и DEC OSF1. Все перечисленные Linux и UNIX системы объединяет одно – наличие стандартных утилит и языков программирования, к которым относятся:

- GAWK – это полноценный язык обработки текстовой информации с синтаксисом, напоминающим синтаксис языка C [2];
- SED – потоковый редактор [3];
- GNU-Cobol – высокоуровневый язык программирования [4];
- Shell – внутрисистемный процедурный язык, схожий по синтаксису с C [5].

Начнем с языка Shell, который является «скриптовым языком». Скрипт, написанный на языке Shell – это компьютерная программа, предназначенная для запуска с помощью оболочки UNIX/Linux интерпретатора командной строки. Различные диалекты сценариев оболочки считаются скриптовыми языками. К диалектам языка Shell относятся:

- KornShell (ksh) – в нескольких возможных версиях, таких как ksh88, Korn Shell '93 и других;
- Bash – один из старейших терминалов (интерпретаторов командной строки), до сих пор широко используемая;
- C подобный терминал (csh);
- GNU Bash (bash);
- tcsh, основной терминал для языка программирования Tcl/Tk.

В настоящее время в системе школьного образования начинают обучение программирования с языка Python или Pascal. На взгляд автора, при переходе по программе импортозамещения от Windows к Linux системам необходимо пересмотреть программу обучения и начать обучение с языка Shell.

Язык Shell – внутрисистемный язык исполнения сценариев, который работает при запуске служб и приложений, а также при установке или удалении пакетов обновления и обработке репозитариев.

По своей сути Shell (под словом Shell мы будем понимать интерпретаторы команд такие как sh, bash, csh, ksh, tcsh, zsh) представляет собой просто макропроцессор, выполняющий команды. Термин «макропроцессор» означает функциональность, при которой текст и символы расширяются для создания более крупных выражений.

Unix терминал является одновременно интерпретатором команд и языком программирования (это касается BSD, AIX, Solaris, macOS). В качестве

интерпретатора команд оболочка предоставляет пользовательский интерфейс для богатого набора утилит GNU.

Возможности языка программирования позволяют комбинировать эти утилиты. Файлы, содержащие команды, могут быть созданы и сами станут командами. Эти новые команды имеют тот же статус, что и системные команды в таких каталогах, `/usr/bin`, что позволяет пользователям или группам создавать собственные среды для автоматизации своих общих задач.

Терминалы могут использоваться интерактивно или в фоновых процессах. В интерактивном режиме они принимают ввод, вводимый с клавиатуры. При фоновом выполнении командный процессор выполняет команды, считанные из файла.

Командный процессор (терминал) имеет ряд особенностей таких как:

- Синхронное выполнение команд GNU;
- Асинхронное выполнение команд GNU.

Терминал, а точнее скрипт, запущенный в терминале, ожидает завершения синхронных команд, прежде чем принять дальнейшие входные данные, а асинхронные команды продолжают выполняться параллельно с терминалом (в фоновом режиме), пока командный процессор читает и выполняет дополнительные команды.

Различные сложные конструкции перенаправления позволяют детально контролировать ввод и вывод этих команд, а также контролировать содержимое окружения команд.

Терминал по своей сути предоставляет набор встроенных команд и утилит, реализующих функциональность, которую невозможно или неудобно получить с помощью отдельных утилит или дополнительно установленных сторонних программных продуктов (модулей).

Например, `cd`, `break`, `continue` и `exes` не могут быть реализованы вне терминала, поскольку они манипулируют самим терминалом. Встроенные команды `history`, `getopts`, `kill` или `pwd`, среди прочего, могут быть реализованы в отдельных утилитах, но их удобнее использовать как встроенные команды.

Хотя выполнение команд имеет важное значение, большая часть сложности их применения обусловлена встроенными в них языками программирования. Как и любой другой язык высокого уровня, терминал предоставляет переменные окружения, конструкции управления потоком, кавычки и функции.

Командный процессор предлагает функции, предназначенные специально для интерактивного использования, а не для расширения языка программирования. Эти интерактивные функции включают управление заданиями, редактирование командной строки, историю команд и псевдонимы, а также циклы.

SED (Stream Editor) – редактор потока обычно используется для фильтрации текста, т.е. он принимает введенный текст, выполняет над ним некоторую операцию (или набор операций) и выводит измененный текст. Обычно используется для извлечения части файла с использованием сопоставления с образцом или замены нескольких вхождений строки в файле. Он может использоваться для выполнения основных преобразований текста во входном потоке (файле или входных данных из конвейера).

Хотя в некотором смысле SED похож на редактор, который допускает редактирование по сценарию (например, `ed`, `sed`), он работает, выполняя только один проход по входным данным и, следовательно, более эффективен, но именно `sed` способность фильтровать текст в конвейере особенно отличает его от других типов редакторов.

GAWK – этот файл представляет собой `awk` подобную программу, которую можно использовать для выбора определенных записей в файле и выполнения над ними операций. Основная функция `awk` – поиск в файлах строк (или других единиц текста), содержащих определенные шаблоны.

Когда строка соответствует одному из шаблонов, `awk` выполняет указанные действия над этой строкой и продолжает обрабатывать входные строки таким образом, пока не достигнет конца входных файлов.

Программы на языке `awk` отличаются от программ на большинстве других языков, поскольку `awk` программы *управляют данными* (т. е. вы описываете данные, с которыми хотите работать, а затем, что делать, когда вы их найдете). Большинство других языков являются *процедурными* и придется очень подробно описать каждый шаг, который должна предпринять программа.

При работе с процедурными языками обычно гораздо сложнее четко описать данные, которые будет обрабатывать ваша программа. По этой причине `awk` программы зачастую легко читать и создавать. При запуске `awk`, вы указываете `awk` программу, которая сообщает `awk` параметры обработки потока. Каждое выражение (шаблон) определяет один шаблон для поиска и одно действие, которое необходимо выполнить при его обнаружении.

Операторы циклов, такие как `if`, `while`, `dowhile` и т.д., управляют потоком выполнения `awk` программ. Большинство `awk` логических операторов созданы по образцу аналогичных операторов в C. Все циклические конструкции начинаются со специальных ключевых слов, таких как `if` и `while`, чтобы отличать их от простых выражений. Многие операторы циклов могут содержать набор операторов для выполнения каких-либо задач.

Например, `if` оператор содержит условие, которое может быть выполнено или нет. Содержащийся набор операторов называется *телом* цикла для того, чтобы включить в тело более одного оператора, их группируют их в один *составной оператор* с помощью фигурных скобок, разделяя их символами новой строки или точкой с запятой.

Формально представленные в данной статье языки программирования AWK (GAWK), SED, SHELL не упоминаются и не изучаются в школьной программе, а как следствие, в программе ВУЗов, что, в свою очередь, ведет к необоснованным ресурсным затратам при строительстве (создании) информационных систем.

В рамках дисциплины «Архитектура информационных систем» был разработан цикл лабораторных работ, который позволяет студентам на базе языков AWK (GAWK), SED, SHELL обрабатывать текстовые данные, а также производить обработку фото-видео потоков и практически любой информации для создания и ведения информационной системы специализированного назначения.

Перечисленные языки незаконно забыты многими преподавателями и тем более чиновниками, составляющими программы обучения, что ограничивает возможности наших выпускников при дальнейшей работе на производстве.

Список используемых источников:

1. Сайт Операционной системы GNU URL: <https://www.gnu.org> (дата обращения 31.03.2024)
2. Сайт Wikipedia Stream Editor URL: <https://en.wikipedia.org/wiki/Sed> (дата обращения 01.04.2024)
3. Сайт Wikipedia Shell script URL: https://en.wikipedia.org/wiki/Shell_script (дата обращения 01.04.2024)
4. Сайт корпорации GNU Cobol URL: <https://gnucobol.sourceforge.io> (дата обращения 01.04.2024)
5. Сайт Wikipedia Shell URL: https://en.wikipedia.org/wiki/Unix_shell (дата обращения 01.04.2024)

УДК 004.273
ГРНТИ 20.15.05

ПРОГРАММА УЧЕТА ПРИСУТСТВИЯ СТУДЕНТОВ КАК ОСНОВА ИЗМЕНЕНИЯ ПОВЕДЕНЧЕСКИХ АЛГОРИТМОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В. В. Громов

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

В докладе рассматривается программа учета присутствия студентов на занятиях как основа для изменения поведенческих алгоритмов преподавателей и студентов при проведении лекций, практических и лабораторных занятий.

Анализируются перспективы внедрения опытной эксплуатации программы учета присутствия студентов для современных информационных систем в условиях импортозамещения и дефицита информационных мощностей.

системы виртуальных машин, программные системы, операционные системы

Данная статья написана по материалам цикла экспериментальных работ, которые были проведены в рамках дисциплины «Архитектура информационных систем» во втором семестре 2024 года.

История создания программы учета присутствия студентов (далее по тексту – PUPS programm unit present student) началась достаточно давно – более пяти лет тому назад – и имеет некоторую предысторию.

На протяжении четырех, а может, и пяти лет автор статьи неоднократно предлагал студентам в качестве темы разработку специального программного обеспечения для учета присутствия студентов на занятиях.

Каждый раз студенты по каким-либо причинам отказывались от решения данной проблемы. Учитывая данный факт, автором было принято решение о дополнительном изучении и всестороннем рассмотрении аспектов данной проблемы. После чего было проведено несколько экспериментов и создано действующее программное обеспечение.

Начнем с главного – СКУД (система контроля и управления доступом), которая идентифицирует студента на входе в здание ВУЗа. Система СКУД соответствует перечню стандартов, которые регламентируют правила ее эксплуатации, а именно:

- ГОСТ Р 51241-2008. Является основным документом с описанием технологии, устройств [1];
- ГОСТ Р ИСО/МЭК 7810-2015. Работа с картами [1];
- ГОСТ Р ИСО/МЭК 19795-1-2007. Правила автоматической биометрической проверки [1];
- ГОСТ Р 50009-2000. Электромагнитная совместимость [1];

- ГОСТ Р 50739-95, ГОСТ IEC 60065-2013. Защита вычислительной техники, аналоговой, видео и аудио аппаратуры от несанкционированного просмотра, копирования информации [1];
- ГОСТ Р 51072-2005. Один из стандартов УПУ – требования при использовании защитных дверей. Аналогичные нормативные документы подбирают при производстве и монтаже других управляемых устройств;
- ГОСТ Р 52931-2008. Системы управления [1];
- ГОСТ 2.601-2006, ГОСТ 2.610-2006. Единые правила для разработки конструкторской документации (ЕСКД) [1].

При работе со СКУД используются и другие стандарты, которые соответствуют конкретной задаче. Полный список приводится в документации к системе конкретного объекта [2].

Идея использовать СКУД для контроля за доступом студентов в здание лишь частично решает проблему контроля, т.к. СКУД не работает во всех аудиториях. Поэтому было приобретено устройство чтения смарт-карт RFID, которое было приобретено на Aliexpress (рис. 1) [2].



Рис. 1. Устройство чтения смарт-карт RFID [3]

Следующим этапом для создания программы PUPS было выбор языка программирования, т.к. это является основой для возможности дальнейшей эксплуатации программы. Выбор остановился на языке GnuCOBOL, который является приемником (OpenCOBOL) – бесплатный современный компилятор COBOL [4].

GnuCOBOL реализует значительную часть стандартов COBOL 85, X/Open и более новых стандартов ISO COBOL (2002, 2014, 2023), а также множество расширений, включенных в другие компиляторы COBOL (IBM COBOL, MicroFocus COBOL, ACUCOBOL-GT и другие) [3].

Почему такой древний язык, а не C++, зададитесь таким вопросом? Ответ предельно прост. Когда автор учился в Санкт-Петербургском университете телекоммуникаций в период с 1988 по 1995 год, в то время не преподавался ни язык Си, ни тем более C++. Изучались языки Fortran, Basic, Pascal.

С 1994 года автору пришлось изучать, а точнее сказать, познакомиться со следующими языками программирования: d-BASE, Foxpro, Clipper, REXX, Shell, Natural & Adabas C.

Внимательно изучив перечень языков, которые имеют компилятор и способны формировать бинарные файлы, выбор остановился на языке GNU-Cobol. В 2023 году автору пришлось сесть за учебники по языку Cobol и с учетом различных его модификаций создать несколько десятков программ, а затем начать программировать систему [4].

Задача была поставлена самой жизнью, т.к. на протяжении более чем 10 лет автор наблюдает, как некоторые студенты прикрываются студсоветом или работой в ВУЗе и систематически пропускают занятия.

Если студент не посещает занятия, может, ему перейти на заочный факультет и освободить свое бюджетное место для студента, который желает очно проходить обучение? Это был главный вопрос, который явился двигателем, для создания программы учета присутствия студентов.

Была написана первая версия программы, которая фиксировала основные данные, но требовалось создание нового интерфейса для терминала.

Создание интерфейса для терминала открытой системы является не тривиальной задачей и требует особых знаний при проектировании информационной системы. Были изучены сотни листов документации по языку GNU-Cobol, написаны сотни строк программ в качестве тренировки, и только после тщательной проверки программа была представлена студентам для проведения тестовых испытаний.

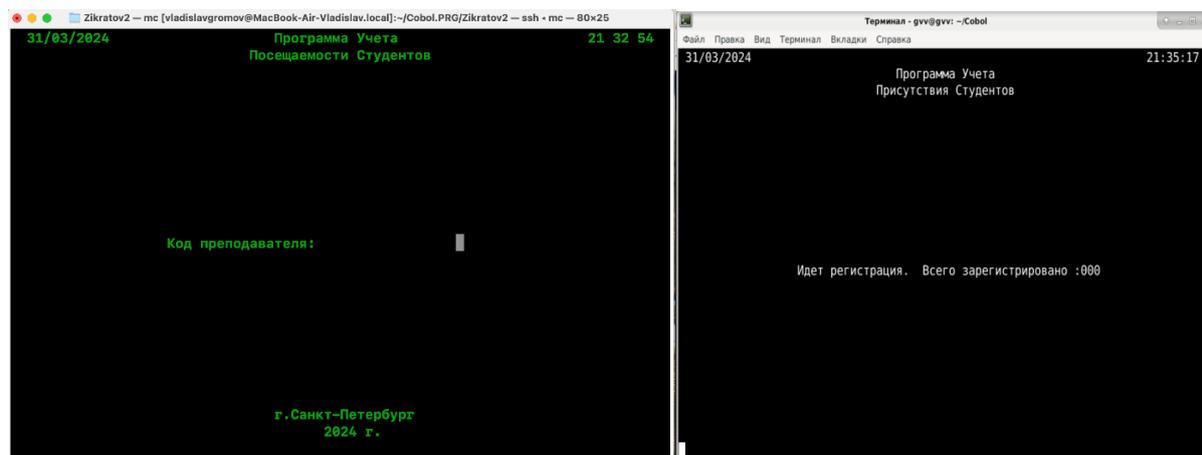


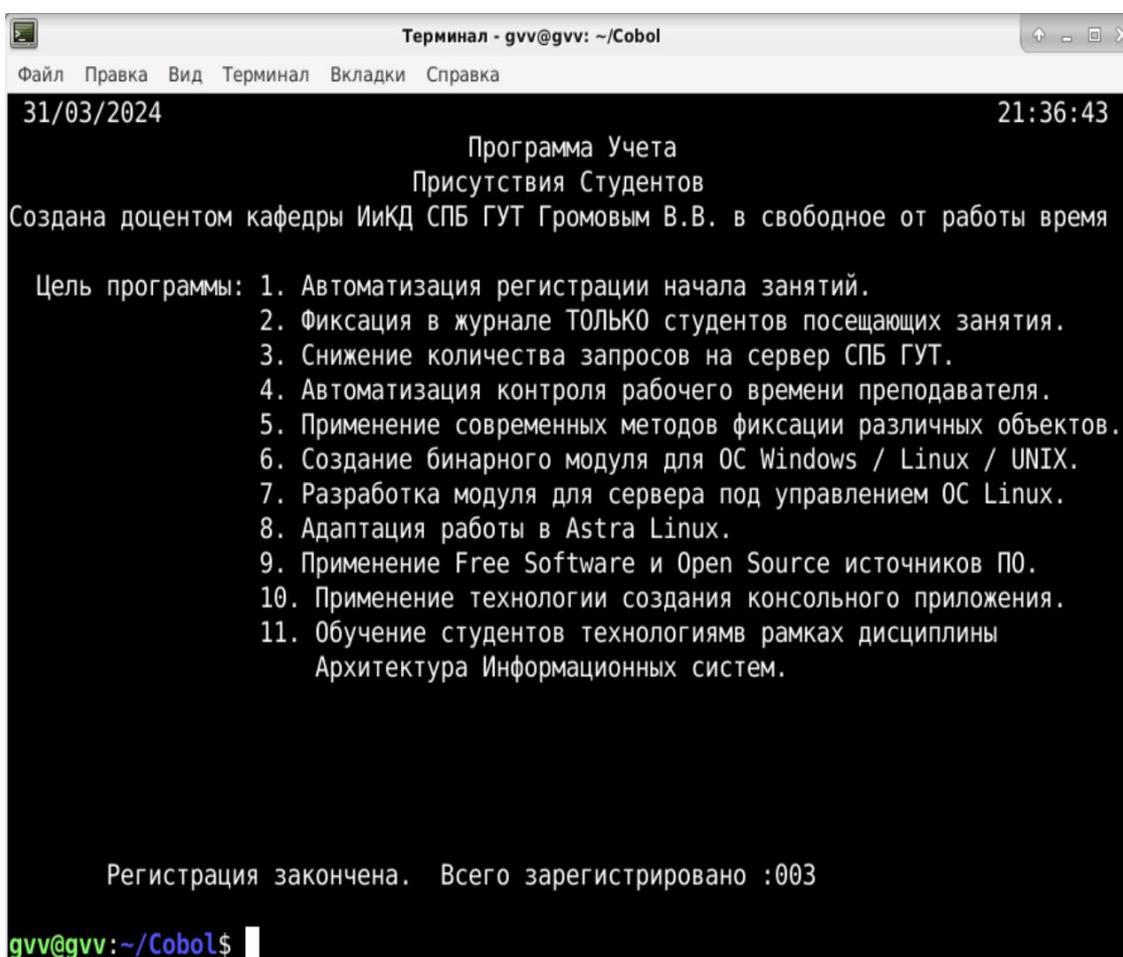
Рис 2. Программа учета посещаемости студентов

На рис. 2 представлены две версии программы учета посещаемости студентов. снимок слева – программы для macOS, снимок справа – для Linux

систем. Есть еще одна версия программы – для работы в среде Windows. Размер бинарных файлов не превышает 100 кВ, размер библиотек – 4 МВ.

Программа работает следующим образом:

- Вызывается программа из командной строки, автоматически после регистрации преподавателя на сервере;
- Регистрируются пропуска присутствующих студентов;
- Формируется файл, в котором содержится информация о зарегистрированных пропусках студентов по системе СКУД;
- После окончания регистрации преподаватель закрывает ведомость, а, как следствие, формируется итоговый файл для загрузки в информационную систему СПбГУТ.



```
Терминал - gvv@gvv: ~/Cobol
Файл Правка Вид Терминал Вкладки Справка
31/03/2024 21:36:43
Программа Учета
Присутствия Студентов
Создана доцентом кафедры ИиКД СПб ГУТ Громовым В.В. в свободное от работы время

Цель программы: 1. Автоматизация регистрации начала занятий.
2. Фиксация в журнале ТОЛЬКО студентов посещающих занятия.
3. Снижение количества запросов на сервер СПб ГУТ.
4. Автоматизация контроля рабочего времени преподавателя.
5. Применение современных методов фиксации различных объектов.
6. Создание бинарного модуля для ОС Windows / Linux / UNIX.
7. Разработка модуля для сервера под управлением ОС Linux.
8. Адаптация работы в Astra Linux.
9. Применение Free Software и Open Source источников ПО.
10. Применение технологии создания консольного приложения.
11. Обучение студентов технологиям в рамках дисциплины
Архитектура Информационных систем.

Регистрация закончена. Всего зарегистрировано :003
gvv@gvv:~/Cobol$
```

Рис 3. Программа учета посещаемости студентов

На рис. 3 продемонстрировано итоговое информационное сообщение, выдаваемое программой, в консоль системы.

Следует отметить, что код программы в операционных системах Windows, macOS, Linux существенно отличается только при описании установок терминала.

Данное несоответствие было обнаружено при компиляции программы в бинарный модуль. Это вызвано необходимостью работы с кириллическими шрифтами. Формально нужно отметить, что исходные тексты GNU-Cobol более качественно отредактированы под macOS, чем под Linux, но на результат данное соответствие не повлияло.

Зачем нужна эта программа? В первую очередь эта программа нужна, чтобы снять нагрузку с центрального сервера СПбГУТ при регистрации студентов на портале [5]. Во вторую очередь данная программа нужна преподавателям, чтобы не производить переключку в аудитории для отметки отсутствующих студентов. В третью очередь, она нужна для руководства СПбГУТ, чтобы контролировать студентов и преподавателей, которые находятся на территории ВУЗа.

Внедрение данной программы на этапе опытной эксплуатации позволило повысить посещаемость, а также улучшить дисциплину студентов. Снизилось число опаздывающих на лекцию и практические занятия. Формально изменились поведенческие алгоритмы поведения как студентов, так и преподавателя.

Автор не сомневается, что внедрение данной программы в информационную систему СПбГУТ позволит не только улучшить посещаемость занятий, но и получить правильную статистику при подсчете числа обучаемых студентов и посещаемости занятий.

Список используемых источников:

1. Сайт ЗАО «Компания Безопасность». URL: <https://www.bezopasnost.ru/services/367> (дата обращения 31.03.2024)
2. Сайт Aliexpress. URL: <https://aliexpress.ru/item/32932022027.html?spm=a2g2w.orderdetail.0.0.6ecc4aa6jTcrDu> (дата обращения 01.04.2024)
3. Сайт Операционной системы GNU. URL: <https://www.gnu.org> (дата обращения 31.03.2024).
4. Сайт корпорации GNU Cobol. URL: <https://gnucobol.sourceforge.io> (дата обращения 01.04.2024)
5. Сайт СПбГУТ. URL: <https://lk.sut.ru/cabinet/?login=yes> (дата обращения 31.03.2024)

УДК 004.023
ГРНТИ 50.41.25**РАЗРАБОТКА АРХИТЕКТУРЫ И СТРУКТУРЫ
ХРАНЕНИЯ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ
НЕЧЕТКИХ ДАТ ИСТОРИЧЕСКИХ АРТЕФАКТОВ****А. А. Груздев, Д. С. Крахмалев, А. А. Павлович**

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

В мире архитектуры и истории существует важная задача – поиск и идентификация артефактов, учитывая различные уровни точности дат их создания. В статье приведен анализ выбора архитектуры для реализации программного компонента, позволяющего решать поставленную задачу. Рассматривается понятие «чистой архитектуры» и ее составляющие. Анализируются варианты систем управления базами данных и структур хранения исходя из четкого и нечеткого формата датировки в системе. Описывается влияние выбранных решений на масштабируемость и эффективность системы.

нечеткая логика, чистая архитектура, база данных, функция принадлежности, масштабируемость системы, реляционное и нереляционное хранилище

В первой части нашего исследования была синтезирована функция принадлежности, оценивающая, насколько данный исторический артефакт соответствует указанной при поиске дате или интервалу. Поиск по промежутку основан на определении площадей пересечения функций принадлежности и искомого промежутка. Приводя пример общего случая, значения площади пересечения функций принадлежности может задаваться следующей формулой:

$$f_{\tau(x,y,a,b)} = \left\{ \begin{array}{l} 0, x \leq y < a \leq b \cup a \leq b < x \leq y \\ \frac{y-a}{b-x}, x < a \leq y \leq b \\ \frac{b-x}{y-a}, a \leq x \leq b < y \\ \frac{y-x}{b-a}, a < x \leq y < b \\ \frac{b-a}{y-x}, x \leq a \leq b \leq y. \end{array} \right\}, \quad (1)$$

где x, y – некоторые числовые параметры, соответствующие поисковому промежутку, a, b – некоторые числовые параметры, соответствующие промежутку нечеткой даты артефакта, причем параметры должны быть упорядочены отношением: $x \leq y, a \leq b$.

После получения итоговой модели необходимо реализовать программный компонент, решающий главную задачу исследования. В первую очередь для этого необходимо выбрать архитектуру приложения, а также решить, какая будет структура хранения и получения необходимых данных.

Правильная архитектура программы играет ключевую роль в разработке сложных программных систем. Под архитектурой программы подразумевается структура, организация и взаимодействие ее компонентов. Выбор архитектурного стиля оказывает существенное влияние на расширяемость и масштабируемость приложения. Это поможет сократить затраты на обслуживание и развитие системы в долгосрочной перспективе. Мы остановили свой выбор на Чистой Архитектуре (*Clean Architecture*), концепция которой представлена на рис. 1.

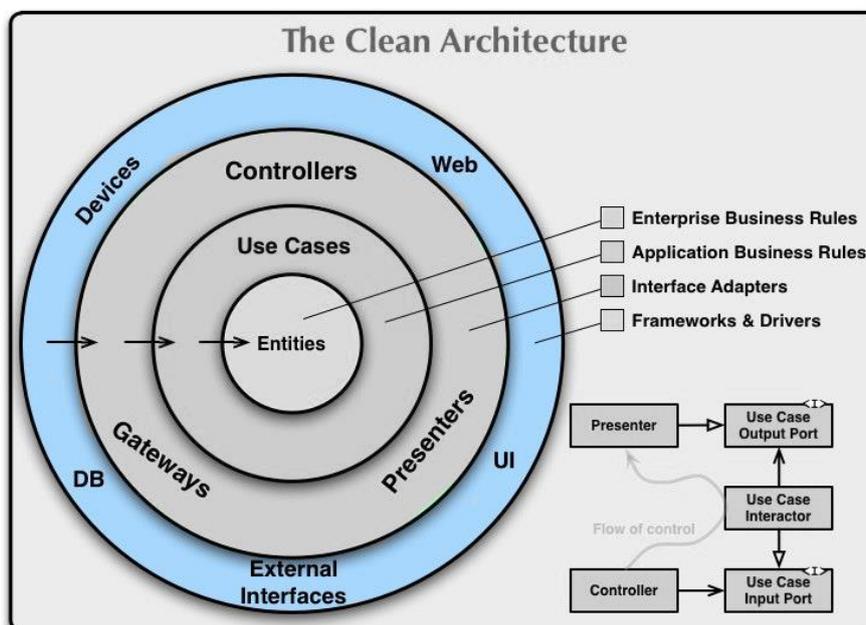


Рис. 1. Модель Чистой Архитектуры

Слой *Entity* представляет собой внутреннюю часть приложения, содержащую бизнес-сущности и бизнес-правила, независимые от каких-либо внешних фреймворков или интерфейсов [1]. Тут располагаются бизнес-сущности, описывающие ключевые объекты предметной области, и бизнес-правила, определяющие логику их взаимодействия. Сущности в слое *Entity* не зависят от каких-либо внешних технологий, фреймворков или деталей реализации. Они представляют собой чистые модели бизнес-логики и остаются стабильными и устойчивыми к изменениям внешних аспектов системы, таких как пользовательский интерфейс или база данных.

Слой *Use Cases* представляет собой верхний уровень системы, ответственный за оркестрацию работы приложения и реализацию бизнес-кейсов.

Он фокусируется на бизнес-сценариях и взаимодействии системы с внешними элементами, такими как пользовательский интерфейс и инфраструктура. *Use Cases* служит мостом между внешним миром и внутренними компонентами, оставаясь независимым от деталей пользовательского интерфейса. В данном слое реализуются бизнес-функции и задачи, которые приложение должно выполнять для достижения бизнес-целей.

Слой *Interface Adapters* являются мостом между уровнями приложения и фреймворками, обеспечивая отвязку бизнес-правил от технических деталей внешних библиотек и фреймворков. *Interface Adapters* могут взаимодействовать с инфраструктурой, включая базы данных, веб-серверы и другие внешние ресурсы.

Слой *Frameworks & Drivers* зависит от интерфейсов, описанных в слое *Interface Adapters*, что позволяет достичь отделения бизнес-правил от любых деталей взаимодействия с внешними ресурсами. Логика данного слоя основана на реализации контрактов интерфейсов, аналогично принципу утиной типизации (*Duck Typing*).

Концепция передачи данных (*DTO - Data Transfer Object*) играет важную роль в архитектуре программных систем [2]. *DTO* может рассматриваться как оболочка или контейнер для передачи данных между различными слоями приложения, обеспечивая разделение ответственности и защиту от нежелательного доступа и изменения данных. Внутренняя логика приложения может изменять и обновлять данные в различных слоях, что может быть вызвано изменением состояния или выполнением бизнес-логики. В таком случае, если мы разрешим прямой доступ к данным между слоями, это может привести к нежелательным и непредсказуемым изменениям, которые затронут другие компоненты системы. Таким образом, при переходе между слоями для разделения ответственности необходимо реализовать дополнительную логику, представленную на рис. 2.

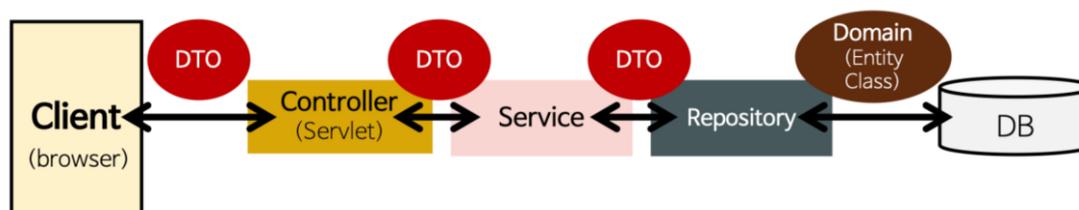


Рис. 2. Концепция Data Transfer Object

После выбора архитектуры необходимо решить, какие следует выбрать хранилища данных и структуры сущностей модели. В случае нашей системы было решено разделить логику для четко и нечетко датированных артефактов, так как в настоящий момент уделяется пристальное внимание повышению производительности систем [3].

Во-первых, данный подход позволит уменьшить нагрузку на хранилище, а также даст спектр возможностей для дальнейшей поддержки системы. Это позволит в любой момент при необходимости сменить хранилище или, наоборот, добавить другое к уже существующим. Помимо этого, это решение положительно влияет на скорость работы поиска в системе. Используя только лишь реляционную базу данных, пришлось бы либо хранить множество пустых полей, что является не самым эффективным и правильным решением, либо использовать формат данных *BSON* (*Binary JSON*). Последнее решение является неэффективным при большом количестве хранимых значений, так как *BSON* обычно занимает больше места, чем другие бинарные форматы из-за того, что используются дополнительные байты для хранения метаданных и типов данных, что может привести к увеличению размера. Также могут возникать сложности при миграции данных, потому что не все реляционные хранилища поддерживают данный формат.

Для нашей системы были выбраны две системы управления базами данных – реляционная *PostgreSQL* и документоориентированное *NoSQL* решение – *MongoDB*.

Для точно датированного исторического артефакта была выбрана реляционная база данных *PostgreSQL*. Предполагается, что для хранимой сущности будет задана вся необходимая информация вплоть до года. Такой вариант системы будет максимально целесообразным, если хранимый артефакт будет представлять точно датированное событие, к примеру, дату написания литературного произведения или известную дату постройки какого-либо исторического памятника.

MongoDB изначально спроектирован для работы с *JSON/BSON* форматами [4], поэтому работа с ними более эффективна и удобна.

Была выбрана структура, предполагающая наличие начала интервала и его конец. Без этих данных будет в любом случае невозможно ранжировать результаты, используя трапециевидную функцию принадлежности.

При желании описать хранимый объект с помощью конструкций «Примерно», «Приблизительно», либо же «Середина/ Начало/ Конец/ Первая половина Эры/ Века / Года / Десятилетия» предлагается использовать поле «*addition*», при наличии которого его значение будет выведено конечному пользователю. При этом функция принадлежности все равно отработает для интервалов, хранимых для определенного артефакта.

На рис. 3 приведен вариант реализации фильтра для *MongoDB*.

Предложенные подходы к архитектуре системы, структуре для хранения и получения данных и математическая основа могут быть применимы для разработки систем поиска и идентификации исторических артефактов, которые учитывают разную точность дат создания и позволяют пользователям находить необходимые данные с высокой степенью вероятности.

```
func SearchFilter(a, b int16) bson.M {
    filter := bson.M{
        "$or": []bson.M{
            {
                "start_date": bson.M{"$gte": a},
                "interval_end": bson.M{"$lte": b},
            },
            {
                "start_date": bson.M{"$lt": a},
                "interval_end": bson.M{"$gte": a, "$lte": b},
            },
            {
                "start_date": bson.M{"$lte": b, "$gte": a},
                "interval_end": bson.M{"$gt": b},
            },
            {
                "start_date": bson.M{"$lt": a},
                "interval_end": bson.M{"$gt": b},
            },
            {
                "start_date": bson.M{"$gte": a, "$lte": b},
            },
        },
    }
    return filter
}
```

Рис 3. Реализация фильтра для MongoDB

Список используемых источников:

1. Мартин Р. Чистая Архитектура. Искусство разработки программного обеспечения СПб.: Питер, 2024. 352 с.: ил. (Серия «Библиотека программиста»). ISBN 978-5-4461-0772-8.
2. Мартин Р. Чистый код: создание, анализ и рефакторинг. СПб.: Питер, 2019. 464с.: ил. ISBN 978-5-4461-0960-9.
3. Будко П. А., Линец Г. И., Мухин А. В., Фомин Л.А. Эффективность, цена и качество информационно-телекоммуникационных систем. Методы оптимизации. СПб: Военная академия связи, 2011. 420 с.
4. Брэдшоу Ш., Брэзил Й., Ходоров К. MongoDB: полное руководство. Мощная и масштабируемая система управления базами данных / пер. с англ. Д. А. Беликова. М.: ДМК Пресс, 2020. 540 с.: ил.

УДК 001.891.32
ГРНТИ 27.35.33

ОЦЕНКА УРОВНЯ ПОДГОТОВКИ СТУДЕНТОВ ПО РЕЗУЛЬТАТАМ ТЕСТИРОВАНИЯ С УЧЕТОМ ИХ ПСИХОФИЗИОЛОГИЧЕСКОГО СОСТОЯНИЯ

А. Н. Губин, В. Л. Литвинов, Е. А. Михайлова, Ф. В. Филиппов

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

В работе анализируются аспекты оценки уровня подготовки студентов с использованием тестирования, учитывая как качество тестовых заданий, так и психофизиологические факторы, влияющие на способности студентов. Рассматриваются математические модели и предлагается методика формирования оценки, учитывающая как сложность заданий, так и физиологические параметры студентов. Представленный метод позволяет более точно оценивать уровень подготовки студентов и может быть использован для оптимизации прогнозирования оценки студента при тестировании.

оценка уровня подготовки, математические модели тестирования, модель Раши, модель Бирнбаума, психофизиологические факторы

Для улучшения качества образовательных процессов в высшей школе обуславливает необходимость широкого применения тестовых форм контроля обучаемых [1].

Комплекс контрольных тестов обычно представляет собой структурированный набор задач, анализ результатов выполнения которых, позволяет измерить уровень учебных достижений студентов относительно всего спектра знаний, умений и навыков, которыми должны овладеть обучающиеся в результате реализации курса обучения по заданной дисциплине.

Оценка уровня подготовки студентов при тестировании существенно зависит как от качества тестовых заданий, включая их сложность [2], так и от совокупности психофизиологических факторов, влияющих на способности студентов к решению задач контрольных тестов [3].

В данном исследовании рассматривается решение задачи оценки уровня подготовки студента, на основе результатов тестирования с учетом сложности тестовых заданий и параметров психофизиологического состояния испытуемых.

Рассматривая вопросы оценки сложности конкретного тестового задания, необходимо учитывать форму представления тестового задания [2-4].

В общем случае сложность тестовой единицы δ_i можно оценить, как:

$$\delta_i = -N \cdot \sum_{i=1}^n p_i (\log p_i),$$

где N – общее количество ответов, предлагаемых в рассматриваемой тестовой единице, n – количество классов понятий, к которым относятся варианты предлагаемых ответов.

При этом вероятность p_i оценивается как отношение:

$$p_i = \frac{n_0}{N_i},$$

где n_0 – количество правильных ответов, N_i – количество предлагаемых ответов, относящихся к i -ому классу понятий, используемых в тестовой единице.

Предлагаемая форма оценки сложности тестовых единиц может быть использована практически для всех форм представления тестовых заданий.

Вероятность правильного ответа при тестировании студентов обычно моделируется логистической функцией, зависящей от разницы значений параметров уровня подготовки тестируемого и сложностью тестовой единицы. Математическая форма модели в данном случае получила наименование модели Раша [3-5] и имеет следующий вид:

$$P\{x_j = 1\} = \frac{e^{\theta_j - \delta_i}}{1 + e^{\theta_j - \delta_i}},$$

где $P\{x_i = 1\}$ – вероятность правильного ответа (функция успеха) на вопросы тестового задания, θ_j – уровень подготовки j -го студента, δ_i – сложность i -ой тестовой единицы.

Как правило, при использовании модели Раша и результатов оценки сложностей отдельных тестовых единиц можно получить выражение для определения обычно латентного значения уровня подготовки j -ого студента при решении i -ого тестового задания, которое имеет следующий вид:

$$\theta_j = \ln\left(\frac{P\{x_i = 1\}}{1 - P\{x_i = 1\}}\right) + \delta_i.$$

Однако данная модель не учитывает психофизиологическое состояние испытуемых во время прохождения тестирования, которое также влияет на результаты тестирования.

В работах [3, 6] предлагается математическая модель для прогнозирования оценки тестирования студентов, учитывающая факторы, такие как межэкзаменационный период, уровень интеллекта и частота сердцебиения:

$$R = \frac{0.6784*LT + 0.12675*IQ}{0.80515*P},$$

где R – прогнозируемая оценка тестирования студента, LT – длительность подготовки, IQ – оценка уровня интеллекта, P – частота пульса.

Однако в данном случае оценка результатов тестирования не учитывает сложности заданий теста.

Для решения задачи оценки уровня подготовки студента с учетом сложности тестов и психофизиологического состояния студента используем трехпараметрическую модель Бирнбаума [4-6]:

$$P\{x_j = 1\} = c_j + (1 - c_j) \frac{e^{\alpha_i(\theta_j - \delta_i)}}{1 + e^{\alpha_i(\theta_j - \delta_i)'}}$$

где c_j – коэффициент, учитывающий психофизиологического состояния j -го студента; α_i – коэффициент, определяющий дифференцирующее свойство модели.

Значение коэффициента c_i определим как:

$$c_j = \frac{1 - P\{x_i = 1\}}{R_j + 1},$$

где R_j – прогнозируемая оценка тестирования j -го студента с учетом его психофизиологического состояния.

Учитывая последние выражения, уровень подготовки испытуемого при решении конкретного тестового задания можно определить, как:

$$\theta_j = \frac{1}{\alpha_i} \left[\ln \left(\frac{P\{x_i = 1\} - c_j}{1 - P\{x_i = 1\}} \right) + \alpha_i \delta_i \right].$$

и далее:

$$\theta_j = \frac{1}{\alpha_i} \left[\ln \left(\frac{2P\{x_i = 1\} + R_j P\{x_i = 1\} - 1}{(1 + R_j)(1 - P\{x_i = 1\})} \right) + \alpha_i \delta_i \right].$$

Пример. В [2] получено решение задачи оценки сложности теста типа «множественный выбор» с одним правильным ответом, которое определяет $\delta_i = 2,11328$. Для данного теста, при реализации функции успеха $P\{x_i = 1\} = 0,9$, $\alpha_i = 1$ и $R = 0,6$, уровень подготовки испытуемого определяется как:

$$\theta_j = \left[\ln \left(\frac{1,8 + 0,6 \cdot 0,9 - 1}{(1 - 0,9)(1 + 0,6)} \right) + 2,11328 \right] = 4,235.$$

Если функция успеха составляет $P\{x_i = 1\} = 0,5$, то оценка уровня подготовки определится как $\theta_j = 1,129$.

Для оценки динамики поправок, учитывающих психофизиологическое состояние студента, рассмотрим графики (рис.1) зависимости θ_j от значений

функции успеха $P\{x_i = 1\}$ для i -го тестового задания с учетом и без учета психофизиологического состояния студента.

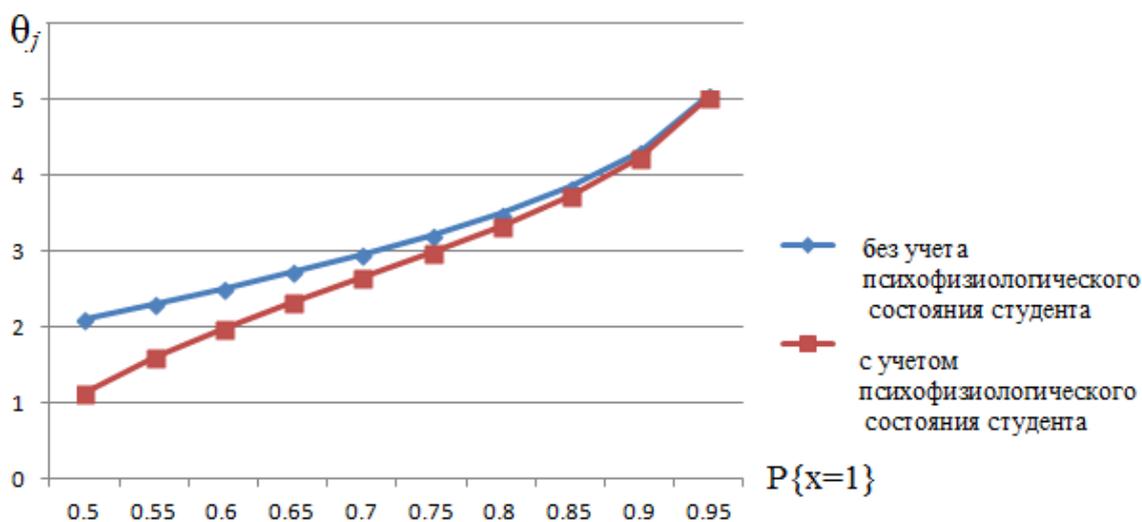


Рис. 1. Уровень подготовки испытуемых с учетом и без психофизиологического состояния студента

Из графика видно, что при низких значениях функции успеха ($P\{x = 1\} = 0,5$), разница между оценками уровня подготовки студентов составляет 78 %. При увеличении значений функции ($P\{x = 1\} = 0,95$) успеха разница между оценками уровня подготовки падает до значения 0,6 %. То есть, для студентов с низким уровнем значений функции успеха (при низкой теоретической подготовке) при ухудшении самочувствия наблюдается существенное снижение значения оценки уровня подготовки по изучаемой дисциплине. В случае высокого уровня подготовки студента влияние самочувствия на оценку уровня подготовки оказывается незначительным. Использование рассмотренного метода оценки уровня подготовки испытуемых, основанного на базе динамического вычисления уровня подготовки обучающихся с учетом психофизиологического состояния студента, позволит в дальнейшем совершенствовать стратегию тестирования и получать более адекватные результаты проверки знаний.

Список используемых источников

1. Аванесов В. С. Научные проблемы тестового контроля знаний. М., 1994.
2. Губин А. Н., Литвинов В. Л., Филиппов Ф. В. Методы анализа и оценки сложности тестовых заданий фондов оценочных средств дисциплины // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. С. 149–151.
3. Райт, Б. Д. (1977). Решение задач измерения с помощью модели Раша. Журнал педагогических измерений, 14 (2), 97-116.
4. Нейман Ю. М., Хлебников В. А. Введение в теорию моделирования и параметризации педагогических тестов. М.: Прометей, 2000.

5. Губин А. Н., Михайлова Е. А. Влияние внешних факторов на успеваемость студентов при прохождении тестирования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ. 2023. Т. 2. С. 590–593.

6. Математическое моделирование психофизиологических факторов успешности обучения студентов первого курса медицинского вуза по дисциплине «биофизика» / Н. И. Колосова, М. А. Лопарева, Е. Н. Денисов и др.. Текст: непосредственный // Молодой ученый. 2017. № 22(156). С. 168–170.

УДК 004.94
ГРНТИ 28.17.31

ИМИТАЦИОННАЯ МОДЕЛЬ ПРОЦЕССА ЗАГРЯЗНЕНИЯ АТМОСФЕРНОГО ВОЗДУХА ДЛЯ МОНИТОРИНГА ЭКОЛОГИЧЕСКОЙ ОБСТАНОВКИ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Предложен способ мониторинга экологической обстановки в городской среде путем применения имитационной модели процесса загрязнения атмосферного воздуха, учитывающей ряд факторов, оказывающих негативное воздействие на окружающую среду. Проведена математическая формализация модели процесса загрязнения атмосферного воздуха. Для создания имитационной модели использована среда моделирования AnyLogic, поддерживающая методы системной динамики. Проведен ряд экспериментов варьирования параметров входных данных, которые позволили сделать прогнозы о факторах, оказывающих наибольшее влияние на экологическую обстановку в городе.

имитационное моделирование, системная динамика, экологический мониторинг, AnyLogic

При проектировании экологических систем применяются методы системного анализа, в первую очередь, для выделения отдельных структурных элементов. Другой важной задачей при реализации системного подхода является установление характера динамических процессов, в которых принимают участия элементы экосистемы. Таким образом, при имитационном моделировании экосистем оправдано применение методов системной динамики [1].

В данной работе разработана математическая модель процесса загрязнения атмосферного воздуха на примере города Луги. Предложенная модель рассматривает состав атмосферного воздуха и позволяет осуществлять мониторинг за его состоянием.

В настоящем исследовании мониторинг состояния атмосферного воздуха будет осуществляться по ряду загрязняющих веществ, наиболее часто вырабатываемых в различных источниках загрязнения (табл. 1).

Все источники загрязнения атмосферного воздуха в городе Луга, выбранном в качестве объекта моделирования, можно разделить на две крупные группы: выбросы от автомобильного транспорта и выбросы из источников загрязнения на предприятиях. Таким образом, на территории города Луги выявлены следующие факторы, оказывающие негативное воздействие на атмосферный воздух:

- выбросы от предприятия ОАО «Лужский абразивный завод» (три площадки в разных частях города);
- выбросы от предприятия ООО «Лужский завод Белкозин»;
- выбросы от предприятия ОАО «Химик»;
- выбросы от автомобильного транспорта.

ТАБЛИЦА 1. Загрязняющие вещества и их фоновая концентрация

№	Вещество	Класс опасности	Фоновая концентрация, мг/м ³
1	Оксиды азота NO _x (в пересчете на NO ₂)	3	0,06
2	Оксид углерода CO	4	3
3	Сажа С	4	0,12
4	Фенол C ₅ H ₆ O	2	0,003
5	Диоксид серы SO ₂	3	0,06
6	Бенз(а)пирен	2	0,3
7	Фторид водорода HF	2	0,02
8.	Углеводороды CH	1	0,01
9.	Формальдегид CH ₂ O	2	0,01

В качестве основы для построения модели процесса загрязнения атмосферного воздуха использована модель системной динамики в среде AnyLogic [2] с главным агентом «Main». Всего в модели спроектировано четыре агента, включая «Main», «Вещество», «Завод» и «Транспорт» (рис. 1).

В агенте «Main» реализована диаграмма, отображающая состав выбросов загрязняющих веществ в атмосферный воздух, потоковый накопитель и два потока (рис. 2). В моделировании методом системной динамики накопитель представляет собой переменную величину, которая эквивалентна динамически изменяемому объему некоторого «вещества». В нашем случае потоковый

накопитель “Csum” характеризует концентрацию загрязняющих веществ в воздухе и с течением времени данное свойство меняет свот-значение.

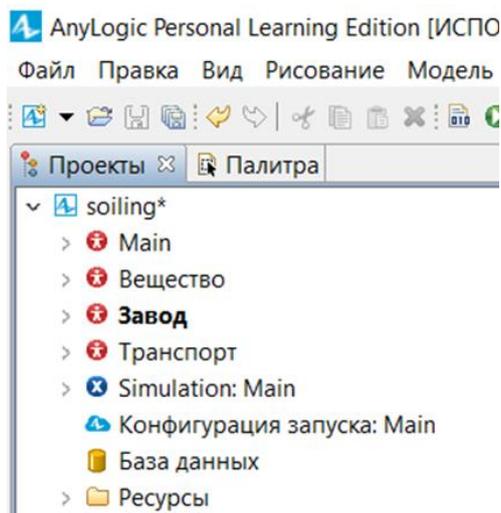


Рис. 1. Отображение структуры имитационной модели

Агент «Завод» содержит информацию о загрязнениях, стационарными источниками которых являются выбросы предприятий, расположенных на территории исследуемого города. Он состоит из динамических переменных, содержащих данные о выбросах загрязняющих веществ от источников на предприятиях, и параметров с постоянным значением (рис. 3).

Динамические переменные используются для описания всех расчетных величин, к которым относятся массы валового выброса загрязняющих веществ, расход газовой смеси, а также расчетные коэффициенты, используемые для вычисления расхода газовой смеси.

Аналогично создаются Агент «Транспорт», предназначенный для расчета загрязняющих веществ от автотранспорта, и агент «Вещество», предназначенный для подсчета суммарной концентрации загрязняющих веществ в атмосферном воздухе в городе с учетом выбросов от всех источников загрязнения и рассеивания вредных веществ.

Спроектированная в системе моделирования AnyLogic имитационная модель процесса загрязнения атмосферного воздуха позволяет оценить экологическую обстановку в городе. Кроме того, благодаря пользовательскому интерфейсу, она позволяет провести эксперимент с варьированием данных, изменение которых может сказываться на загрязнении атмосферного воздуха. На основе модели также строится круговая диаграмма, на которой в наглядном виде представляется информация о составе выбросов вредных веществ.

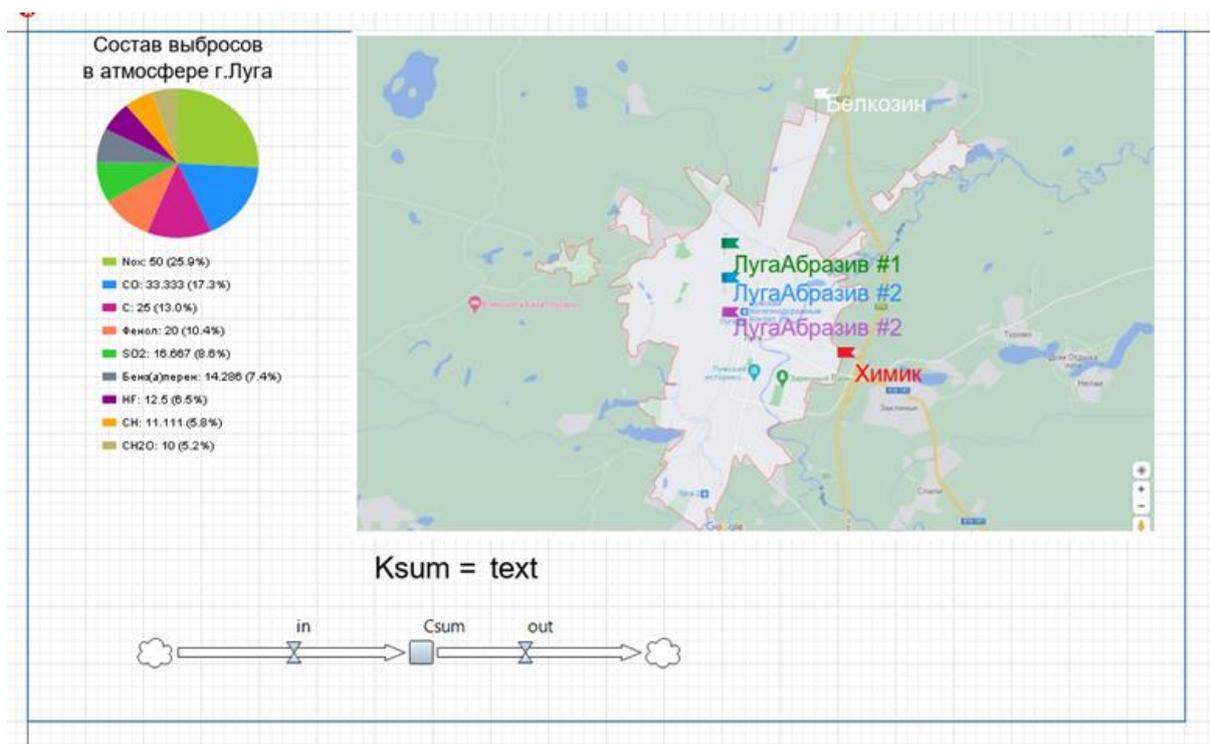


Рис. 2. Структура агента «Main»

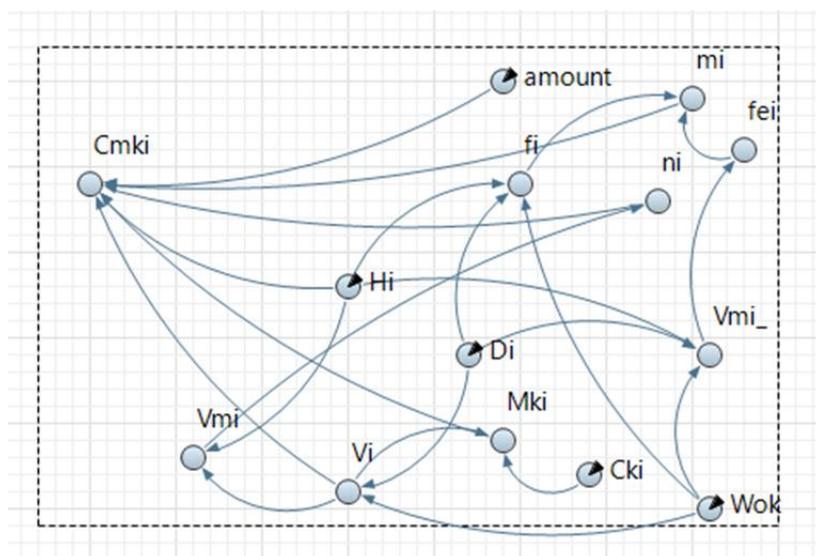
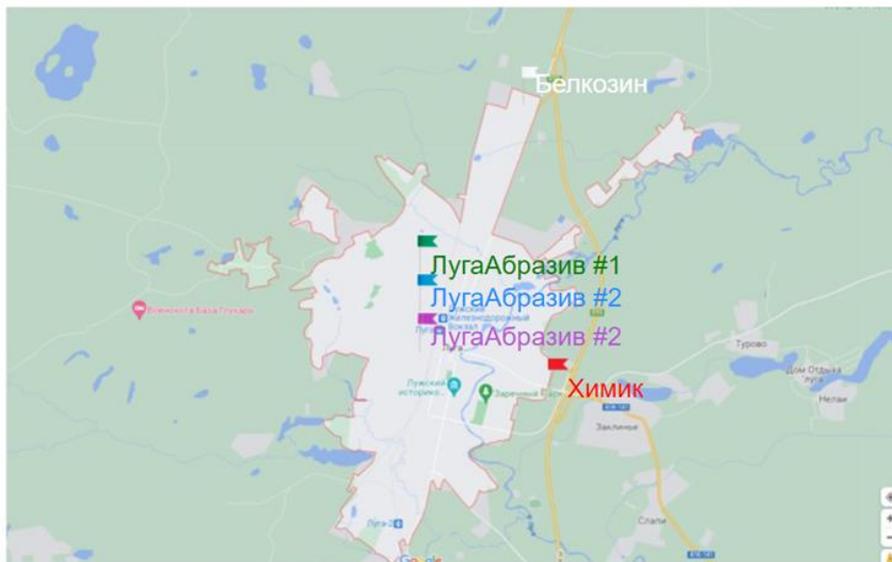
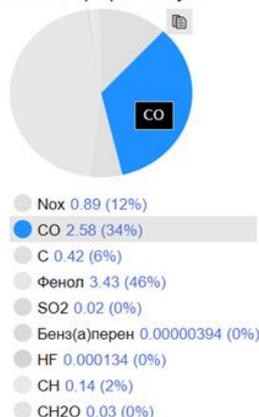


Рис. 3. Структура агента «Завод»

Рассмотрим два эксперимента с варьированием данных с целью прогнозирования, как может измениться экологическая обстановка. В первом случае при снижении интенсивности автотранспортного потока, во втором – в случае сокращения выбросов фенола в окружающую среду.

Для проведения первого эксперимента был произведен расчет выбросов загрязняющих веществ при интенсивности потока, уменьшенного на 50 % в сравнении с исходными данными. Результаты эксперимента представлены на рис. 4.

Состав выбросов
в атмосфере г. Луга

$$K_{sum} = 1.656$$



Рис. 4. Результат расчета выброса загрязняющих веществ в атмосферный воздух при снижении интенсивности автотранспортного потока на 50 %

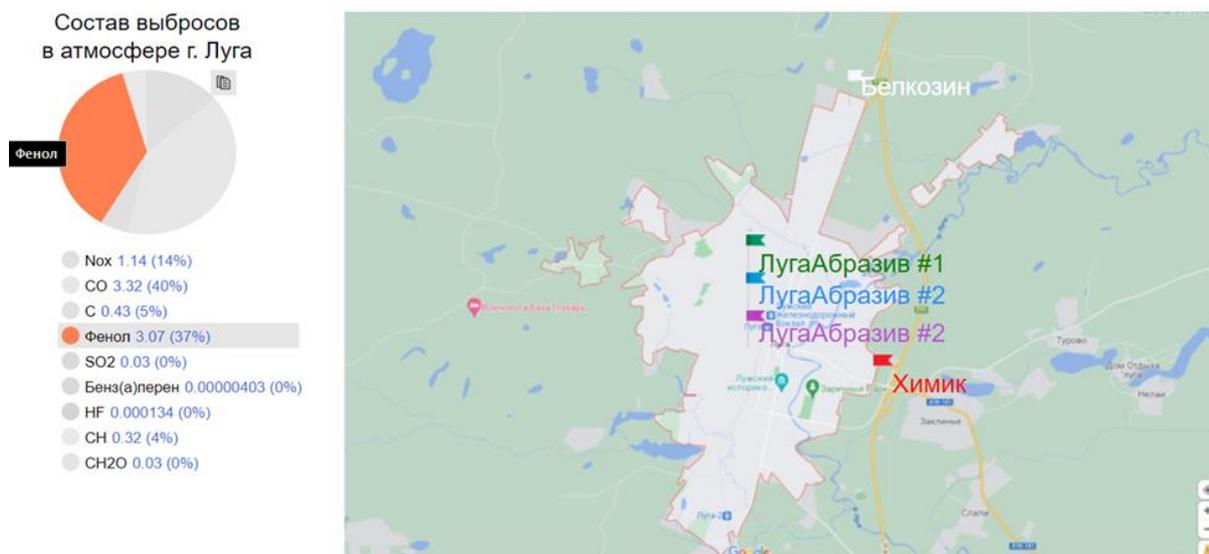
Из диаграммы видно, что вклад оксидов углерода в состав выбросов снизился всего на 4 % (с 38 % до 34 %). Кроме того, снижение значения коэффициента суммарного загрязнения в таком случае является незначительным, и экологическая обстановка по-прежнему остается неблагоприятной.

Во втором эксперименте была снижена масса выброса фенола на площадке № 1 абразивного завода с $0,97 \text{ г/м}^3$ до $0,77 \text{ г/м}^3$ (рис. 5).

На круговой диаграмме видно, что вклад фенола снизился не столь существенно, с 39 % до 37 %. При этом наблюдается снижение коэффициента суммарного загрязнения более, чем в два раза и достижение нормальной экологической обстановки в городе. Это свидетельствует о том, что выбросы фенола являются критически важным фактором для экологической обстановки в городе.

Проведенные эксперименты позволили выявить, что, во-первых, текущая экологическая обстановка требует принятия мер для нормализации ситуации. Во-вторых, было выявлено, что наибольший вклад в загрязнение атмосферного воздуха вносят выбросы фенола от производственных площадок абразивного завода, расположенных в черте города.

Таким образом, использование методов имитационного моделирования является эффективным в оценке экологической обстановки и помогает строить прогнозы изменения экологической ситуации вследствие изменения различных факторов, таких как объемы производственных мощностей, интенсивность транспортного движения, а также внедрения новых технологических процессов.



$$K_{sum} = 0.872$$



Рис. 5. Результат расчета выброса загрязняющих веществ в атмосферный воздух при снижении выброса фенола

Список используемых источников

1. Данилов-Данильян В. И., Митина Н. Н., Малашенков Б. М. Экология: учебник и практикум для академического бакалавриата. М.: Юрайт, 2018. 363 с.
2. Карпов Ю. Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. СПб.: БХВ-Петербург, 2019. 400 с.

УДК 004.4: 530.145
ГРНТИ 28.23.25

ГРАДИЕНТНЫЕ МЕТОДЫ ОБУЧЕНИЯ ПАРАМЕТРИЗОВАННЫХ КВАНТОВЫХ СХЕМ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Исследуются вопросы обучения моделей на основе квантовых схем с использованием градиентных методов. Рассматриваются особенности использования аналитических градиентов для оптимизации параметров вариационной схемы. Показано влияние чувствительности модели на выбор метрики при вычислении градиентов. Приводится сравнение простой стохастической аппроксимации одновременных возмущений с естественным градиентом, основанным на квантовой информации Фишера. Оцениваются затраты на реализацию различных подходов в зависимости от количества параметров модели и скорости обучения.

машинное обучение, градиенты, параметризованные квантовые схемы, оптимизация параметров

Параметризованные квантовые схемы (ПКС), в которых гейты определяются посредством настраиваемых параметров, являются фундаментальным строительным блоком алгоритмов квантового машинного обучения. В [1] исследуется большой набор шаблонов ПКС с различной мерой *выразимости* и *способности запутывания*, используемых в гибридных квантово-классических алгоритмах. Для ряда из этих шаблонов в библиотеке *qiskit* разработаны функции для формирования ПКС, состоящих из чередующихся слоев однокубитных гейтов вращения, за которыми следуют двухкубитные управляемые гейты. Например, на рис. 1 представлены ПКС, построенные с использованием функций *RealAmplitude* и *TwoLocal* для двух кубит с двумя чередующимися слоями.

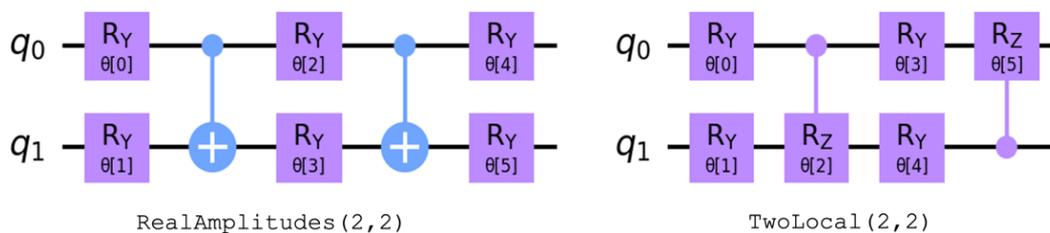


Рис. 1. Параметризованные двухкубитные квантовые схемы

Подобная процедура построения схем кодирует N характеристик как вращения на N параметризованных гейтах на n кубитах и использует квантовую схему постоянной глубины. ПКС, построенные с использованием этой процедуры на практике, показали наибольшую эффективность.

Как и классические модели, мы можем обучать ПКС выполнять задачи, управляемые данными, представленными вектором параметров $\vec{\theta}$. Задача обучения формально выражается как минимизация функции потерь $f(\vec{\theta})$. Для ПКС в роли этой функции выступает математическое ожидание $\langle \Psi(\vec{\theta}) | \hat{H} | \Psi(\vec{\theta}) \rangle$, где $\Psi(\vec{\theta})$ – параметризованное квантовое состояние, а \hat{H} – гамильтониан [2].

Пусть, у нас есть функция потерь $f(\vec{\theta})$ и метод вычисления градиента функции $\vec{\nabla} f(\vec{\theta})$, начиная с некоторой начальной точки. Классическим способом минимизации функции является обновление параметров $\theta_1, \theta_2, \dots$ в направлении наибольшего спуска функции: $\vec{\theta}_{n+1} = \vec{\theta}_n - \eta \vec{\nabla} f(\vec{\theta})$, где η скорость обучения – гиперпараметр для контроля величины обновления. Этот метод называется *градиентным спуском*. Параметризованное состояние формируется в виде некоторой ПКС $U(\vec{\theta})$ с необходимым числом параметров. В общем виде его можно записать как $|\Psi(\vec{\theta})\rangle = U(\vec{\theta})|00 \dots 0\rangle$. Для расчета градиентов на основе ПКС, состоящей только из вращений Паули, в [3] предложена простая формула:

$$\frac{\partial f}{\partial \theta_i} = \frac{f\left(\vec{\theta} + \frac{\pi}{2} \vec{e}_i\right) - f\left(\vec{\theta} - \frac{\pi}{2} \vec{e}_i\right)}{2},$$

мы будем использовать эту формулу при расчете простых градиентов.

Следует отметить, что простой градиентный спуск не всегда является лучшей стратегией. В [4] реализована идея натуральных градиентов состоящая в том, чтобы изменить способ определения θ_{n+1} из θ_n , учитывая чувствительность модели. В простом градиенте используется евклидово расстояние $d_e = \|\vec{\theta}_{n+1} - \vec{\theta}_n\|_2$, которое не учитывает особенности модели ПКС. При использовании натуральных градиентов вместо этого используется расстояние, которое зависит от модели:

$$d_g = \|\langle \Psi(\vec{\theta}_n) | \Psi(\vec{\theta}_{n+1}) \rangle\|^2 = \|\vec{\theta}_n - \vec{\theta}_{n+1}\|_{g(\vec{\theta})},$$

– эта метрика называется квантовой информацией Фишера $g_{ij}(\vec{\theta})$. Расстояние между двумя бесконечно близкими точками на статистическом дифференциальном многообразии является информационным различием между ними:

$$g_{ij}(\vec{\theta}) = Re \left\{ \left\langle \frac{\partial \Psi}{\partial \theta_i} \middle| \frac{\partial \Psi}{\partial \theta_j} \right\rangle - \left\langle \frac{\partial \Psi}{\partial \theta_i} \middle| \Psi \right\rangle \left\langle \Psi \middle| \frac{\partial \Psi}{\partial \theta_j} \right\rangle \right\}.$$

Интуитивно понятно, что чем более резко изменяется функция потерь $f(\vec{\theta})$ в зависимости от θ , тем больше «информации» содержится в измерениях. Вблизи оценки максимального правдоподобия низкая информация Фишера указывает, что максимум является неглубоким и имеется много близких значений, а высокая информация Фишера указывает на резкость максимума.

На основе квантового натурального градиента вычисление θ_{n+1} из θ_n выполняется по формуле:

$$\vec{\theta}_{n+1} = \vec{\theta}_n - \eta g^{-1}(\vec{\theta}) \vec{\nabla} f(\vec{\theta}_n).$$

Для вычисления натурального градиента в библиотеке *qiskit* имеется функция *NaturalGradient()*. Как показано в [4], квантовый натуральный градиент приближается к цели существенно быстрее, чем в случае с простым градиентным спуском.

В качестве следующей модернизации методов обучения ПКС следует рассмотреть метод оптимизации *SPSA* (*Simultaneous Perturbation Stochastic Approximation*), стохастическая аппроксимация одновременных возмущений [4]. *SPSA* – это метод оптимизации, при котором градиент выбирается случайным образом, для того, чтобы уменьшить количество оценок:

$$\vec{\nabla} f(\theta) = \begin{pmatrix} \frac{\partial f}{\partial \theta_1} \\ \vdots \\ \frac{\partial f}{\partial \theta_n} \end{pmatrix} \cong \frac{1}{2\varepsilon} \begin{pmatrix} f(\vec{\theta} + \varepsilon \vec{e}_1) - f(\vec{\theta} - \varepsilon \vec{e}_1) \\ \vdots \\ f(\vec{\theta} + \varepsilon \vec{e}_n) - f(\vec{\theta} - \varepsilon \vec{e}_n) \end{pmatrix} \cong \frac{f(\vec{\theta} + \varepsilon \vec{\Delta}) - f(\vec{\theta} - \varepsilon \vec{\Delta})}{2\varepsilon} \vec{\Delta}^{-1}.$$

Поскольку нас не волнуют точные значения, а только сходимость, несмещенная выборка в среднем должна работать одинаково хорошо. Как показано в [5], *SPSA* будет прыгать из-за случайной выборки, но будет сходиться при тех же граничных условиях, что и простой градиент. Для реализации этого метода в библиотеке *qiskit* имеется функция *SPSA()*.

Аналогичную процедуру можно проделать и для натуральных градиентов, распространив случайную выборку не только на градиент, но и на квантовую информацию Фишера. Данная процедура реализована в *qiskit* с помощью функции *QNSPSA()*.

Используя указанные функции библиотеки *qiskit*, исследуем различия в минимизации потерь при использовании различных градиентов и способов оптимизации для двух шаблонов *RealAmplitude* и *TwoLocal*. Как видно из рис. 2, характер графиков для различных шаблонов отличается мало. Существенным отличием в обоих случаях является более быстрое достижение целевого значения при использовании квантового натурального градиента.

Кривая потерь метода оптимизации *SPSA* (и *QNSPSA*) выглядит не так гладко, как для простого градиента, но не влияет на скорость сходимости.

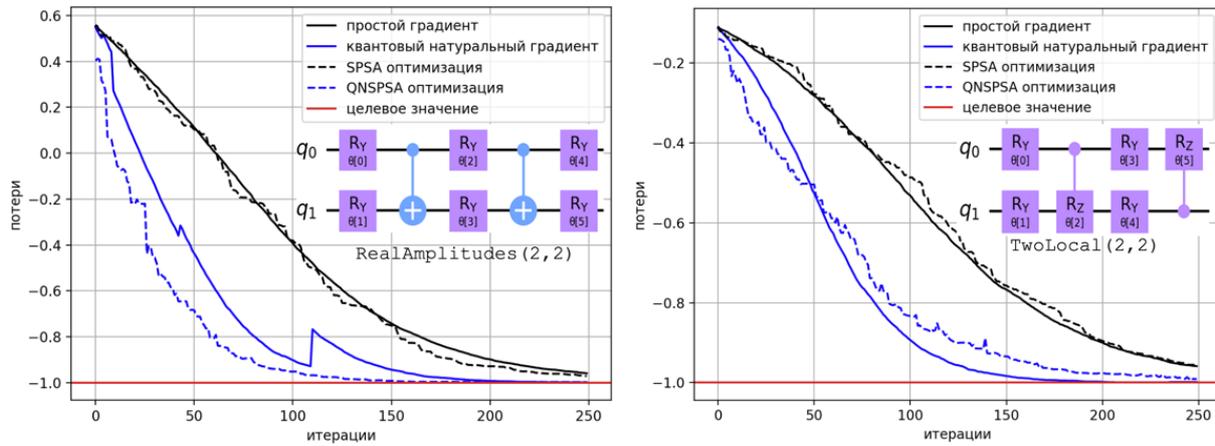


Рис. 2. Графики функции потерь для четырех градиентов двухкубитных схем

Рассмотрим, как изменится кривая потерь при увеличении числа кубитов в ПКС при том же количестве оптимизируемых параметров. Для этого возьмем однослойные трехкубитные схемы, также построенные с использованием функций *RealAmplitude* и *TwoLocal*. Графики функций потерь (рис. 3) показывают, что заметных изменений не произошло, за исключением того, что существенно изменились кривые для схемы *TwoLocal*, где натуральный градиент значительно быстрее достигает целевого значения.

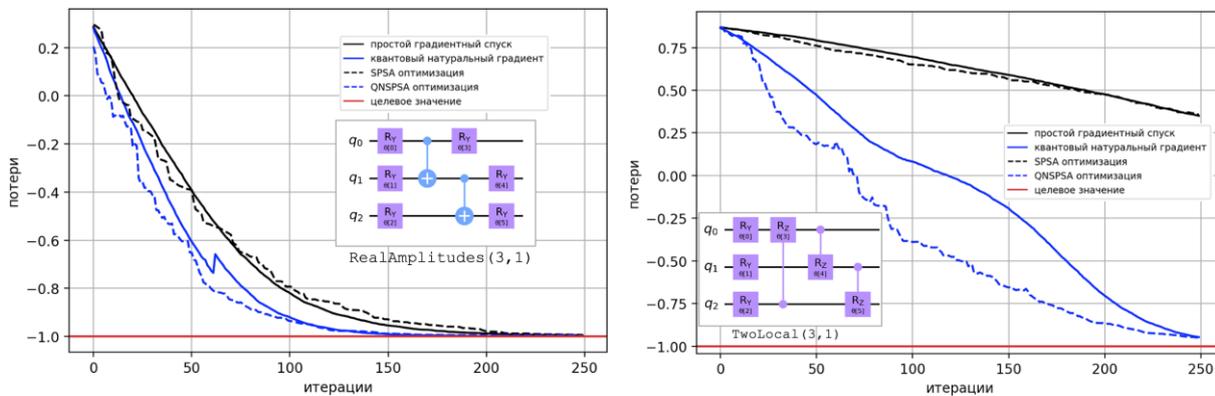


Рис. 3. Графики функции потерь для четырех градиентов трехкубитных схем

Данные на графиках функции потерь (рис. 3 и 4) получены при фиксированной скорости обучения $learning_rate = 0,05$. Функции *SPSA()* и *QNSPSA()* в качестве входного параметра скорости обучения $learning_rate$ позволяют задавать значение *None*, при этом скорость автоматически меняется в соответствии с моделью ПКС. Чтобы улучшить сходимость, алгоритмы стохастической аппроксимации используют не постоянную скорость обучения, а экспоненциально убывающую.

Посмотрим, как скажется это изменение на процессе оптимизации параметров в простейшем случае для двухкубитных схем. Для наглядности оставим на графиках рис. 4 кривые испытаний с фиксированной скоростью обучения и дополним их результатами стохастической аппроксимации с варьируемой скоростью (*var_rate*). Следует отметить, что, когда наряду со стохастической аппроксимацией дополнительно используется квантовый натуральный градиент, наблюдаются большие прыжки, обусловленные случайной выборкой. Тем не менее, это не оказывает влияния на ход процесса оптимизации. Результаты испытаний показывают, что вне зависимости от топологии схемы стохастическая аппроксимация гораздо быстрее справляется с решением задачи оптимизации в достижении целевого значения.

Здесь отчетливо наблюдается преимущество алгоритмов стохастической аппроксимации с варьированием скорости обучения, позволяющих существенно сократить время обучения. По крайней мере, это справедливо для квантовых схем с небольшим числом оптимизируемых параметров. Чтобы проверить преимущество алгоритмов оптимизации с варьированием скорости обучения был проведен эксперимент для квантовых схем на пяти кубитах. На рис. 5 представлены результаты эксперимента для ПКС построенной с использованием функций *RealAmplitude* и *TwoLocal* для пяти кубит с двумя чередующимися слоями, которые включают 15 и 20 настраиваемых параметров, соответственно.

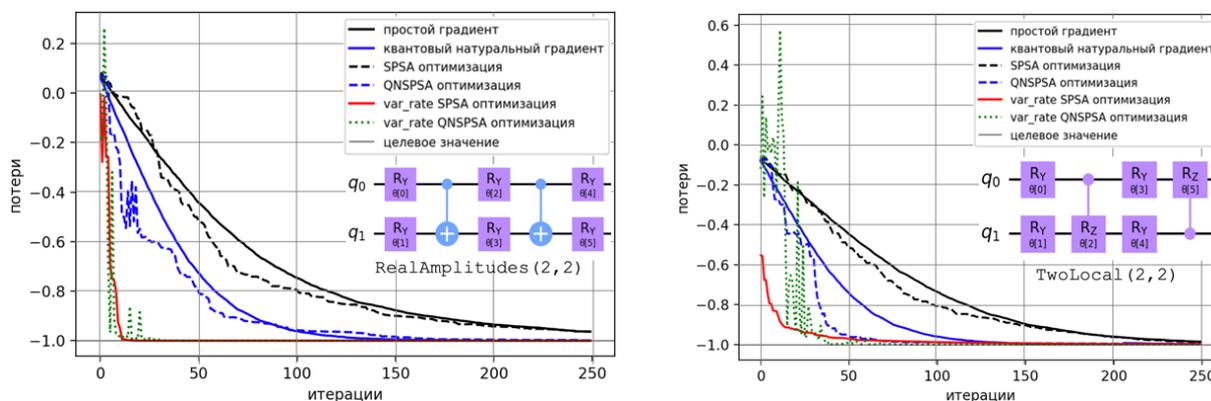


Рис. 4. Графики функции потерь с добавлением стохастической оптимизации

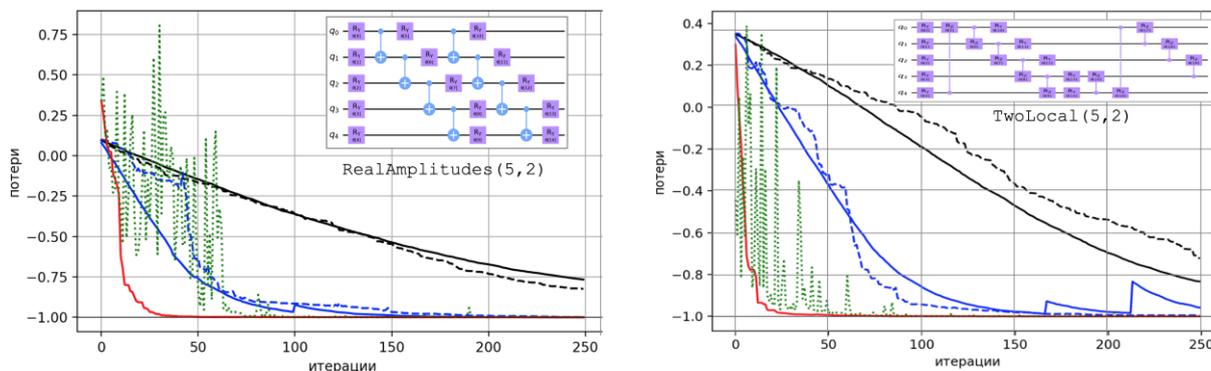


Рис. 5. График потерь при обучении параметризованной пятикубитной квантовой схемы

Данный результат отчетливо демонстрирует преимущество метода оптимизации *SPSA* с варьированием скорости обучения (красная линия). Квантовый натуральный градиент *QNSPSA* с использованием стохастической аппроксимации показывает сравнимый результат.

Список используемых источников

1. Sim S., Johnson P. D., Aspuru-Guzik A. Expressibility and entangling capability of parameterized quantum circuits for hybrid quantum-classical algorithms // *Advanced Quantum Technology*. 2019. № 2. P. 1900070. arXiv:1905.10876.
2. [https://ru.wikibrief.org/wiki/Variational_method_\(quantum_mechanics\)](https://ru.wikibrief.org/wiki/Variational_method_(quantum_mechanics)) (дата обращения 17.01.2024).
3. Schuld M., Bergholm V., Gogolin C., Izaac J. and Killoran N. Evaluating analytic gradients on quantum hardware // *Physical Revview*. 2019. A 99. P. 032331. arXiv:1811.11184.
4. Stokes J., Izaac J., Killoran N. and Carleo J., Quantum Natural Gradient // *Quantum*. 2020. 4. P. 269. arXiv:1909.02108.
5. Gacon J., Zoufal C., Carleo G. and Woerner S. Simultaneous Perturbation Stochastic Approximation of the Quantum Fisher Information. arXiv:2103.09232.

УДК 004.94
ГРНТИ 50.47.31

МОДЕЛИРОВАНИЕ ГИБКОГО ПРОИЗВОДСТВЕННОГО МОДУЛЯ НА ОСНОВЕ РАСКРАШЕННОЙ СЕТИ ПЕТРИ

И. Н. Дорофеев, А. Г. Любимов

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

В статье рассматривается гибкий производственный модуль, включающий накопитель, промышленный робот и технологическое станочное оборудование. Управление гибким производственным модулем осуществляется от локальной системы управления. В состав системы управления, в общем случае, могут входить система числового программного управления технологического оборудования и система управления промышленным роботом. Моделирование модулем выполнено с помощью раскрашенной сети Петри, учитывающей гибкость обработки изделий с разными технологическими характеристиками в рамках единого технологического процесса. Разработанная модель раскрашенной сети Петри позволяет описать структуру управляющей программы гибкого производственного модуля.

гибкий производственный модуль, локальная система управления, раскрашенная сеть Петри

Специфичность современных задач автоматизации производства заключается в учете углубляющегося разделении труда и технологической специализации, что характерно для мелкосерийных и серийных производств. Разработка и внедрение гибких автоматизированных систем (ГПС) позволяет решать задачи автоматизации такого рода производств [1]. Гибкость производства предусматривает быструю перестройку станочного оборудования на обработку деталей с различными конструктивными характеристиками в рамках одного технологического процесса.

Гибкая производственная система представляет собой управляемую средствами вычислительной техники совокупность технологического оборудования, автоматизированной системы технологической подготовки производства и системы обеспечения функционирования, обладающая свойством автоматизированной переналадки при изменении программы производства изделий [2]. Основной принцип организации ГПС – модульное построение, в соответствии с которым производство komponуется из отдельных типовых модулей и систем.

В качестве основного компоновочного элемента ГПС выступает гибкий производственный модуль (ГПМ). В механообрабатывающем произ-

водстве ГПМ представляет собой технологическое оборудование, автономно осуществляющее весь цикл работ, связанный с изготовлением или обработкой изделий.

В простейшей типовой комплектации ГПМ, как правило, включает: накопитель деталей и заготовок (стол-паллета), промышленный робот и станочное оборудование с магазином инструмента (рис. 1). Каждый компонент ГПМ оснащен собственной системой управления. Все системы управления компонентами объединены в локальную систему управления (СУ ГПМ).

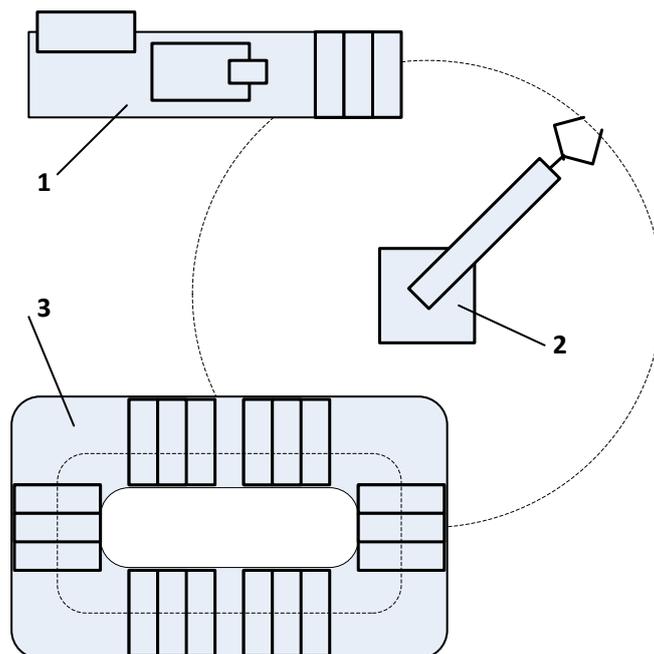


Рис. 1 Схема ГПМ: 1 – многофункциональный станок с ЧПУ и магазином инструмента; 2 – промышленный робот; 3 – накопитель заготовок и деталей (стол-паллета)

Взаимодействие компонентов осуществляется управляющей программой в СУ ГПМ. Для разработки управляющей программы необходимо учитывать следующие аспекты:

- определение процессов, выполняемых параллельно компонентами ГПМ;
- каждому процессу должна быть поставлена в соответствие собственная управляющая программа;
- определение условий и порядок вызова управляющих программ для каждого компонента.

С учетом указанных аспектов разрабатывается алгоритм управляющей программы СУ ГПМ. Для этих целей, как правило, выполняется моделирование технологического процесса для ГПМ. В качестве наиболее подходящего средства для моделирования распределенных систем и параллельных процессов используется математический аппарат сетей Петри [3, 4].

Показано, что сеть Петри представляет собой наглядную и хорошо формализованную модель описания дискретных динамических систем с параллельными процессами. Модель сети Петри обладает высоким уровнем абстракции и оперирует только двумя понятиями: *событие* и *условие*. В классической модели сети Петри события и условия представлены абстрактными символами из двух непересекающихся множеств, называемых соответственно множеством *переходов* T и множеством *позиций* P . В графическом представлении сетей Петри позиции обозначаются кружками (эллипсами), а переходы барьерами (прямоугольниками). Позиции (условия) и переходы (события) имеют отношения непосредственной зависимости, обозначаемые на графе направленными *дугами* E . Выполнение условий определяется *маркировкой* (*разметкой*) M , которая обозначается *метками* (*фишками*) в соответствующих позициях. Модель сети Петри формально представляется четверкой вида $\langle P, T, E, M_0 \rangle$, где M_0 соответствует начальной маркировке сети. Динамика поведения модели определяется *срабатыванием* переходов. Переход срабатывает, если выполнены все условия для наступления соответствующего события (во всех позициях, соединенных входными дугами с переходом имеется хотя бы одна метка). Срабатывание переходов приводит к изменению маркировки сети, что отражает динамику функционирования моделируемой системы. Классические сети Петри, как правило, применяются для моделирования простых технологических процессов. При моделировании сложных технологических процессов в гибких производственных системах приходится учитывать следующие основные ограничения применения классических сетей Петри:

- события (переходы) мгновенны во времени и не отражают реальные временные характеристики операционных циклов при обработке деталей с различными конструктивными параметрами;
- гибкость ГПМ предполагает необходимость переналадки общего станочного оборудования и разделения операций по множеству типов обрабатываемых деталей, что неизбежно приводит к формализации сложных параллельных процессов.

Для учета такого рода функциональных особенностей моделируемых систем применяются расширения классических сетей Петри (временные, раскрашенные и т.д.).

На рис. 2 представлена модель временной сети Петри, описывающая динамику функционирования ГПМ (рис. 1) для одного типа обрабатываемых деталей. Спецификация модели приведена в табл. 1.

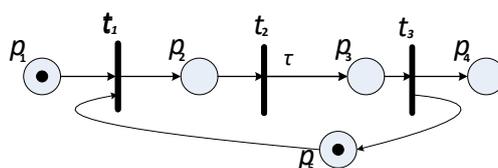


Рис. 2. Модель ГПМ в нотации временной сети Петри

ТАБЛИЦА 1. Спецификация модели временной сети Петри

Наименование позиций и переходов	Содержание
p_1	Деталь находится в накопителе
p_2	Деталь находится на рабочем столе станка
p_3	Технологическая операция на станке выполнена
p_4	Изделие выгружено на накопитель
p_5	Промышленный робот готов к загрузке следующей детали в станок
t_1	Программа робота по загрузке детали из накопителя в станок
t_2	Программа станка с ЧПУ по обработке детали
t_3	Программа робота по выгрузке изделия из станка в накопитель
τ	Время выполнения технологической операции на станке

Представленная модель позволяет разработать программу управления вызовами локальных программ в СУ ГПМ при условии, что для обрабатываемых деталей требуется выполнение одной и той же технологической операции. Вместе с тем, гибкость производственного модуля предусматривает возможность обработки деталей с различными конструктивными параметрами, в общем случае, в требуемой технологической последовательности. Следовательно, для множества N типов деталей необходимо разработать N моделей (рис. 2), соответственно. Кроме того, потребуется быстрая переналадка станка (выбор программы и установка инструмента) для обработки деталей соответствующего типа. Для моделирования процесса переналадки в моделях ГПМ требуется ввести дополнительные позиции и переходы. Очевидно, общая модель ГПМ в нотации классической сети Петри становится достаточно громоздкой.

Предлагается разработку управляющей программы в СУ ГПМ выполнять на основе моделей временных и раскрашенных (цветных) сетей Петри (РСП). В классических сетях Петри все метки являются одинаковыми. В ГПМ каждый тип деталей требует вызова только тех программ управления компонентами, которые соответствуют технологической операции обработки детали конкретного типа.

Предлагается каждому типу деталей, обрабатываемых в ГПМ, назначить метку определенного цвета. Цвет метки, как правило, должен отражать основные данные типа деталей и соответствующие им технологические операции. Применение нотаций РСП позволяет в модели ГПМ «раскрашивать» технологические операции, выполняемые на одном и том же многофункциональном станке в цвета, соответствующие каждому типу деталей. Переходы в модели РСП определяют отношения между

входными и выходными метками. Входные дуги переходов получают предусловия, которые определяют цвет метки для его запуска. Метка, находящаяся в позиции или переходе, раскрашивает его в соответствующий цвет, что означает в СУ ГПМ необходимые условия для вызова программы обработки для конкретного типа детали. На рис. 3 показана модель ГПМ в нотации раскрашенной сети Петри.

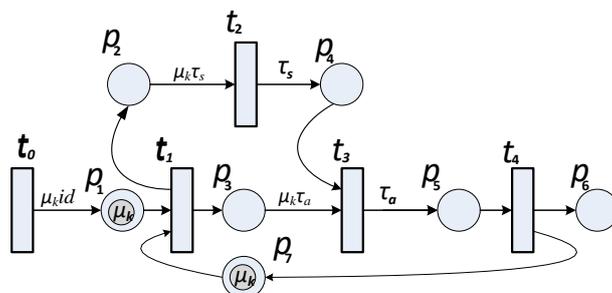


Рис. 3. Модель ГПМ нотации временной РСП

Отметим, что представление модели в нотации РСП компактно описывает динамику работы ГПМ. Раскраска меток позволяет показать обработку множества типов деталей на одном и том же оборудовании ГПМ. В общем случае, для k -го типа детали цвет метки определяет следующие данные ($\mu_k id$, $\mu_k \tau_s$, $\mu_k \tau_a$), где:

- $\mu_k id$ – идентификационный номер типа детали;
- $\mu_k \tau_s$ – параметр типа программы переналадки станка;
- $\mu_k \tau_a$ – параметр типа программы технологической операции;
- τ_s – время переналадки станка;
- τ_a – время выполнения технологической операции на станке.

Изображение переходов в виде прямоугольников подчеркивает тот факт, что каждый такой переход представляет множество действий (локальных программ) для обработки различных типов деталей. Спецификация модели приведена в табл. 2.

ТАБЛИЦА 2. Спецификация модели временной РСП

Наименование позиций и переходов	Содержание
p_1	Деталь k -го типа находится в накопителе
p_2	Требуется переналадка станка для k -го типа детали
p_3	Деталь загружена на рабочий стол станка
p_4	Переналадка закончится через время τ_s
p_5	Технологическая операция на станке выполнится через τ_a
p_6	Изделие k -го типа выгружено на накопитель
p_7	Промышленный робот готов к загрузке детали в станок

Наименование позиций и переходов	Содержание
t_0	Программа запуска обработки деталей всех типов
t_1	Программа работа по загрузке детали из накопителя в станок
t_2	Программа переналадки станка для обработки k -го типа детали
t_3	Программа станка с ЧПУ по обработке детали
t_4	Программа работа по выгрузке изделия из станка в накопитель

Список используемых источников

1. Выжигин А. Ю. Гибкие производственные системы: учебн. пособие. М.: Машиностроение, 2009. 288 с. ISBN 978-5-94275-434-1.
2. ГОСТ 26228-90. Системы производственные гибкие. Термины и определения, номенклатура показателей. Национальные стандарты. 1991. 11 с.
3. Котов В. Е. Сети Петри. М.: Наука, 1984. 160 с.
4. Питерсон Дж. Теория сетей Петри и моделирование систем: пер. с англ. М.: Мир, 1984. 264 с.

УДК 004.031
ГРНТИ 20.51.19

ПРИМЕНЕНИЕ WEB-ТЕХНОЛОГИЙ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ОБЪЕКТАМИ

Д. И. Евсеев, А. Г. Любимов, Н. А. Чебыкин

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

В работе рассматриваются подходы и решения разработки распределённых систем контроля и управления технологическими процессами и объектами на основе SCADA систем и технологий промышленного Интернета вещей. В качестве перспективных направлений организации удаленного доступа в системах контроля и управления показаны применение пользовательских приложений с использованием мобильных средств телекоммуникаций и web-браузеров, на основе web-ориентированных SCADA систем, а также полнодуплексного протокола WebSocket для управления технологическими процессами и объектами в реальном масштабе времени.

распределенная система контроля и управления, web-технологии, протокол WebSocket, WebScada система

Современные тенденции в организации автоматизированных производств направлены в сторону удалённого мониторинга и управления технологическими процессами и объектами, которые в свою очередь могут находиться на значительном удалении друг от друга. Такого рода системы контроля и управления рассматриваются как распределенные системы. Одной из основных характеристик распределенных систем принято считать способ [1], при помощи которого пользователи и объекты взаимодействуют между собой независимо от того, где и когда происходит такое взаимодействие. При этом, независимо от способов и технологий удаленного взаимодействия пользователей и объектов, в распределенных промышленных системах автоматизированного управления такое взаимодействие организуется с применением технологий SCADA систем [2]

В промышленном производстве SCADA представляет собой программный продукт, предназначенный для обеспечения работы в реальном масштабе времени систем мониторинга (сбора, обработки, отображения и архивирования) и управления технологическими процессами и объектами. SCADA-системы соответствуют третьему уровню промышленной автоматизации и обеспечивают функции диспетчерского управления и сбора данных в системах автоматизированного управления технологическими процессами (АСУТП). Основное назначение SCADA-системы заключается в выполнении функций агрегации данных и управления устройствами ниж-

него уровня и обеспечения взаимодействия с уровнем операторского управления. Построение систем контроля и управления на основе классического подхода к построению АСУ ТП, как правило, основывается на использовании технологий промышленных сетей (Ethernet, Modbus, Profibus и т.п.) В настоящее время на рынке промышленной автоматизации представлен достаточно широкий набор SCADA-систем разработки и исполнения различных производителей. Разнообразие представленных производителями контроллеров и собственно SCADA продуктов требует использования соответствующих драйверов. Производители SCADA систем на контроллерах собственного производства (например, Siemens SIMATIC), как правило, используют встроенные драйверы. Для вариантов использования контроллеров разных производителей в состав SCADA-систем разработчики предлагают набор соответствующих драйверов. Наиболее широкое распространение получили варианты разработки SCADA-систем для взаимодействия практически на всех уровнях автоматизации путем использования универсальных клиент-серверных технологий OPC (Open Platform Communications), представляющих единый интерфейс для сбора данных и управления различными устройствами [3].

В настоящее время можно выделить следующие наиболее перспективные решения к организации удаленного доступа в распределенных системах контроля и управления:

- применение технологий промышленного Интернета вещей (IIoT);
- применение универсального интерфейса сбора данных и управления различными устройствами OPC UA (Unified Architecture);
- применение полнодуплексной технологии WebSocket.

Интернет-вещей (IIoT) – это технология объединения в единую сеть физических объектов («вещей») для взаимодействия друг с другом и пользователями через Интернет, которая широко применяется уже много лет в бытовой сфере (технология «Умный дом») и реализации сбора данных от распределенных объектов (например, автоматизированная система коммерческого учета электроэнергии (АСКУЭ)). Для обмена данными в IIoT широкое применение получили протоколы физического уровня: LoRaWAN (протокол беспроводного доступа широкого радиуса действия), NB-IIoT (узкополосный «Интернет вещей») и ZigBee (стек протоколов беспроводного доступа малого радиуса действия) и ряд других протоколов. Сопряжение такого рода сетей IIoT с глобальной вычислительной сетью Интернет предполагает использование специализированных сетевых шлюзов (gateway).

В концепции Industry 4.0 (четвертая промышленная революция) технология IIoT определяется [4] как «взаимодействие между вещами (продуктами, услугами, местами и прочее) и людьми, которое обеспечивается взаимосвязанными технологиями и различными платформами». Современная

промышленная индустрия рассматривает применение технологий IoT в качестве основной сетевой инфраструктуры удаленного доступа в SCADA-системе, объединяющей интеллектуальные устройства (сенсоры, актуаторы) и современные информационные технологии [5]. Структуру распределенной системы удаленного контроля и управления технологическими процессами и объектами можно представить в следующем виде (рис. 1).

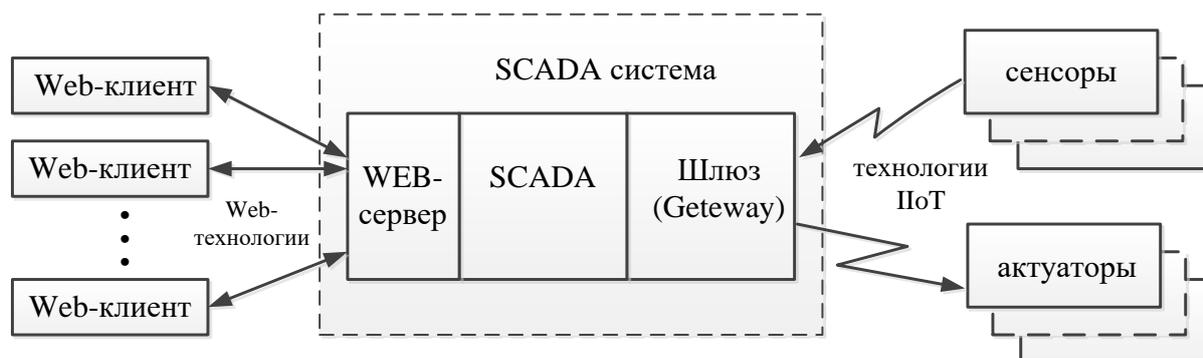


Рис. 1. Структура распределенной системы удаленного контроля и управления

В промышленной автоматизации SCADA-систему четвертого поколения рассматривают [6], главным образом, в качестве концепции, объединяющей web-технологии операторского (пользовательского) уровня и технологий IoT уровня автоматического контроля и управления. Принято считать, что IoT начинаются там, где заканчиваются классические SCADA-системы. Современные тенденции в архитектуре IoT направлены на использование web-технологий. В качестве протоколов в IoT находят применение протоколы HTTP, WebSocket.

Традиционно применяемый в системах автоматизации протокол HTTP обеспечивает взаимодействие клиента с сервером в режиме запрос – ответ, что не в полной мере отвечает современным требованиям к системам автоматизации управления технологическими процессами. Для организации полнодуплексного режима в системе автоматизации используется протокол прикладного уровня WebSocket, работающий поверх TCP соединения и обеспечивающий режим реального времени.

Удаленность от объектов управления и мобильность операторов (пользователей) в распределенных системах контроля и управления вызвали появление в SCADA-системах четвертого поколения с технологией IoT новых решений в области аппаратного обеспечения, сетей передачи данных, облачных вычислений и обработки больших объемов данных. В качестве примера готовых решений современных SCADA-систем [6, 7], обеспечивающих функционал удаленного контроля и управления в распределенных системах с использованием персональных средств телекоммуникаций (планшетов и смартфонов) и облачных вычислений заслуживают внимание SCADA-платформа фирмы Siemens (SIMATIC WinCC Open Architecture) и

MasterSCADA 4D российского производства компании МПС софт. MasterSCADA 4D – это продукт нового поколения SCADA-систем. В нем, по сравнению с предыдущими версиями, существенно расширены инструменты по созданию распределенных систем с возможностью использования технологий IIoT. При этом применение OPC UA, в качестве основного протокола IIoT, обеспечивает работу с устройствами разных производителей в режиме реального времени. Среда визуализации MasterSCADA 4D реализуется web-браузером в стандарте HTML5.

Вместе с тем, представленные готовые решения SCADA-систем с технологией IIoT для организации распределенных систем контроля и управления технологическими процессами и объектами, направлены главным образом на применение крупными предприятиями на рынке промышленной автоматизации. Для предприятий малого и среднего бизнеса такие решения могут оказаться функционально избыточными и экономически неприемлемыми. При этом предлагаемые решения по визуализации технологических процессов с использованием персональных мобильных средств (планшетов и смартфонов) и стандартных браузеров в предлагаемых SCADA-системах, не всегда отвечают потребностям пользователей. В связи с этим, можно считать перспективным направлением организацию мобильного доступа к удаленным объектам контроля и управления с использованием стандартных браузеров или специальных нативных (native) и прогрессивных (PWA) приложений [8]. В настоящее время на рынке средств автоматизации уже получили применение Web-ориентированные SCADA-системы (WebSCADA), обеспечивающие отображение технологического процесса непосредственно в браузере с использованием HTML5 и JavaScript (например, WebDisCo – продукт компании «ФИОРД», г. Санкт-Петербург).

В заключение можно выделить следующие тенденции и технические решения при разработке систем удаленного контроля и управления технологическими процессами и объектами:

- применение web-технологий, обеспечивающих контроль и управление с любых мобильных платформ и операционных систем;
- разработка пользовательских (собственных) web-приложений с WebSCADA функционалом на основе IIoT технологий;
- применение протокола WebSocket, обеспечивающего полнодуплексный процесс контроля и управления в режиме реального времени;
- использование интеллектуальных датчиков и исполнительных механизмов при переходе к технологии «Web-вещей» (Web of Things).

Список используемых источников

1. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. СПб.: Питер, 2003. 877 с.

2. Автоматизация диспетчеризации производственных процессов промышленных предприятий. А. А. Мусаев, Ю. М. Шерстюк. // URL: <https://szma.com/wp-content/uploads/2016/10/art21.pdf>

3. Просто о стандартах OPC DA и OPC UA // Средства и системы промышленной автоматизации. URL: <https://asutp.ru/publikacii/2021/04/29/prosto-o-standartah-opc-da-i-opc-ua>

4. Шваб К. Четвертая промышленная революция / К. Шваб. «Эксмо», 2016 (Top Business Awards) ISBN 978-5-699-90556-0

5. «Интернет вещей» в промышленности: обзор ключевых технологий и трендов. Ли Да Сюй (Li Da Xu), Ву Хе (Wu He) - whe@odu.edu, Сянчан Ли (Shanchang Li) - shanchang.li@bristol.ac.uk, перевод Алексей Осотов. // Приложение к журналу CONTROL ENGINEERING РОССИЯ IIoT апрель 2017. URL <https://controlengrussia.com/internet-veshhej/klyuchevy-h-tehnologij>

6. Климков К. С. Промышленный Internet вещей и облачные технологии в современных SCADA-системах // Автоматизация в промышленности. 2017. № 7. С. 22–24.

7. Современные технологии удаленного доступа к технологическим и производственным данным в SCADA-системах на примере WinCC OA. / С. Соловьев, Андрей Серов // Control Engineering Россия. 2016. URL: https://controlengrussia.com/scada-sistemy/wincc_oa

8. Абрамов А. Е., Калагур Д. А., Шабанов А. П. Анализ тенденций развития технологий прогрессивных веб-приложений. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). XII Международная научно-техническая и научно-методическая конференция. сб. науч. ст. в 4-х т. СПб. СПбГУТ, 2023. Т. 2. С. 8–11.

УДК 004.04:37
ГРНТИ 20.15.05:14.39

МОДЕЛИРОВАНИЕ ПЛАНИРОВЩИКА ЗАДАЧ ДЛЯ РОДИТЕЛЕЙ И ДЕТЕЙ С СИСТЕМОЙ ВОЗНАГРАЖДЕНИЯ

А. О. Жаранова, М. В. Котлова, К. А. Нерман

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

Актуализирована разработка планировщика задач для родителей и детей с системой вознаграждения. На основе анализа существующих сервисов выделены требования к разрабатываемой информационной системе. Сформирована модель информационной системы планировщика задач для родителей и детей с системой вознаграждения, описаны ключевые элементы модели. Основные функциональные возможности системы представлены на диаграмме вариантов использования. Описан жизненный цикл задачи, включающий процессы выполнения, проверки и начисления баллов. Предложен алгоритм рекомендаций заданий, основанный на выполненных задачах ребенка.

цифровая платформа, моделирование, мотивация детей, финансовое образование, воспитание детей, управление временем, организация расписания

В условиях динамично развивающегося информационного общества важно использовать современные технологии для оптимизации различных процессов, включая образование и воспитание детей.

Задача моделирования и разработки планировщика задач с системой вознаграждения актуальна в силу высокой занятости родителей и необходимости мониторинга ритма жизни ребенка. Система может способствовать созданию более комфортных условий для развития детей, снижению стресса у родителей, улучшению коммуникации между родителем и ребенком, повышению мотивации детей к учебе и саморазвитию.

Целью информационной системы является помощь родителям в эффективном управлении повседневной жизнью ребенка и формировании у детей полезных навыков, а также стимулировании их к качественному использованию времени через внедрение системы поощрений [1].

Задачами информационной системы являются улучшение взаимоотношений между детьми и их родителями, помощь в налаживании более тесной связи между ними и повышение качества коммуникации в семье. В рамках этой системы взаимодействие становится дополнительной возможностью для обсуждения проблем и разрешения конфликтов.

В моделируемой системе родители могут создавать задачи для своих детей и устанавливать баллы, которые можно заработать за их выполнение. Дети могут просматривать список задач и выполнять их, получая за это назначенные баллы. При отметке задания выполненным родитель должен

подтвердить его выполнение, чтобы начислить баллы ребенку. Кроме того, родители могут добавлять «подарки» в список вознаграждений, которые дети могут «покупать». Каждая активность отмечается категорией, а затем, на основе выполненных ребенком заданий, формируется диаграмма интересов ребенка, способствующая определению характеристик личности с целью последующей мотивации и развития необходимых навыков.

В настоящий момент существует не так много планировщиков задач для родителей и детей с системой вознаграждения. Рассмотрены несколько конкурентоспособных информационных систем: СберKids, Тинькофф Джуниор, OurHome, KidsBonus и KiteTools. В большинстве приложений отсутствует возможность формирования профиля ребенка, что не позволяет родителю лучше узнать интересы своего ребенка посредством визуального представления системой тех заданий, которые он выполняет чаще остальных, а также отсутствует функционал подтверждения выполнения ребенком задания, что может привести к получению баллов обманным способом. Важный недостаток рассмотренных систем также состоит в том, что они являются мобильными приложениями. Моделируемая система будет являться веб-приложением, доступным с любого устройства.

Сравнительный анализ существующих систем позволил определить функциональные требования для моделирования и разработки планировщика задач для родителей и детей.

Ключевыми пользователями проектируемой системы являются группы «Родитель» и «Ребенок», которые имеют следующий функционал:

- родители и дети должны иметь отдельные аккаунты с двумя разными ролями «Родитель» и «Ребенок» и возможностью входа в приложение, родитель регистрирует ребенка через функционал внутри своего аккаунта;
- родитель может формировать список вознаграждений для ребенка путем добавления изображений и стоимости в баллах для каждой награды;
- родитель может создавать задания для ребенка, указывая название задания, срок выполнения, описание и количество баллов за выполнение;
- ребенок должен просматривать назначенные ему задания;
- ребенок должен отмечать выполненные задания и получать баллы;
- родитель должен иметь возможность подтвердить или отклонить выполнение задания ребенком;
- система должна отображать количество накопленных ребенком баллов на экране и у родителя, и у ребенка;
- родитель должен иметь возможность просматривать диаграммы интересов детей отдельно для каждого ребенка;
- ребенок должен иметь возможность обменять свои баллы на подарки-вознаграждения, которые родитель определил за выполнение заданий.

Помимо этого, системой управляет пользователь с ролью «Администратор», который имеет возможность создавать в таблице пользователей любые аккаунты, добавлять подарки в список вознаграждений любого ребенка, просматривать все подарки в системе, добавлять задания в список заданий любого ребенка, просматривать все задания всех пользователей-детей, управлять географическим стеком, удалять пользователей и ограничивать им доступ к системе.

На основе функциональных требований сформирована модель информационной системы, представленная на рис. 1.

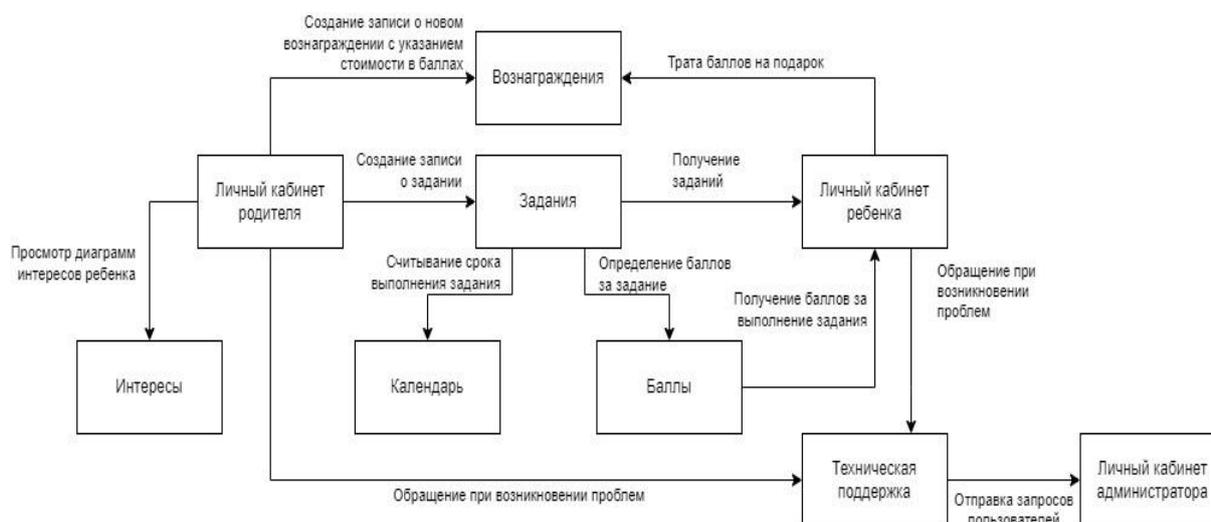


Рис. 1. Модель информационной системы планировщика задач для родителей и детей

На основе функциональных требований и алгоритма работы системы составлена диаграмма прецедентов [2], представленная на рис. 2.

Алгоритм работы системы при условии честного выполнения ребенком задания включает следующие шаги.

1. Родитель регистрирует свой аккаунт в системе.
2. Родитель входит в систему.
3. Родитель создает аккаунты для детей, назначая им логины и пароли.
4. Родитель создает задачу для ребенка в системе, указывая ее описание, срок выполнения, количество баллов за выполнение.
5. Родитель создает подарок для ребенка, прикрепляя фотографию награды и назначая стоимость в баллах.
6. Ребенок входит в аккаунт по данным родителем логином и паролю.
7. Ребенок просматривает список задач в системе и выбирает ту, которую он хочет выполнить.
8. Ребенок выполняет задачу в соответствии с ее описанием и сроком выполнения, ставит отметку о выполнении.
9. Родитель подтверждает выполнение задачи.
10. Ребенок получает назначенное количество баллов.

11. Ребенок просматривает список подарков и выбирает желаемый подарок в соответствии с количеством баллов у него в наличии.
12. Ребенок нажимает кнопку «Купить».
13. Подарок меняет статус на «Куплено».

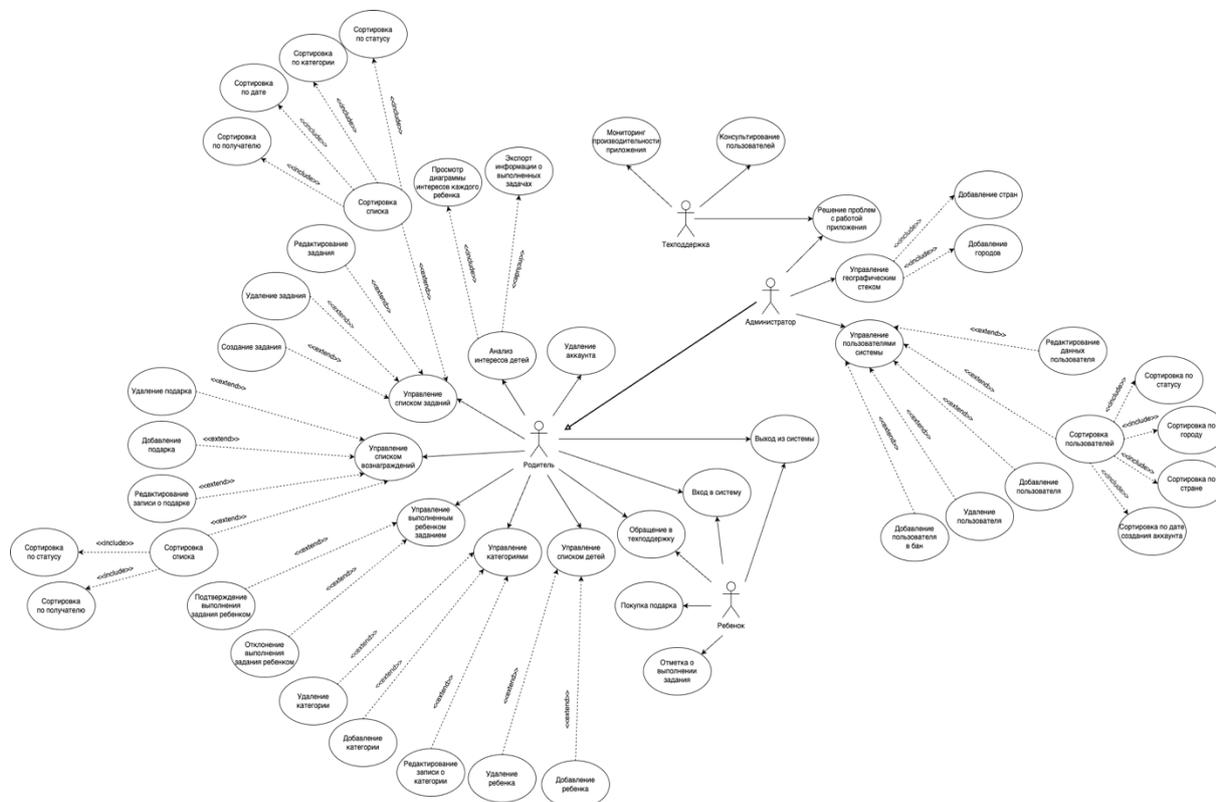


Рис. 2. Диаграмма прецедентов ИС планировщика задач с системой вознаграждения

Для описания процесса движения задачи с этапа добавления задачи до момента начисления баллов за ее выполнение разработана EPC-диаграмма [3], представленная на рис. 3.

В этой диаграмме учтена функция подтверждения или отклонения родителем выполненного ребенком заданием.

В перспективах развития планировщика задач с системой вознаграждения большой потенциал имеет функционал, направленный на улучшение понимания родителем интересов детей. Алгоритмы рекомендаций будут обрабатывать выполненные задания ребенка и на их основе генерировать новые задания, входящие в область интересов ребенка.

Для этого могут использоваться следующие алгоритмы: алгоритм Apriori, коллаборативная (user-based) фильтрация и контентная (content-based) фильтрация.

Наиболее подходящим алгоритмом рекомендаций является контентная (content-based) фильтрация, так как этот алгоритм напрямую учитывает предпочтения детей и может оперативно реагировать на изменения этих предпочтений.

Для реализации контентной (content-based) фильтрации необходимо добавить заданию следующие характеристики: сложность выполнения (легкая, средняя, сложная); ключевое слово (например, гимнастика или посуда); место выполнения (например, дом или улица).

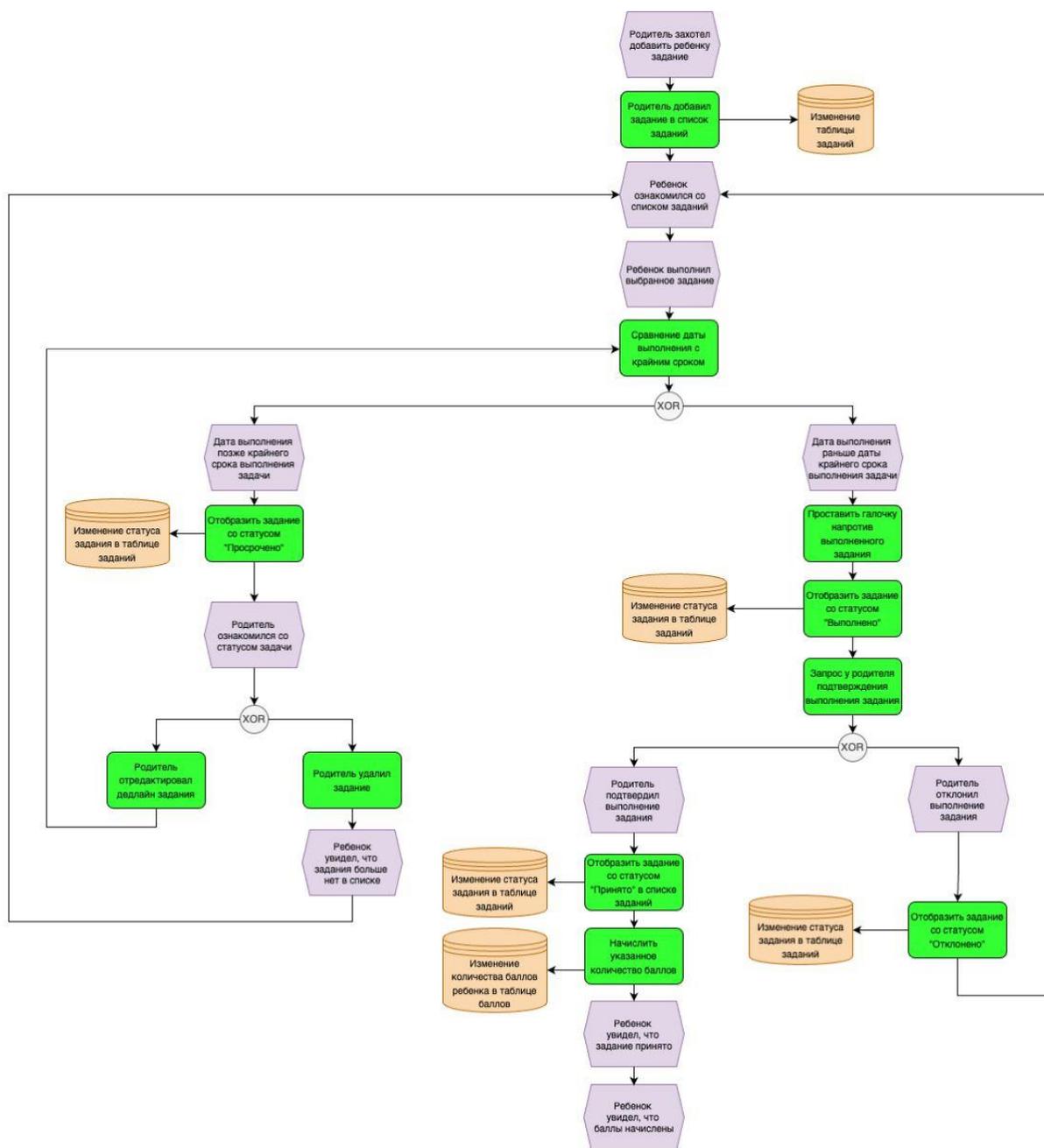


Рис. 3. EPC-диаграмма процесса движения задачи

Алгоритм является быстрым и простым в реализации, хорошо работает с помощью описательных данных, не нуждается в данных о других пользователях и не зависит от их количества в системе. Также у данного алгоритма нет проблемы «холодного старта», поскольку можно внести в стек заданий

заранее заготовленные задачи под различные профили пользователей, а самому ребенку предложить выбрать несколько категорий, которые ему интересны.

Список используемых источников

1. Жаранова А. О., Нерман К. А. Проектирование информационной системы трекера задач с системой вознаграждения // 77-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая Весна – 2023»: сб. науч. ст. в 2-х т. СПб: СПбГУТ, 2023. Т. 1. С. 220–225.

2. Котлова М. В., Давыдова Е. В. Методы и средства проектирования информационных систем и технологий. СПб.: СПбГУТ, 2015. 62 с.

3. Арзуманян М. Ю., Деревянко М. А. Моделирование бизнес-процессов. СПб.: СПбГУТ, 2014. 48 с.

Статья представлена заведующим кафедрой ИУС СПбГУТ, кандидатом технических наук, доцентом В. Л. Литвиновым.

УДК 004.94:004.021
ГРНТИ 28.17.33:50.39

РАЗРАБОТКА АЛГОРИТМА АВТОМАТИЗИРОВАННОГО ПОСТРОЕНИЯ МОДЕЛЕЙ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ДЛЯ СИСТЕМЫ ПРОЦЕДУРНОЙ ГЕНЕРАЦИИ ВИРТУАЛЬНЫХ ПРОСТРАНСТВ

А. О. Жаранова, Г. Д. Слезак

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

Обоснована актуальность создания и применения алгоритма автоматизированного построения моделей локальных вычислительных сетей для систем процедурной генерации виртуальных пространств. Описаны требования к структуре данных алгоритма в целях совместимости с конечной информационной системой. Сформирована и описана структура алгоритма и его данных. Выбраны лингвистическое и программное обеспечения с учётом целей использования проектируемого алгоритма. Выполнена реализация алгоритма с использованием выбранного обеспечения. Представлены возможности расширения алгоритма и его адаптации для различных конечных информационных систем.

локальные сети, процедурная генерация, симуляция, игровой движок, алгоритм, симулятор

В современном мире новые технологические решения появляются с такой стремительностью, что специалистам трудно успевать реализовать их на практике. Это применимо и к сфере образования, и в особенности к сфере широкого использования обучающих игр и симуляторов. Игровое обучение в определенных случаях [1] позволяет добиваться более высоких показателей усвояемости материалов дисциплин по сравнению с классическими методами обучения и тестирования, при этом эффективно поддерживая интерес обучающегося к преподаваемой дисциплине [2].

В сфере администрирования информационных систем, которая выбрана для рассмотрения, наблюдается использование заранее заготовленных вариантов заданий, которые не адаптируются под навыки обучающегося и ограничены по количеству. Разрабатываемый алгоритм призван решить эту проблему путём автоматизированной генерации модели локальной вычислительной сети для дальнейшего использования данной модели в системе генерации виртуальных пространств, в которых обучается пользователь.

Прежде чем переходить к разработке алгоритма, необходимо определить требования к структуре его данных.

Данный алгоритм планируется использовать в совокупности с системой анализа навыков пользователя, в которой в качестве выходных данных

используются числовые параметры – предполагаемая сложность, текущий уровень навыков и другие. Алгоритм должен принимать на вход набор параметров из данной системы, далее на основе заданных параметров и в соответствии с генерируемым типом задания генерировать модель локальной вычислительной сети, которая может быть использована для генерации объектов и их свойств. Схема, описывающая входные и выходные параметры, представлена на рис. 1.

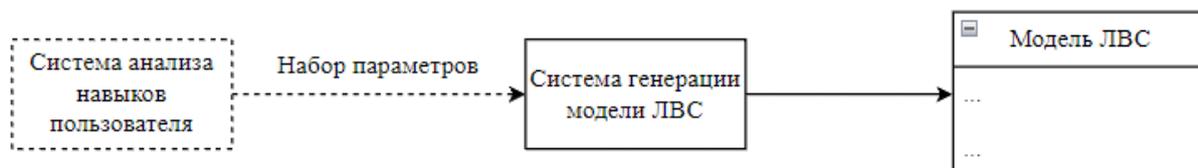


Рис. 1. Схема входных и выходных параметров алгоритма

Генерируемая локальная вычислительная сеть должна частично отражать сети, используемые на предприятиях, при этом оставаясь понятной для обучающегося. В связи с этим имеет смысл генерировать сеть с топологией вида «дерево» с заданным количеством уровней, где на верхних уровнях, как правило, используются маршрутизаторы; на средних уровнях – коммутаторы, объединяющие конечные узлы в отдельные подсети (например, разделение на подсети рабочих станций разных отделов на предприятии); на нижнем уровне – конечные узлы (как правило, рабочие станции). Схема описанной структуры локальной вычислительной сети представлена на рис. 2.

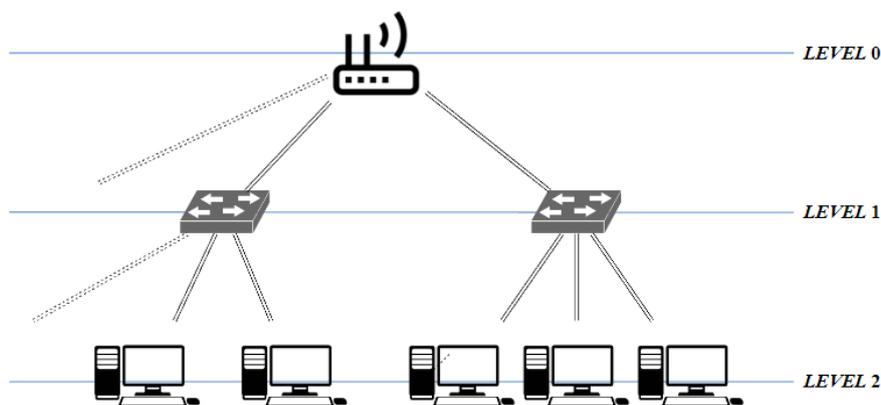


Рис. 2. Типичная обобщенная структура локальной вычислительной сети предприятия

Для обработки и хранения подобной структуры в программном виде можно использовать графы. Существует возможность представить граф в виде матрицы смежности или матрицы инцидентности, но в данном алгоритме использована именно матрица смежности в связи с неориентированностью графа.

Предполагаемый граф не будет иметь петель, так как не подразумевается соединение узлов с самими собой, и, следовательно, можно использовать диагональ матрицы смежности для других целей. Необходимо хранить данные об уровнях каждого узла, поэтому решено поместить информацию об уровнях в диагональ результирующей матрицы.

Предполагаемый граф является неориентированным, а предполагаемая матрица, представляющая граф, является симметричной, так как физические соединения в локальной вычислительной сети имеют двусторонний характер, и решение о передаче или принятии сигнала принимается соответствующими узлами, а не типом физической среды передачи.

В данной версии алгоритма веса ребер не учитываются.

Таким образом, матрица смежности A , представляющая результирующий граф, будет иметь следующий вид:

$$A = \begin{pmatrix} 0 & \cdots & a_{i,j} \\ \vdots & \ddots & \vdots \\ a_{i,j} & \cdots & n \end{pmatrix},$$

где $a_{i,i}$ – уровень узла i , $a_{i,j} = a_{j,i}$ – наличие соединения между узлами при значении 1 и его отсутствие при значении 0, n – значение последнего уровня дерева.

Представленная структура использована при формировании классов алгоритма. Фрагмент диаграммы классов представлен на рис. 3.

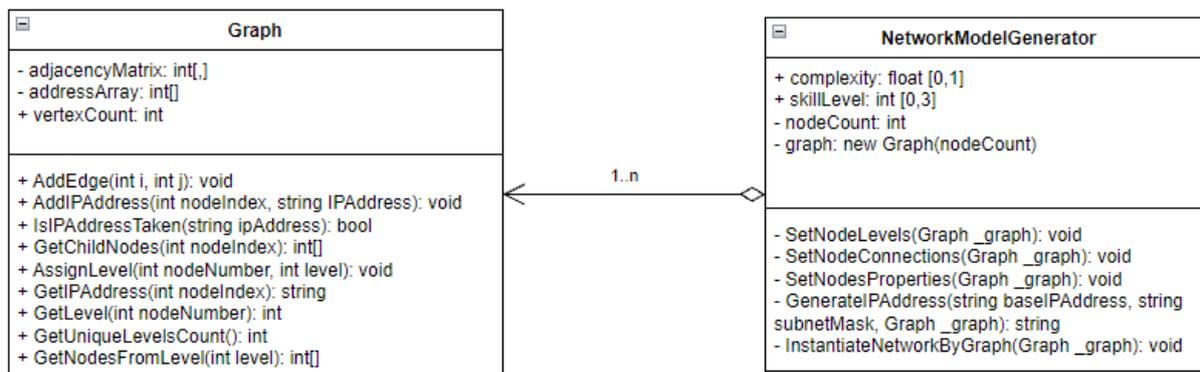


Рис. 3. Фрагмент диаграммы классов

Класс Graph содержит матрицу смежности, массив IP-адресов каждого узла, а также вспомогательные поля и методы, используемые при работе с классом графа.

Класс NetworkModelGenerator содержит поля со значениями параметров, получаемых из системы анализа навыков пользователя и влияющих на конечную модель локальной вычислительной сети, а также служебные поля и методы, используемые при работе с классом генератора модели.

Для реализации полученных классов выбрана кроссплатформенная среда разработки компьютерных игр (игровой движок) Unity [3]. Программный код выполнен на языке программирования C#.

Фрагменты программного кода алгоритма на языке C# представлены на рис. 4.

```

using System;
using System.Collections.Generic;
using System.Linq;
using UnityEngine;

public class Graph
{
    private int[,] adjacencyMatrix;
    private string[] addressArray;

    public int vertexCount { get; private set; }

    public Graph(int vertices)
    {
        adjacencyMatrix = new int[vertices, vertices];
        addressArray = new string[vertices];
    }

    public void AddEdge(int i, int j)
    {
        adjacencyMatrix[i, j] = 1;
    }

    public void AddIPAddress(int nodeIndex, string ipAddress)
    {
        addressArray[nodeIndex] = ipAddress;
    }

    public bool IsIPAddressTaken(string ipAddress)
    {
        return addressArray.Contains(ipAddress);
    }

    // <summary>
    // Возвращает массив с индексами узлов, дочерних для данного узла
    // </summary>
    // <param name="nodeIndex">индекс узла</param>
    // <returns>массив индексов</returns>
    public int[] GetChildNodes(int nodeIndex)
    {
        List<int> children = new List<int>();
        for (int i = 0; i < adjacencyMatrix.GetLength(0); i++)
        {
            if (adjacencyMatrix[i, nodeIndex] == 1)
            {
                children.Add(i);
            }
        }
        return children.ToArray();
    }

    public void AssignLevel(int nodeNumber, int level)
    {
        adjacencyMatrix[nodeNumber, nodeNumber] = level;
    }

    public string GetIPAddress(int nodeIndex)
    {
        return addressArray[nodeIndex];
    }
}

using System;
using System.Collections.Generic;
using System.Linq;
using UnityEngine;

public class NetworkModelGenerator : MonoBehaviour
{
    private System.Random random;

    [Header("References")]
    [SerializeField] private GameObject nodePrefab;
    [SerializeField] private GameObject connectionCablePrefab;
    [SerializeField] private Transform spawnPosition;

    [Header("Parameters")]
    public int defaultNodeCount = 7;

    private int nodeCount;

    [Range(0f, 1f)] public float complexity = 0.5f;
    [Range(1, 3)] public int skillLevel = 1;

    [SerializeField] private int[] levelNodesCountLowerBounds = new int[4];
    [SerializeField] private int[] levelNodesCountUpperBounds = new int[4];

    private int[,] levelNodesCountBounds;

    void Start()
    {
        random = new Random();
    }

    // Починить
    public void SetNodeLevels(Graph _graph)
    {
        // ...
    }

    private int[] DivideArray(int groupsCount, int[] source)
    {
        // ...
    }

    public void SetNodeConnections(Graph _graph)
    {
        // ...
    }

    public void InstantiateNetworkByGraph(Graph _graph)
    {
        // ...
    }
}
    
```

Рис. 4. Фрагменты программного кода алгоритма

Алгоритм выполняется следующим образом:

- в соответствии с установленными в генераторе правилами и полями формируется матрица смежности, ее репрезентация в виде графа представлена на рис. 5;



Рис. 5. Репрезентация примера матрицы смежности в графическом виде

- каждому узлу присваивается уникальный IP-адрес, сгенерированный на основе адреса верхнего узла (маршрутизатора) и маски подсети;
- подготовленная модель сети готова к использованию в конечной информационной системе, коей и является игровой движок.

Примеры результатов генерации объектов виртуального пространства на основе вариантов результирующих моделей локальной вычислительной сети представлены на рис. 6.

В данной итерации алгоритма характер генерируемой локальной сети зависит от успеваемости обучающегося при выполнении заданий заданного типа и от выбранного самим пользователем уровня сложности. Иными словами, если пользователь обладает слабым пониманием устройства локальных

сетей и принципов их администрирования в определённых аспектах, то при генерации задания ему будет предложена условно более простая локальная сеть (небольшое количество узлов и уровней). Аналогично, продвинутому в заданной теме пользователю предлагаются задания с сетями с большим числом узлов и уровней.

Несмотря на то, что условная «сложность» генерируемой сети зависит от навыков пользователя, структура локальной вычислительной сети генерируется псевдослучайным образом (количество уровней, узлов, соединения между узлами), а параметры сложности и навыков пользователя влияют только на границы интервалов возможных значений.

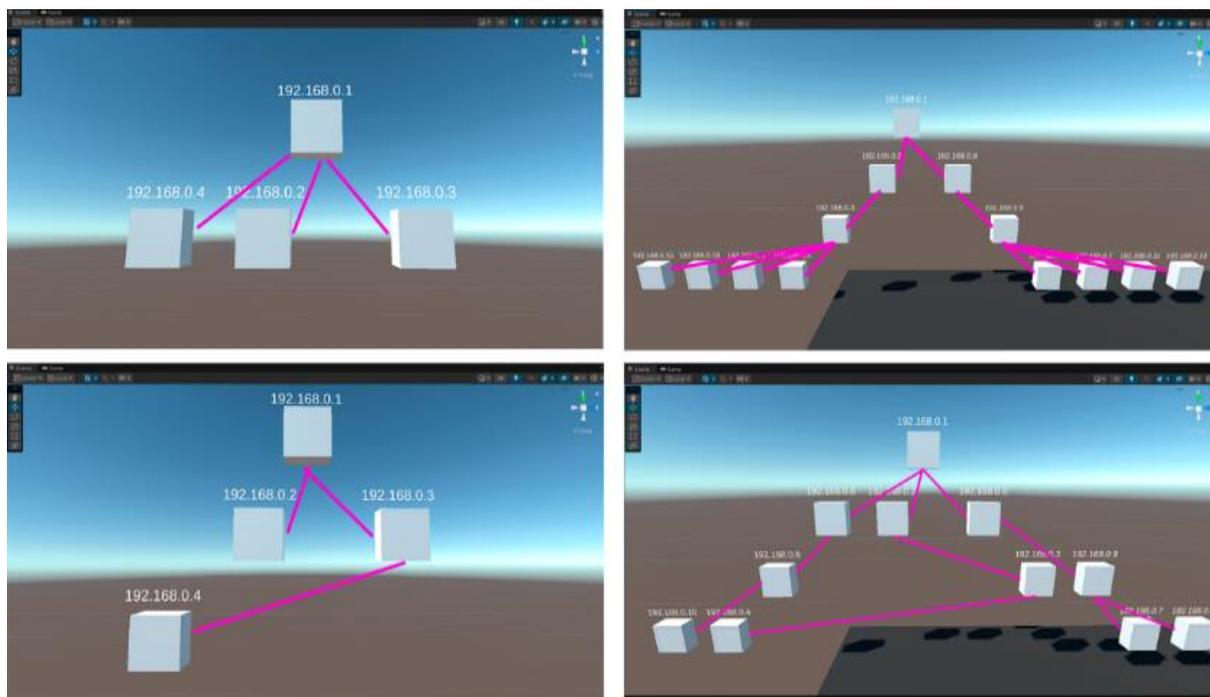


Рис. 6. Примеры вариантов результатов генерации

Разработанный алгоритм имеет следующие возможности расширения: автоматическая генерация масок подсетей; генерация других свойств узла (тип устройства, название и др.); генерация свойств соединений; генерация случайных IP-адресов в подсетях; создание наборов констант для реализации разных видов заданий; выдача рекомендаций по результатам выполненных заданий; интеграция алгоритма анализа навыков.

Данный алгоритм имеет следующие перспективы использования: создание имитационных моделей локальных вычислительных сетей; создание обучающих игр и симуляторов по администрированию локальных вычислительных сетей; использование в высших учебных заведениях при изучении дисциплин, связанных с системным администрированием.

Таким образом, с учетом определенных требований выполнена реализация алгоритма автоматизированного построения моделей локальных вычислительных сетей для системы процедурной генерации виртуальных пространств на языке C#. Описаны возможности расширения алгоритма и перспективы его использования.

Список используемых источников

1. Valentová, Monika & Brečka, Peter. Assessment of Digital Games in Technology Education. International Journal of Engineering Pedagogy // iJEP. 2023. DOI:10.3991/ijep.v13i2.35971 (дата обращения: 25.02.2024)

2. Pineda-Martínez, M.; Llanos-Ruiz, D.; Puente-Torre, P.; García-Delgado, M.Á. Impact of Video Games, Gamification and Game-Based Learning on Sustainability Education in Higher Education // Preprints.org. 2023. DOI: 10.20944/preprints202305.0715.v1 (дата обращения: 27.01.2024)

3. Unity Documentation // Unity Technologies. URL: <https://docs.unity.com> (дата обращения: 10.02.2024)

Статья представлена заведующим кафедрой ИУС СПбГУТ, кандидатом технических наук, доцентом В. Л. Литвиновым.

УДК 004.89
ГРНТИ 28.23.00

ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: ОСНОВНЫЕ ХАРАКТЕРИСТИКИ, ПРИМЕНЕНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В УПРАВЛЕНИИ ЗНАНИЯМИ

Е. А. Женихов, О. А. Пекарская

Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева

Статья посвящена описанию интеллектуальных информационных систем, их характеристик, классификации, применению, а также роли в управлении знаниями. Представлена методика интеллектуального анализа данных с помощью интеллектуальных информационных систем. Отмечено, что сегодня в нашей стране особо актуально создание необходимых условий для разработки и внедрения технологий искусственного интеллекта, прежде всего, в целях повышения качества жизни населения, укрепления национальной безопасности, развития различных сфер экономики, здравоохранения, культуры, образования.

Интеллектуальные информационные системы, интеллектуальный анализ данных, управление знаниями, оперативная аналитическая обработка данных, логико-математическая система

Сегодня интеллектуальные информационные системы (ИИС) быстро внедряются в нашу жизнь, предоставляя широкие возможности в обеспечении информационной национальной безопасности страны, для развития различных секторов народного хозяйства, финансового сектора, здравоохранения, образования и культуры.

Современная ИИС – это уникальный механизм, синтезирующий возможности систем управления базами данных, и совокупность технологий искусственного интеллекта. В состав ИИС включены программные, лингвистические средства, а также инструменты математической логики, чтобы реализовывать основную цель данных систем – осуществление поддержки самой разнообразной человеческой деятельности на основе поиска информации в режиме специфического диалога на естественном языке (рис. 1).

ИИС имитируют когнитивные функции человека, например, функцию самообучения; осуществляют поиск различных решений, самостоятельно подготавливая информацию для них, даже если не существует предварительный алгоритм; выбирают оптимальные решения [1].

Отличительная черта ИИС – это база знаний, которая записана на магнитном носителе информации в том виде, который понятен эксперту и пользователю, для потребностей которого ИИС и создается.

Логика считается одним из основных корней искусственного интеллекта. Ведь еще в V веке до нашей эры Аристотель изобрел силлогистическую логику, первую формальную дедуктивную систему рассуждения. Паскаль создает первую механическую цифровую вычислительную машину в 1642 году.

В 1957 году Ньюэл, Шоу и Саймон, авторы The Logic Theorist, разработали General Problem Solver (GPS), который, по сути, представляет собой компьютерную программу, предназначенную для работы в качестве универсальной машины для решения задач.

Одним из первых языков в ИИС является LISP (List Processor), созданный Дж. Маккарти, на многих диалектах которого (INTERLISP, FRANZLISP, QLISP) написаны мировые экспертные системы, системы естественно-языкового общения.

Логический язык PROLOG, который, начиная с 1980-х годов, достаточно активно использовался при изучении элементов математической логики, принципов логического программирования и проектирования баз знаний, основан на том, что факты в нем описываются в форме логических предикатов с конкретными значениями.

В настоящее время при создании ИИС наблюдается отход от этих двух традиционных классических языков при решении задач искусственного интеллекта [2].



Рис. 1. Общая классификация современных интеллектуальных информационных систем [2]

Так, например, язык программирования Python, относящийся к высокоуровневым языкам программирования общего назначения, имеющий огромное и очень активное сообщество разработчиков, популярен и в области информационных систем, использующих искусственный интеллект. Этот язык, с простым, гибким и легко читаемым синтаксисом, обладает еще широчайшей библиотечной экосистемой: PyTorch, TensorFlow, Keras, Google Jax, NumPy, SciPy, Pandas, NLTK, OpenCV, Matplotlib, Hugging Face transformers.

ИИС по сравнению с другими информационными системами имеют ряд особенностей:

- умение коммуницировать;
 - умение решать сложные задачи, в том числе с нечеткой логикой (пример – нейронные сети);
 - способность к самообучению;
 - адаптивность к потоку информационных данных;
 - наличием особой интеллектуальной базы данных.
- Рассмотрим подробнее классификацию ИИС, представленную на рис. 2.



Рис. 2. Классификация ИИС

Умение коммуницировать, заложенное в системах с коммутативными способностями, предполагает, что коммуникационные свойства будут очень

зависеть от естественно-языкового интерфейса, позволяющего транслировать конструкции естественного человеческого языка на внутримашинный язык с обязательным учетом морфологии (для правильности написания слов идет обращение к словарям), синтаксиса (для разделения входных сообщений на фрагменты с более детальной грамматической проверкой) и семантику (для смысловой верификации) естественного языка.

Естественно-языковой интерфейс решает задачи доступа к интеллектуальным базам данных, контекстного поиска текстовой информации, голосового ввода команд, компьютерного перевода.

Гипертекстовые системы предназначены для реализации поиска по ключевым словам в базах текстовой информации, с учетом сложной семантической организации ключевых слов, которая отражает различные смысловые отношения терминов [2].

Контекстная помощь позволяет реализовать проблемный подход, при котором пользователь уже сразу описывает всю проблему (ситуацию), а затем уже начинает действовать система в целом, при этом поиск рекомендаций система осуществляет уже самостоятельно в зависимости от сложившейся ситуации.

Системы когнитивной графики отвечают за графические образы, генерация которых осуществляется на базе происходящих событий для общения пользователя с ИИС в ситуациях, когда от обучаемого требуется не только принятие решений, но и конкретные действия.

Экспертные системы, в своей работе использующие накопленные базы знаний, решают сложные управленческие задачи, диагностируют ситуации, обосновывают управленческие решения.

Для таких динамических систем, как многоагентные, характерна интеграция в базе знаний нескольких разнородных источников знаний, обменивающихся между собой получаемыми результатами на динамической основе. Эти системы отлично справляются в ситуациях, когда:

- нужно использовать различные источники знаний, позволяющие устранять возникающие противоречия.
- возникают условия многозадачности, решения параллельных проблем;
- появляется необходимость выбора одной стратегии среди множества альтернатив;
- проводят операции с «большими данными», и необходимо прерывать выполнение заданий при получении дополнительных данных или знаний [3].

Свойство самообучающихся систем – применение методов автоматической классификации, если речь идет о реальной ситуации. В таких систе-

мах либо есть «учитель», который задает классообразующий признак, характеризующий некоторый класс ситуаций, либо система сама определяет классы ситуаций.

В индуктивных системах используется восхождение от частного к общему. Рассмотрим последовательность классификации примеров.

1. Происходит выбор признака классификации.
2. В зависимости от выбранного признака множество примеров разбивается на подмножества.
3. Далее проводится проверка на соответствие подмножества примеров одному подклассу.
4. Процесс классификации заканчивается, когда устанавливается принадлежность подмножества примеров одному подклассу.
5. Если у подмножества примеров отсутствует совпадение классообразующего признака, то процесс классификации проводится повторно, начиная с первого пункта [3].

Нейронные сети построены по аналогии с работой человеческого мозга. Здесь для проведения параллельных вычислений используются простые процессоры, которые передают друг другу сигналы по сети.

Прецедентные экспертные системы обладают базами знаний, содержащих непосредственно ситуации или прецеденты. В этих системах осуществляется поиск решений по аналогии.

Информационное хранилище отличается от интеллектуальной базы данных тем, что в информационном хранилище находится значимая информация из оперативной базы данных, на базе которой реализуется OLAP (On-Line Analytical Processing) технология.

При оперативном ситуационном анализе выполняются следующие задания:

- находится профиль потребителей заданных объектов хранения;
- определяется, каким образом объекты хранения изменяются со временем;
- проводится корреляционный анализ.

Структура адаптивной информационной системы изменяется со временем в зависимости от того, каким образом меняется проблемная область.

Адаптивная информационная система (система с репозиторием) обладает следующими свойствами:

- наличие адекватной поддержки организации бизнес-процессов;
- умение адаптироваться к реорганизации бизнес-процессов;
- возможность минимизировать затраты на реконструкцию информационной системы.

Рассмотрим теперь общий алгоритм процесса формирования знаний, показанный на рис. 3.

Извлечение знаний по обычным технологиям очень трудозатратно, и в инженерии знаний сегодня интенсивно внедряются методы, направленные на то, чтобы извлекать знания из накопленных фактов автоматически. Интерпретация данных, когда определяется смысл данных, а затем согласовываются и корректируются результаты с использованием многовариантного анализа, – необходимая часть работы интеллектуальных информационных экспертных систем.

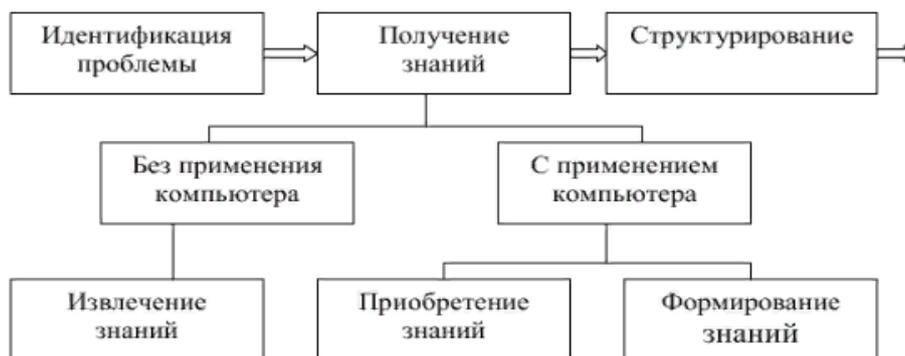


Рис. 3. Общий алгоритм процесса формирования знаний [4]

В основе этих методов лежат известные из логики методы индуктивного вывода и ряд методов распознавания образов – «раскопка данных и открытие знаний». В отечественной литературе используется термин «интеллектуальный анализ данных (ИАД)» [4]. На стадии свободного поиска ИИС определяет сложнейшие логические закономерности, строит линии тренда, использует самые разнообразные методики корреляционно-регрессионного анализа, в том числе и динамические модели.

Система сама анализирует содержимое баз данных и делает правдоподобные предсказания относительно этих значений. Прогнозирование дает возможность предсказать развитие событий в будущем, опираясь на имеющиеся в нашем распоряжении исходные данные, предусматривая использование параметрической динамической модели с варьированием параметров для отработки совпадения моделируемых значений с имеющимися экспериментальными значениями.

В нашей стране сегодня ИИС используются в разных федеральных проектах. Федеральный проект «Искусственный интеллект» – это уникальная, активно реализуемая с 2021 года программа внедрения ИИС в различные отрасли промышленности, здравоохранение, образование и культуру [6].

В заключение хотелось бы процитировать слова В. В. Путина из его выступления на Международной конференции по искусственному интеллекту Artificial Intelligence Journey в ноябре 2023 года: «С внедрением искусственного интеллекта в науку, в образование, в здравоохранение, да и во все сферы нашей жизни, человечество начинает новую главу своего существования».

Список используемых источников

1. Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» от 24.04.2020 № 123-ФЗ (последняя редакция) URL: <http://www.consultant.ru> (дата обращения: 19.02.2024)

2. Андрейчиков А. И. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник А. И. Андрейчиков, О. Н. Андрейчикова. М. ИНФРА-М, 2024. 530 с.

3. Никишова М. И. Применение технологий искусственного интеллекта в системе корпоративного управления : дис. ... канд. экон. наук: 08.00.05 / Никишова Мария Игоревна. М., 2021. 195 с.

4. Горохов А. В., Мартынов В. А., Гаврин В. А. Искусственный интеллект // Выпуск студенческой науки. 2022. Вып. 4(68). С. 159–168.

5. Волокобинский М. Ю., Зильберман А. А. Особенности защиты информации в вычислительных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 482–485

6. Пекарская О. А., Парфенова И. А. Правовые основы безопасности личности в современном обществе // Сборник статей по материалам XIX Международной научно-практической конференции «Гражданская оборона и природно-технические системы». Воронеж, 2023. С. 424–427.

УДК 004.056
ГРНТИ 81.93.29

СПОСОБ ПОВЫШЕНИЯ ЦЕЛОСТНОСТИ ФАЙЛОВ ИНФОРМАЦИОННЫХ РЕСУРСОВ СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ АТАК

В. А. Задбоев, В. А. Липатников, В. В. Нефедов

Военная академия связи имени маршала советского союза С. М. Буденного

Постоянно прогрессирующие в своем развитии современные компьютерные технологии делают актуальными различные задачи в сфере кибербезопасности. Разработка наиболее эффективного способа защиты файлов в настоящее время становится одной из важных задач большинства разработчиков.

Исполняемые файлы, вложение информации, обеспечение целостности, сеть передачи данных

Введение. В статье [1] рассмотрен способ управления кибербезопасностью (КБ) инфраструктуры интегрированной организации с распознаванием вторжений и анализом динамики действий нарушителя на основе нейро-нечетких сетей и когнитивного моделирования. Функции алгоритма управления: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в информационную сеть и распознавание вторжения, выбор и реализация способа защиты. В статье [2] предложен способ управления информационной безопасностью (ИБ), основанный на добавлении в демилитаризованную зону информационно-вычислительной сети выделенного сервера, на котором с помощью технологии контейнерной виртуализации развертывается виртуальная копия реальной сети, включающая сетевые сервисы. Злоумышленник, производящий подготовку компьютерной атаки на сеть, предполагает, что взаимодействует с реальной сетью. В статьях [1] и [2] не рассматривается вопрос обеспечения целостности файлов информационных ресурсов сети передачи данных (СПД) в условиях атак. Таким образом, подтверждается актуальность разработки способа обеспечения целостности файлов ИР СПД в условиях атак.

Объект исследования – информационные ресурсы СПД (ИР СПД).

Предмет исследования – целостность файлов ИР СПД от атаки.

Цель – повысить целостность файлов ИР СПД в условиях атак.

Задача – разработать способ повышения целостности файлов ИР СПД в условиях атак путем скрытого внедрения информации в исполняемые файлы.

Решение: Основная идея способа заключается в управлении формированием файла с регулярным внедрением ключа и осуществлением оперативного контроля целостности файла на основе оценки энтропии. На рис. 1 представлено описание способа повышения целостности файла посредством вложения в него «ключа».

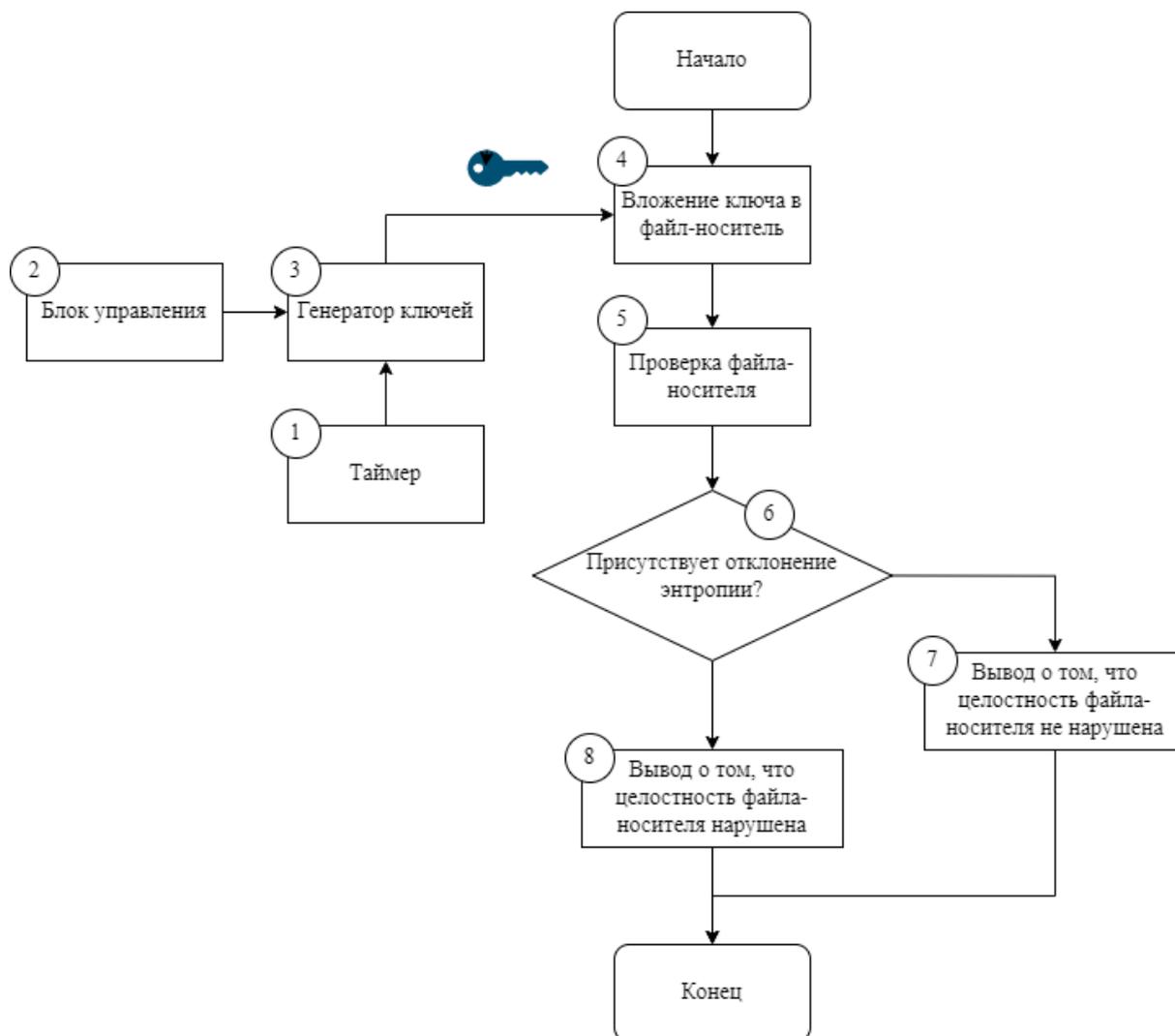


Рис. 1. Способ повышения целостности файла посредством внедрения в него «ключа»

Таймер – отвечает за частоту генерации ключа. Оператор системы сам выбирает промежуток времени, через который будет создан новый ключ. Так, например, ключ может генерироваться раз в сутки или, напротив, раз в один час. Блок управления – отправляет генератору ключей (3) параметры последовательности, которую необходимо создать. Под параметрами в данном случае понимается: длина ключа, количество используемых символов и алгоритм генерации последовательности. Генератор ключей – получая на вход необходимые данные от блока управления (2) в установленный таймером (1) промежуток времени создает последовательность, созданную

на основе исходных параметров. Ключ, после своей генерации (3), вкладывается в выбранный файл-носитель по алгоритму вложения, который также был выбран оператором заранее, основываясь на исходных параметрах файла-носителя [3]. Далее следует проверка файла-носителя на наличие отклонения энтропии (6). В случае, если отклонение присутствует можно делать вывод о том, что целостность файла была нарушена. В такой ситуации оператор (автоматизированная система) принимает необходимые меры к файлу (приостанавливает сеанс у пользователя, который работал с данным файлом, удаляет файл с компьютера атакующего и т.д.).

Вычисление энтропии. В СПД информация о ожидаемых и реальных результатах работы в определенный период времени считается предсказуемой. Различия между фактическими и прогнозными значениями на конкретных этапах времени имеют вероятностный характер и связаны со случайными отклонениями. Разности этих значений (исходы) предполагают собой множество $X = \{x_1, x_2, \dots, x_i, \dots, x_M\}$, состоящее из M элементов. На представленном множестве должно быть задано распределение вероятностей $p(x)$, в случае если любому исходу x_i поставлено в соответствие число $p(x_i)$ такое, что для всех $i = 1, 2, \dots, M$ должно быть $p(x_i) \geq 0$, $\sum p(x_i) = 1$. Множество X совместно с заданным на нем распределением вероятностей считается дискретной группой $\{X, p(x_i)\}$.

Имея в своем распоряжении дискретный ансамбль с M возможными состояниями (разностями):

$$X = \left\{ \begin{matrix} x_1, x_2, \dots, x_i, \dots, x_M \\ p_1, p_2, \dots, p_i, \dots, p_M \end{matrix} \right\}, p_i = p(x_i) \geq 0, \sum_{i=1}^M p_i = 1, \quad (1)$$

При увеличении размерности группы, количество полученных вероятностей также увеличивается. Чтобы избежать увеличения размерности данных, необходимо использовать построение гистограммы. Это позволит получить наименьшие значения вероятностей с незначительной потерей точности расчетов. Вероятности p_i не равны между собой, необходимо, чтобы мера неопределенности была непрерывной функцией вероятностей p_i , $i = 1, 2, \dots, M$ элементов дискретного ансамбля:

$$H(X) = - \sum_{i=1}^M p(x_i) \log p(x_i). \quad (2)$$

В данном вероятностном ансамбле энтропия $H(X)$ позволяет измерять информацию количественно [4].

Из анализа результатов $H(X)$ для различных состояний реализации плана можно сделать вывод о степени неопределенности при выборе прогнозных вариантов. Если все вероятности $p(i)$ одинаковы, то $H(X)$ достигнет максимального значения, также и по формуле Хартли. Представленная формула Шеннона позволяет рассчитывать значение энтропии только на основе вероятностных характеристик отклонений. Однако она не учитывает вероятность взаимодействия рассматриваемого элемента i со всеми остальными $(M-1)$ элементами дискретного ансамбля. Этот недостаток может быть устранен одним из рассматриваемых теоретических и практических методов [4]. Анализируя энтропию можно делать выводы о изменении файла.

Таким образом, предложен способ, повышающий целостность файлов информационных ресурсов сети передачи данных в условиях атак. Данный способ может выступать в качестве решения защиты файлов, поскольку способен обеспечивать проверку целостности файла.

Список используемых источников

1. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя // Информационно-управляющие системы. 2022. № 1. С. 54–67. DOI: 10.31799/1684-8853-2022-1-54-67

2. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4. С. 67–76.

3. Штеренберг С. И., Нефедов В. В., Андрианов В. И., Липатников В. А. Методика скрытного внедрения исполняемого кода в распределенные информационные системы с помощью агентного подхода // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 1. С. 76–85.

4. Липатников В. А., Ложечкин А. А., Шевченко А. А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6. С. 112–120.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ВОЗМОЖНОСТЕЙ ОТЕЧЕСТВЕННЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

В. А. Задбоев, Н. А. Роговой, А. А. Шевченко

Военная академия связи имени маршала Советского Союза С. М. Буденного

Статья посвящена исследованию технологий и инструментов, разработанных в России, предназначенных для обеспечения информационной безопасности в сетях передачи данных. В работе проводится анализ существующих средств мониторинга, выявляются их основные характеристики, преимущества и недостатки. Особое внимание уделяется их применимости в контексте защиты от современных угроз и атак, таких как кибератаки и утечки данных.

Информационная безопасность, сети передачи данных, мониторинг, SIEM-системы, инциденты

Введение. Информационная безопасность стала одной из наиболее актуальных и важных проблем в современном мире. С ростом числа цифровых угроз и увеличением объема цифровых данных защита информации становится предметом первостепенной важности для государственных и частных организаций. В этой связи, отечественные разработчики и производители предоставляют ряд средств и решений для мониторинга информационной безопасности. В данной статье рассматривается анализ возможностей отечественных средств, применяемых для мониторинга информационной безопасности сетей передачи данных [1].

Решение. Для начала необходимо установить наиболее приоритетные задачи мониторинга ИБ СПД, а именно:

- контроль исключения использования заводских (простых) паролей доступа к телекоммуникационному оборудованию (ТКО), контроль за сменной паролей к ТКО СПД [2];
- контроль использования уникальных IP-адресов для ТКО СПД;
- контроль подлинности подключения к ТКО СПД (для предотвращения замены оборудования);
- проверка правильности настроек правил фильтрации и маршрутизации на ТКО СПД;
- контроль правильности настроек туннелирования на ТКО СПД;
- контроль корректности настроек VLAN (VPN) в СПД;
- контроль актуальности используемых учетных записей (настройка DNS-сервера и ActiveDirectory) в СПД;

- контроль отключения (блокированием) неиспользуемых портов ТКО СПД;
- контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через общедоступный сегмент СПД (с целью исключения передачи конфиденциальной информации);
- контроль качества каналов связи.

В целях обеспечения информационной безопасности предприятия и организации, применяющие в процессе деятельности информационные и автоматизированные системы, используют *SIEM* системы. Системы *SIEM* (*Security Information and Event Management*) – это инструменты, которые осуществляют непрерывный мониторинг информационных систем, производят анализ событий безопасности в режиме реального времени, исходящих от сетевых устройств, средств защиты информации, IT-сервисов, инфраструктуры систем и приложений, а также помогают выявлять инциденты информационной безопасности [3].

SIEM системы выполняют важные функции сбора, анализа и уведомления о событиях безопасности, но не способны предотвращать угрозы. Они осуществляют сбор данных из различных источников, их хранение для последующего анализа, а также корреляцию и обработку, предоставляя инструменты для экспертного анализа событий и оповещение администраторов.

Крупные предприятия разных отраслей являются основными пользователями *SIEM*-решений [4]. Эти системы позволяют обнаруживать нарушения безопасности среди большого объема событий и оперативно реагировать на них. Кроме того, *SIEM*-системы принимают участие в проведении аудитов для проверки соответствия требованиям безопасности.

SIEM система собирает данные о событиях безопасности из различных источников, включая системы аутентификации, антивирусы, межсетевые экраны, системы обнаружения вторжений, прокси-серверы, сетевые устройства, журналы событий серверов и рабочих станций, журналы аудита баз данных, почтовые и файлообменные серверы, а также другие бизнес-приложения. Это позволяет обеспечить полный охват событий в информационно-технологической и безопасной информационной инфраструктуре предприятия [5].

Полученную информацию *SIEM* анализирует с использованием правил, содержащих набор условий, триггеров, счетчиков и сценариев ответных действий. Хотя *SIEM* не способна противодействовать злонамеренным действиям нарушителей, данное решение обеспечивает наиболее полное представление о возникающих событиях безопасности.

В России *SIEM*-системы востребованы крупным бизнесом и государственными учреждениями. Корпорации ищут высокопроизводительные, масштабируемые и надежные решения. Коммерческий сектор ценит соотношение «цена-качество». Государственные учреждения также требуют

сертификацию по требованиям регуляторов. *SIEM* используются для создания центров оперативного управления (*SOC*), которые объединяют события из разных источников, проводят анализ и оповещают о нарушениях информационной безопасности.

На фоне растущего интереса к концепции «импортозамещения», на рынке появились отечественные решения *SIEM*. Компания «Первый Русский *SIEM*» представила систему *RUSIEM*, а компания *Positive Technologies* предложила *MaxPatrol SIEM*. Кроме того, НПО «Эшелон» усовершенствовала свою систему КОМРАД. Хотя существуют и другие производители *SIEM*-систем (например, *Tibco Loglogic*, *OSSIM*, *SIEM Security Capsule* от российской компании ООО «ИТБ», *SearchInform* и другие), их доля на российском рынке пока незначительна.

Рассмотрим возможности некоторых *SIEM*-систем подробнее.

1. *Ankey SIEM* – это инновационный программный комплекс, разработанный компанией «Газинформсервис» в сотрудничестве с лидером отрасли HPE [6].

Основные особенности *Ankey SIEM*:

- основано на высокотехнологичном ядре HPE *ArcSight*, признанном эталоном в области *SIEM*-решений;
- предоставляет широкий спектр поддержки и опыт ведущего мирового производителя *SIEM*-технологий;
- имеет уникальный движок для интеграции с «нестандартными» источниками информации через передовые механизмы сбора событий;
- включает дополнительные программные модули для расширенного анализа и визуализации данных, а также контроля целостности конфигураций;
- обеспечивает инструментарий для индивидуальной, комплексной и модельной обработки событий для выявления потенциальных взаимосвязей и инцидентов;
- предоставляет эффективный анализ данных с помощью сценарного подхода, интерактивных отчетов и исследовательской аналитики;
- позволяет интерактивно формировать выборки данных и использовать различные формы их представления;
- предоставляет оценку эффективности защитных мер и самой *SIEM*-системы;
- включает механизмы оценки эффективности расследования инцидентов кибербезопасности;
- анализирует статистические показатели и выявляет отклонения от нормальной работы источников и *SIEM*-системы;
- предоставляет «высокоуровневые» панели для управленческой оценки общей безопасности организации.

На основании Приказа Минкомсвязи России от 21.07.2017 № 382 программный комплекс *Ankey SIEM* зарегистрирован в едином реестре российских программ для ЭВМ и БД под регистрационным № 3685.

Планируется сертификация программного комплекса *Ankey SIEM* по требованиям ФСТЭК.

Анализ возможностей *Ankey SIEM* показал, что данный комплекс позволяет решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества связи каналов

2. *MaxPatrol SIEM* – является продуктом российской компании *Positive Technologies* и тесно интегрирован с другими решениями компании [7]. Он доступен как в программном, так и в программно-аппаратном исполнении (*MaxPatrol SIEM LE*).

Уникальной особенностью *MaxPatrol SIEM* является актив-ориентированный подход, который обеспечивает стабильную работу системы в условиях изменений в ИТ-инфраструктуре компании. Правила корреляции определяются не для конкретных IP-адресов или их групп, а для динамических групп активов (компьютеров, серверов и прочего), формируемых по определенным признакам и подверженных изменениям по мере развития сети.

Информация в *MaxPatrol SIEM* постоянно обновляется новыми данными об ИТ-инфраструктуре, полученными из новых событий, результатов сканирования, сетевого трафика и данных от агентов на конечных точках, что создает полную ИТ-модель предприятия. Эта функция позволяет оценивать возникающие инциденты с учетом конкретных узлов сети и уменьшает количество ложных срабатываний за счет анализа событий в контексте текущих параметров хостов.

MaxPatrol SIEM успешно применяется для создания Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Преимущества *MaxPatrol SIEM* включают:

- полноценный функционал управления активами, позволяющий создавать и обновлять группы активов по различным критериям;
- автоматическое построение и обновление топологии сети, что улучшает понимание инфраструктуры и упрощает расследование инцидентов;
- автоматическое определение приоритета инцидентов на основе важности активов, что снижает нагрузку на операторов системы;
- наличие открытого стандартизированного API, для интеграции с другими системами.

MaxPatrol SIEM входит в реестр российского ПО № 1143, имеет сертификат Минобороны РФ № 3044 и сертификат ФСТЭК России № 3734.

Анализ возможностей *MaxPatrol SIEM* показал, что данный комплекс позволяет также решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи.

3. *RuSIEM* – инновационная разработка отечественной компании РУСИЕМ, являющейся резидентом Сколково и работающей над этим проектом с 2014 года. Это решение обеспечивает централизованный и распределенный сбор событий из различных систем, включая СКУД (системы контроля и управления доступом), автоматическое обнаружение инцидентов в области информационных технологий, информационной безопасности и бизнес-процессов с использованием правил корреляции и механизмов искусственного интеллекта [8].

RuSIEM состоит из нескольких модулей, один из которых *Analytics. RuSIEM Analytics* – модуль, который можно установить дополнительно к основной системе *RuSIEM*, предназначен для обнаружения атак и аномалий в режиме реального времени без необходимости создания специальных правил корреляции.

Этот модуль позволяет:

- обнаруживать инциденты с помощью искусственного интеллекта и анализа симптомов;
- автоматически создавать карту ИТ-активов на основе данных из событий и трафика;
- оценивать соответствие стандартам безопасности и внутренним политикам по техническим параметрам, включая пользовательские стандарты;
- генерировать подробные аналитические отчеты, включающие сложные расчеты и анализы.

RuSIEM предлагает широкий набор визуализаций данных, включая дашборды, карту взаимосвязей, выборки по событиям, аналитику, отчеты и инциденты [9]. Это решение также позволяет отслеживать активности и доступы персонала с новых устройств и приложений, таких как другие браузеры, IP-адреса и операционные системы.

Анализ возможностей *RuSIEM* показал, что данный комплекс позволяет также решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи [10].

Заключение. Результаты анализа отечественных средств, применяемых для мониторинга ИБ, говорят о том, что в последние годы отечественные решения в области системы комплексной безопасности и мониторинга ИБ продемонстрировали значительное развитие и успешно конкурируют на

глобальном рынке. Однако, они не в полной мере позволяют решать приоритетные задачи мониторинга ИБ, так как в них не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи. В связи с чем необходимо устанавливать дополнительные системы, что влечет избыточность, влияющую на объемы вычислительных мощностей, необходимых для эксплуатации всех продуктов, обеспечивающих ИБ.

Список используемых источников

1. Бутакова Н. Г., Трунова А. А. Анализ интеграции средств мониторинга и аудита информационной безопасности корпоративной сети // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 534–538.

2. Шевченко А. А. Предложения по построению упреждающей системы управления информационной безопасностью информационной системы // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 года. СПб.: ФГКВОУВО «Военная академия связи имени Маршала Советского Союза С.М. Буденного» МО РФ, 2020. С. 248–256.

3. Соколов А. М. Современные решения в области информационной безопасности локальных сетей // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы XIII Межрегиональной научно-практической конференции, Брянск, 30 апреля 2021 года. Брянск: Брянский государственный технический университет, 2021. С. 244–248.

4. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4(89). С. 67–76. DOI: 10.15217/issnl684-8853.2017.4.67

5. Попов С. В., Шамкин В. Н. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности // Вестник Тамбовского государственного технического университета. 2012. Т. 18. № 1. С. 27–37.

6. Липатников В. А., Коршунов Г. И., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4(95). С. 61–72. DOI: 10.31799/1684-8853-2018-4-61-72

7. Нашивочников Н. В., Лукашин А. А., Большаков А. А. Применение аналитических средств в системе операционного мониторинга и анализа безопасности кибер-физических систем для предприятий топливно-энергетического комплекса // Математические методы в технике и технологиях (ММТТ). 2019. Т. 2. С. 63–67.

8. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры / В. А. Липатников, // Информационные системы и технологии. 2016. № 2(94). С. 128–140.

9. Гончарова Т. С. Сравнение и выбор средств мониторинга событий информационной безопасности // Colloquium-Journal. 2019. № 28-2(52). С. 20–22.

10. Бухарин А. В., Ишимов А. С., Кузин П. И. [и др.] Способ прогнозирования состояния объектов связи и информации // Телекоммуникации. 2023. № 2. С. 16–22. DOI: 10.31044/1684-2588-2023-0-2-16-22

УДК 681.5
ГРНТИ 50.03.03КОРРЕКЦИЯ СИСТЕМ АВТОМАТИЧЕСКОГО
УПРАВЛЕНИЯ И МОДЕЛИРОВАНИЕ

О. И. Золотов, Т. В. Матюхина, М. Б. Олефиренко, С. М. Сотенко

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

В теории линейных систем автоматического управления широкое распространение получил метод синтеза корректирующих устройств по логарифмическим частотным характеристикам, однако при моделировании более удобной оказывается работа с передаточными функциями системы. Переход к передаточным функциям позволяет более гибко применять различные методы оптимизации структуры проектируемой системы. Статья посвящена обоснованию, разработке и совмещению этих подходов в единую методику.

системы автоматического управления, частотные характеристики, передаточные функции системы

В системах автоматического управления часто встречается задача синтеза корректирующих устройств по заданным качественным показателям переходного процесса и заданной статической ошибки. Таких методик известно несколько. Наиболее удобной и достаточно долго используемой является идея синтеза, основанная на прямой связи качественных показателей переходного процесса с логарифмическими частотными характеристиками разомкнутой системы. Идею этого метода предложил в свое время Солодовников В. В., и она представляет собой следующее: поскольку существует однозначная связь между такими показателями как время регулирования t_p , перерегулирование σ в % и видом логарифмической частотной характеристики, то можно по заданным показателям качества сформировать желаемую логарифмическую амплитудно-частотную характеристику разомкнутой системы [1]. Пример такой характеристики приведен на рис. 1.

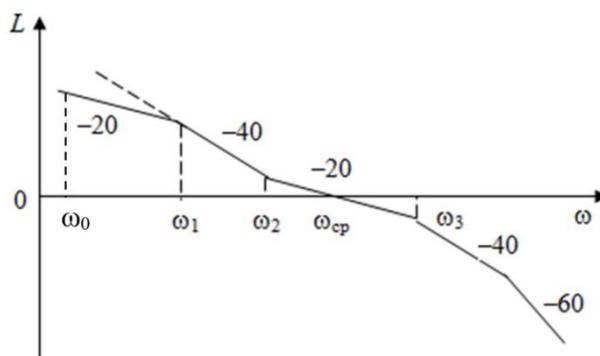


Рис. 1. Желаемая ЛАЧХ разомкнутой системы

Обычно синтез желаемой характеристики необходимого вида состоит из трех частей: синтез области низких частот (НЧ) $0 \leq \omega \leq \omega_2$, синтез области средних частот (СЧ) $\omega_2 \leq \omega \leq \omega_3$ и синтез высокочастотного участка $\omega_3 \leq \omega \leq \infty$. Но для определенности рассмотрим простейший случай синтеза для статической системы, в которой задано t_p , перерегулирование σ и статическая ошибка. Первое, что делается, определяется частота среза ω_{cp} в области средних частот. Для этого используется номограмма, представленная на рис. 2.

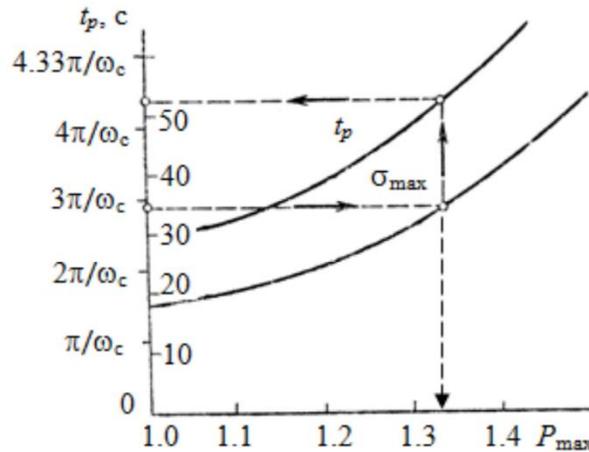


Рис. 2. Номограмма В.В. Солодовникова для определения частоты среза ω_{cp}

По диаграмме на рис. 2 определяем частоту среза ω_{cp} . А по номограмме, представленной на рис. 3, вычисляем длину этого среднечастотного участка, определяемого частотами ω_2 и ω_3 .

Наклон характеристики должен быть -20 дБ на декаду, и после того, как определяется длина этого участка в виде ΔL , представленной на номограмме, можно определить границы СЧ участка в виде значения частот ω_2 и ω_3 . НЧ участок в нашем случае, поскольку система статическая, будет представлять собой горизонтальную линию, идущую на уровне $20 \lg K$, где K – коэффициент усиления разомкнутой системы, который полностью определяет статическую ошибку. Точка пересечения горизонтального участка с желаемой ЛАХ обозначим ω_0 . Тогда желаемая ЛАХ полностью определится частотами сопряжения ω_0 , ω_1 , ω_2 и ω_3 .

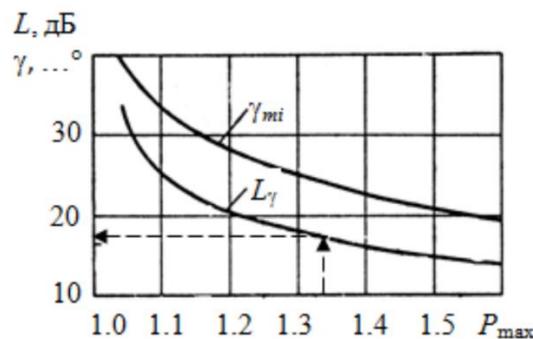


Рис. 3. Номограмма для определения длины среднечастотного участка

Получив желаемую характеристику разомкнутой системы и зная частотные характеристики нескорректированной системы, достаточно легко получить частотную характеристику корректирующего устройства графически. Далее осуществляем практическую реализацию частотной характеристики в виде реального устройства. В статье предлагается совместить этот подход с современными возможностями получения реальных устройств в виде их цифровых двойников. Поэтому мы заменяем желаемую частотную характеристику разомкнутой системы на соответствующую желаемую передаточную функцию разомкнутой системы. Для представленной характеристики соответствующая передаточная функция будет иметь вид:

$$W(p) = \frac{K(T_2p+1)}{(T_0p+1)*(T_1p+1)*(T_3p+1)}.$$

Эта операция очень легко формализуется в виде алгоритма программы и может быть легко реализована доступными средствами. Таким образом мы получаем решение первой части задачи в виде алгоритма получения желаемой передаточной функции разомкнутой системы. А далее можно получить передаточную функцию корректирующего устройства, имея передаточную функцию нескорректированной системы. Рассмотрим в данном случае один из простейших вариантов, когда систему можно разбить на две части: корректирующее устройство и нескорректированная часть, соединённые последовательно. Тогда передаточная функция будет:

$$W_{\text{КУ}}(p) = \frac{W_{\text{ж}}(p)}{W_{\text{нс}}(p)}.$$

Таким образом, общая передаточная функция будет равна желаемой, и тогда легко получить передаточную функцию корректирующего устройства. Поскольку передаточная функция КУ может быть представлена в виде отношения полиномов, то в таком виде она легко реализуется с помощью любых программных продуктов, таких как MATLAB, Simulink или программа имитационного моделирования CLASSIC. Реализация базируется на структурном подходе, в соответствии с которым сначала формируется структура, которую можно реализовать из нескольких соединённых элементов или из одного элемента. А затем в каждый элемент вводится передаточная функция, соответствующая непосредственно той передаточной функции, которую нужно моделировать. При моделировании передаточная функция вводится в виде коэффициентов полинома числителя и полинома знаменателя.

Затем встает вопрос о практической реализации этого корректирующего устройства. В случае, если удастся общую передаточную функцию разомкнутой системы получить равной желаемой, то в силу однозначности

связи передаточной функции и частотных характеристик с качественным показателем переходного процесса мы можем гарантировать при замыкании такой системы обеспечение заданных качественных показателей. Реализация корректирующего устройства возможна в виде определенных реальных элементов, как это делалось раньше. Но в данном случае предлагается, и это значительно удобнее, использование цифрового двойника модели корректирующего устройства в качестве реального звена системы автоматического регулирования. Таким образом предлагается идея – синтез желаемой передаточной функции и ее дальнейшая реализация в виде цифрового двойника. Естественно, если необходимо сочетание непрерывных сигналов с моделируемыми числовыми величинами, то необходимо использовать соответствующие аналого-цифровые или цифро-аналоговые преобразователи, что в принципе может быть очень легко реализовано. В данном случае рассмотрен сравнительно простой вариант, но предлагаемая процедура легко масштабируется как для систем с астатизмом первого порядка, так и для систем второго и т.д. порядка. При этом в данных случаях коэффициент усиления будет определять не статическую ошибку, а ошибку соответствующего уровня слежения при различных вариантах включения корректирующего устройства. Различные варианты получения формулы для передаточной функции корректирующего устройства определяется общей структурной теорией, которая достаточно широко изложена в различных работах [2–4].

Список используемых источников

1. Душин С. Е., Зотов Н. С., Имаев Д. Х. и др. Теория автоматического управления: учебник для вузов / под ред. В. Б. Яковлева. М.: Высшая школа, 2003. 562 с.
2. Золотов О. И., Пустыльников Л. М. Управленческая парадигма (избранные главы): монография. СПб.: СПбГУТ. 2021. 340 с.
3. Даринский Ю. В., Золотов О. И., Пустыльников Л. М. Теория управления: управление структурами: монография. СПб.: Изд-во «Элмор» / ООО «Техномедиа», 2012. 276 с.
4. Даринский Ю. В., Золотов О. И., Пустыльников Л. М., Фейгин О. О. Об управлении состоянием к управлению структурой: монография. СПб.: СПбГУТ, 2019. 286 с.

УДК 517.977.1
ГРНТИ 50.03.03

О РОЛИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ПРИНЯТИЯ РЕШЕНИЯ, ПРИМЕНИТЕЛЬНО К УПРАВЛЕНИЮ СТРУКТУРАМИ С ОБРАТНОЙ СВЯЗЬЮ

О. И. Золотов, Т. В. Матюхина, О. В. Раковский

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

Классические системы автоматического управления с обратной связью могут быть применены во многих областях. При этом они могут сочетаться с использованием искусственного интеллекта. Однако, до сих пор не определено место искусственного интеллекта в системах с обратной связью. Можно рассмотреть данный вопрос на примере принятия решения в медицинской области, где присутствует большое количество вербальной информации, а нечеткие границы решений приводят к задействованию механизмов нечеткой логики.

методы лечения, теория управления, принцип обратной связи, нейронная сеть, экспертная система

Классическая система автоматического управления с обратной связью строится на следующей логике. Есть объект управления. Его выходная координата измеряется и сравнивается с заданным значением. Разность этих величин, после ряда преобразований, подается на вход объекта, и система автоматически стремится эту разность свести к нулю.

Соответствующий подход может быть применен в различных областях. При этом классическая система может сочетаться с системами принятия решений и, таким образом, с использованием искусственного интеллекта. Однако, до сих пор нет оценки места искусственного интеллекта в классических структурах с обратной связью. Эту задачу можно рассмотреть на различных примерах, где необходимо использовать алгоритмы принятия решения. Одним из подходящих вариантов являются системы принятия решений в медицинской области.

Классическая схема лечения пациента основана на определенной последовательности действий. На основании симптомов заболевания и результатов анализов врачом определяется необходимая медикаментозная терапия. Пациент проходит курс лечения, в результате которого наблюдаемые показатели его здоровья изменяются, в сторону улучшения, ухудшения или остаются неизменными. Полученные таким образом данные анализируются лечащим врачом, который в результате принимает решение о продолжении лечения, изменения дозировки применяемых средств, прекращения курса

лечения или другие корректирующие рекомендации. Такой процесс носит циклический характер и может быть представлен схемой (рис. 1).



Рис. 1. Структурная схема медикаментозного лечения пациента

Если сравнить между собой схему лечения и систему управления с обратной связью, можно увидеть их сходство. Таким образом, можно использовать математический аппарат для описания процесса лечения.

Пусть структура R_1 – это структура, рассматриваемая нами без стабилизирующих обратных связей и в отсутствии возмущений, отождествляемая одиночным блоком R_1 (рис. 2).

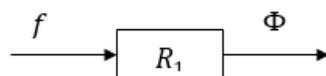


Рис. 2. Блок структуры R_1

В качестве такого первоначального объекта, т. е. блока R_1 может выступать пациент, к которому применяется некоторое медикаментозное воздействие f , после чего берутся анализы, являющиеся результатом такого воздействия Φ .

Необходимо контролировать процесс лечения и вносить корректировку в терапию. Для этой цели замкнем структурную схему на рис. 2 обратной связью. Пусть блок R_{oc} – блок цепи (канала) обратной связи. Соединение нескольких таких блоков может быть заменено одним блоком с оператором R (рис. 3).

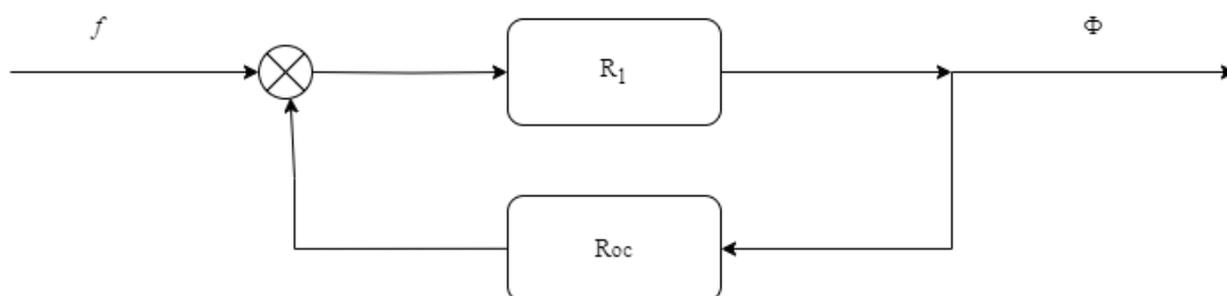


Рис. 3. Структурная схема R

Операторное соотношение, связывающее в новой структурной схеме операторы блоков R_1 , R_{oc} и R , запишется в виде:

$$R = \frac{R_1}{(1 - R_1 R_{oc})} = (1 - R_1 R_{oc})^{-1} R_1 \Leftrightarrow R = R_1 \circ R_{oc}. \quad (2)$$

Таким образом, нам удалось связать традиционный метод лечения с хорошо известным аппаратом, описывающим классическую схему системы управления с обратной связью.

Дальнейшую автоматизацию медикаментозного воздействия можно предположить в виде применения экспертной системы (ЭС). Для этого представляется удобным использовать продукционную модель, основанную на правилах выбора необходимой корректирующей обратной связи, в соответствии с изменяемыми входными параметрами. Такими параметрами могут быть численные или качественные результаты анализов, полученных у пациента.

В качестве примера рассмотрим случай лечения анемии у пациента с недостаточным содержанием железа в крови.

Анамнез = анемия на фоне низкого уровня железа.

Медикаментозное воздействие = препарат Фенюльс или Сорбифер Дурулес

Анализ = уровень железа.

ЭС получает в качестве входных данных Анализ, а также информацию о длительности лечения. В зависимости от показателя уровня железа (низкий/высокий) и продолжительности курса лечения выбирается соответствующее правило из базы знаний. Результатом применения соответствующего правила будет рекомендация продолжить курс лечения, изменение дозировки препарата, если необходимо, отмена препарата с консультацией врача, прекращение курса терапии с рекомендацией по срокам возобновления курсового приема. Если же срок лечения превышает установленный срок, а результата достичь не удастся, информация о пациенте передается для консультации врача.

В отличие от использования для выработки рекомендаций нейронных сетей, когда основное внимание уделяется наиболее вероятному варианту событий и состояний, применение экспертных систем позволяет получать рекомендации по дополнительному обследованию и методам лечения на основании базы знаний, аналогичной той, которая используется человеком.

Тем не менее, применение нейронных сетей может быть эффективно при распознавании и вероятностной классификации признаков заболевания, путем анализа снимков, выполненных медицинским оборудованием (рентген, УЗИ), фотографий выявленных внешних поражений кожи, а также совокупности параметров результатов анализов.

Результирующая структура может быть представлена в виде рис. 4.

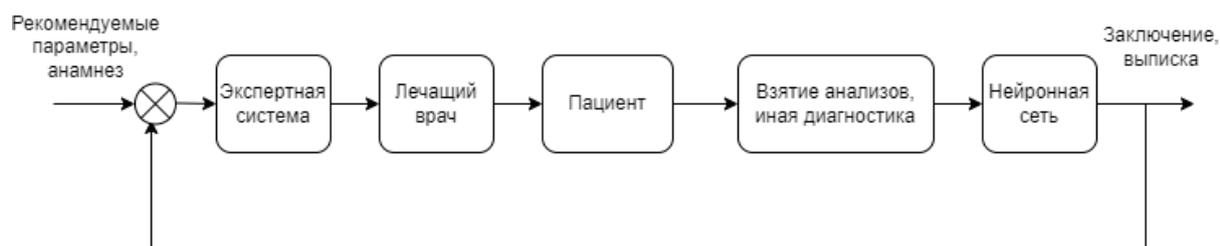


Рис. 4. Структурная схема автоматизированной системы выработки медицинских рекомендаций

Несмотря на то, что в схеме предусмотрена имитация деятельности медицинского специалиста, учитывая влияние решений на здоровье человека, соответственно и цену ошибки, в схеме учитывается присутствие лица, принимающего решение (ЛПР), ответственного за конечный результат лечения. На схеме в качестве ЛПР выступает Лечащий врач.

Подобная схема может быть применена не только в чисто медицинской системе, но и в смежных областях, например, в спорте. В качестве входящего воздействия могут выступать показатели нагрузки, режима дня, питания, медицинской стимуляции. В качестве выходных данных могут быть показатели мониторинга состояния организма, анализы, спортивные достижения.

Учитывая множество критериев, влияющих на процесс лечения или спортивные достижения, можно рассматривать человека не просто как объект, а как структуру, имеющую множество внутренних параметров, которые не всегда просто представить математически. Таким образом, представляется использовать вместо механизма управления с обратной связью механизм управления структурами, рассмотренный в [1–4].

Список используемых источников

1. Бутковский А. Г., Бабичев А. В., Похьюлайнен С. К единой геометрической теории управления. М.: Наука, 2001. 352 с.
2. Золотов О. И., Пустыльников Л. М., Даринский Ю. В., Фейгин О. О. От управления состоянием к управлению структурой. СПб.: СПбГУТ, 2019. 287 с.
3. Золотов О. И., Пустыльников Л. М. Теория управления и сохранение структур. СПб.: СЗТУ, 2011. 319 с.
4. Золотов О. И., Матюхина Т. В., Раковский О. В. Использование принципа обратной связи в управлении структурами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. Т. 2. С. 663–666.

УДК 517.929.4
ГРНТИ 27.23.21

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ РЕШЕНИЙ ЛИНЕЙНЫХ СИСТЕМ НА БАЗЕ ОПЕРАЦИОННОГО ИСЧИСЛЕНИЯ

Н. С. Измайлов, Е. Р. Искулов, В. В. Курдубова

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

В данной работе рассматриваются такие приложения теории функций комплексного переменного, как операционное исчисление и теория устойчивости. Операционное исчисление является мощным инструментом для анализа и проектирования систем управления, а теория устойчивости позволяет оценить устойчивость динамических систем и предсказать их поведение в различных условиях. Применение методов операционного исчисления позволило решать задачи, связанные с исследованием устойчивости решений линейных дифференциальных уравнений. Для некоторых известных аналитических критериев устойчивости, были написаны консольные приложения на языке С.

операционное исчисление, теория устойчивости, С++

Теория функций комплексного переменного является одной из фундаментальных областей математики, которая нашла широкое применение в различных областях науки и техники [1].

С помощью операционного исчисления можно анализировать свойства систем-управления, такие, как: устойчивость, чувствительность к возмущениям, способность подавлять шумы. Кроме того, операционное исчисление позволяет проектировать системы управления с заданными свойствами, оптимизировать их параметры и улучшать производительность.

Применение методов теории устойчивости способствует оценке устойчивости систем при помощи анализа корней характеристического уравнения. Эти методы позволяют определить, какие значения параметров системы приводят к устойчивости или неустойчивости системы. Также теория устойчивости позволяет проектировать системы с заданными свойствами устойчивости и оптимизировать их параметры.

Примерами применения операционного исчисления и теории устойчивости являются проектирование автоматических регуляторов для промышленных процессов, управление роботами и автоматических транспортных систем, анализ и проектирование электронных цепей и систем связи, а также моделирование и управление физическими системами, такими как летательные аппараты и автомобили [2].

Различные интегральные преобразования функций могут оказаться очень полезными при решении систем линейных дифференциальных уравнений. Многие из них основаны на теории функций комплексного переменного.

Одним из них является **преобразование Лапласа**:

$$F(p) = \lim_{b \rightarrow +\infty} \int_0^b e^{-pt} f(t) dt = \int_0^{+\infty} e^{-pt} f(t) dt$$

где параметр $p = \sigma + i\omega$ – комплексное число, $\sigma = Re p, \omega = Im p$ [3].

Практические применения линейного преобразования Лапласа основаны на его основных свойствах, теореме о дифференцировании и теореме об интегрировании оригинала функции.

Благодаря этим теоремам одним из важных приложений операционного исчисления является решение линейных обыкновенных дифференциальных уравнений с постоянными коэффициентами. Схема решения задачи Коши с помощью преобразования Лапласа приведена на рис. 1.

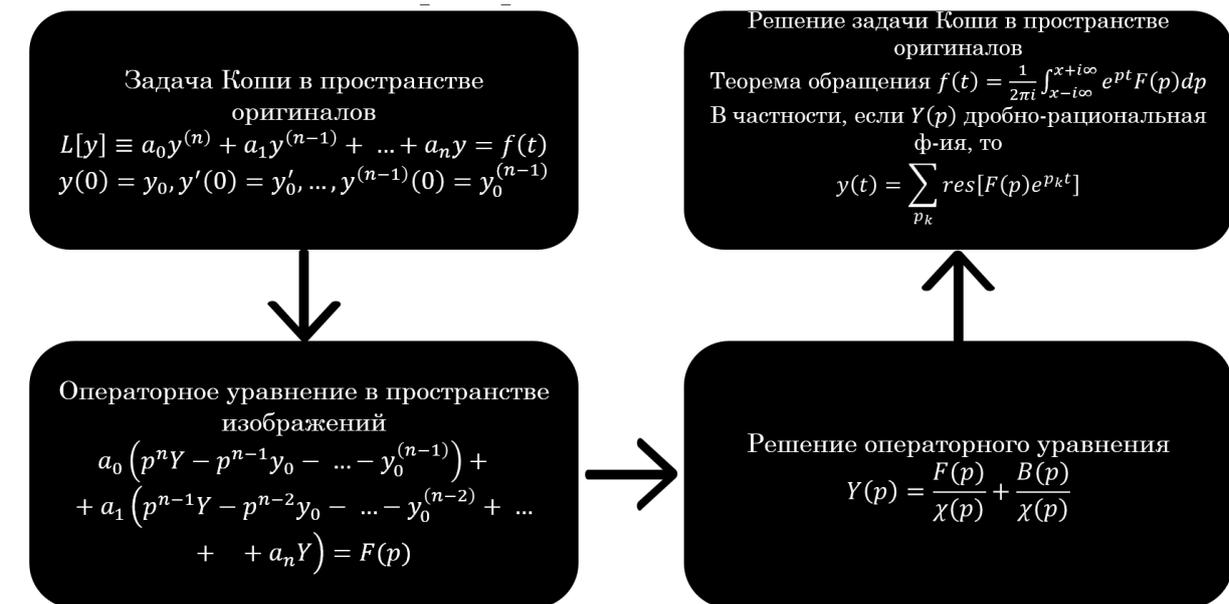


Рис. 1. Схема решения задачи Коши

Базируясь на операционном исчислении, можно исследовать устойчивость решений линейных дифференциальных уравнений.

На рис. 2 изображено устройство, которое преобразует входной сигнал $f(t)$ в реакцию (отклик) системы $y(t)$.

Устойчивость линейной системы подразумевает, что система, находящаяся в состоянии равновесия, после воздействия на нее (возмущении)

должна возвращаться к состоянию равновесия. Другими словами, устойчивая система способна сохранять свое равновесное состояние при небольших изменениях входных параметров или возмущающих воздействиях [4, 5].

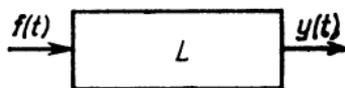


Рис. 2. Устройство преобразования сигнала

Исследование устойчивости решения линейной системы сводится к исследованию устойчивости тривиального решения соответствующего ему линейного однородного дифференциального уравнения (далее – ЛОДУ). То есть, при изучении вопросов устойчивости решений ЛОДУ достаточно ограничиться исследованием устойчивости его нулевых решений.

Имеют место следующие теоремы.

Теорема А. Для того, чтобы линейная система, описываемая обыкновенным линейным дифференциальным уравнением с постоянными действительными коэффициентами, была асимптотически устойчивой, необходимо и достаточно, чтобы все корни p_k характеристического многочлена $\chi(p)$ оператора L имели отрицательные действительные части, т.е. $Re p_k < 0$.

Теорема Б (необходимое условие устойчивости Стодолы): для того, чтобы многочлен с действительными коэффициентами:

$$P(z) = z^n + a_1 z^{n-1} + \dots + a_n$$

был многочленом Гурвица, необходимо, чтобы все его коэффициенты были положительными [6].

Использование характеристического уравнения для проверки устойчивости системы может быть затруднительным в случае высоких порядков систем. Существуют специальные критерии, основанные на теоремах А и Б, что значительно упрощает процедуру проверки устойчивости. Первый критерий – критерий устойчивости Рауса -Гурвица; второй – критерий Льенара -Шипара.

На основе этих критериев был разработан программный код (на языке С++). Приведем ниже кратко его алгоритм.

Алгоритм вычисления критерия устойчивости Рауса-Гурвица

1. Начало программы.
2. Создание массива для хранения данных.
3. Ввод исходных данных.
4. Создание дополнительного массива для матрицы Гурвица. Его обработка.

5. Проверка условия на положительность всех главных диагональных миноров матрицы Гурвица.

6. Вывод в консоль ответа.

7. Конец программы.

Заметим, что если хотя бы один из определителей критерия Рауса Гурвица меньше нуля, то система будет неустойчивой. При этом, если первый определитель отрицателен, то процесс проверки устойчивости прекращается. Если же отрицательных определителей нет, но есть определители, равные нулю, то такая система находится на границе устойчивости, то есть является нейтральной.

Для исследования устойчивости систем автоматического управления (далее – САУ), имеющих порядок характеристического уравнения $n \geq 5$, удобно применять одну из модификаций алгебраического критерия устойчивости Гурвица, предложенную в 1914 г. П. Лъенаром и Р. Шипаром.

Алгоритм критерия устойчивости Лъенара-Шипара подобен алгоритму нахождения критерия устойчивости Рауса-Гурвица. Однако, он отличается тем, требуется вдвое меньше расчетов главных диагональных миноров матрицы Гурвица, что удобно при исследовании САУ высоких порядков.

Отметим, что алгебраические критерии устойчивости позволяют лишь установить, устойчив или неустойчив процесс регулирования. На вопрос, как быстро процесс затухает, они ответа не дают. Может оказаться, что САУ устойчива, но переходный процесс в ней затухает чрезвычайно медленно, и такая система оказывается практически непригодной к использованию. Оценка влияния на устойчивость параметров того или иного звена требует дополнительных исследований. Вместе с тем, когда известны значения коэффициентов характеристического уравнения и требуется установить лишь факт наличия, применение алгебраических критериев позволяет быстрее достичь цели.

Список используемых источников

1. Фукс Б. А., Левин В. И., Функции комплексного переменного и их приложения, 1951. 308 с.
2. Соломенцев Е. Д., Функции комплексного переменного и их применения: учеб. пособие для студентов вузов. М.: Высш. шк., 1988. 167 с.
3. Краснов М. Л., Киселев А. И., Макаренко Г. И. Функции комплексного переменного. Операционное исчисление. Теория устойчивости. 1971. 256 с.
4. Меркин Д. Р. Введение в теорию устойчивости движения, изд. 3-е, 1987. 304 с.
5. Краснов М. Л., Киселев А. И., Макаренко Г. И. Операционное исчисление. Теория устойчивости: задачи и примеры с подробными решениями: учеб. пособие.
6. Романовский П. И. Ряды Фурье. Теория поля. Аналитические и специальные функции. Преобразование Лапласа, 1957. 292 с.

Статья представлена научным руководителем, кандидатом технических наук начальником научно-исследовательского отдела научно-исследовательского центра Тихоновым С. С.

УДК 004.6, 659.3
ГРНТИ 28.23.24

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ДЛЯ БОРЬБЫ С ФЕЙКОВЫМИ НОВОСТЯМИ

И. В. Ильина, А. Климов, В. П. Шелехов

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

В современном мире распространение фейковых новостей стало серьезной проблемой, подрывающей доверие к средствам массовой информации, людям и даже государствам, искажающей общественный дискурс и даже влияющей на выборы и другие важные общественные и политические деятельности. Признавая необходимость решения этой проблемы, технологические инновации все чаще используются для борьбы с распространением дезинформации. В этой статье рассматриваются различные технологические решения и их потенциал для смягчения воздействия поддельных новостей в цифровом обществе.

фейк, массовая информация, блокчейн, ИИ, искусственный интеллект, данные, новости

Начнем с понятия фейковой новости-Информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных (СМИ) с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду. Авторы поддельных новостей часто используют броские заголовки или полностью сфабрикованные истории для увеличения читательской аудитории и цитируемости [1].

Один из основных технологических подходов к борьбе с фейковыми новостями предполагает разработку сложных алгоритмов и моделей машинного обучения и ИИ (это отдельное направление компьютерных наук, которое занимается разработкой систем, анализирующих информацию и решающих задачи аналогично тому, как это делает человек).

Эти алгоритмы анализируют множество факторов, включая достоверность источника, соответствие информации известным фактам и язык, используемый для передачи сообщения. Используя огромные объемы данных, эти алгоритмы могут обнаруживать и помечать потенциально вводящую в заблуждение или ложную информацию, тем самым сокращая ее распространение на онлайн-платформах. Важно понимать, что в настоящее время ИИ не может знать, что новость на 100% является фейком и финальную редактуру и отсеивания ложных и настоящих новостей должен осуществлять человек [2,3]. Такие компании, как Google и Facebook, вложили значительные средства в такие алгоритмы, чтобы усилить модерацию контента и уменьшить распространение поддельных новостей в своих экосистемах (рис.1).

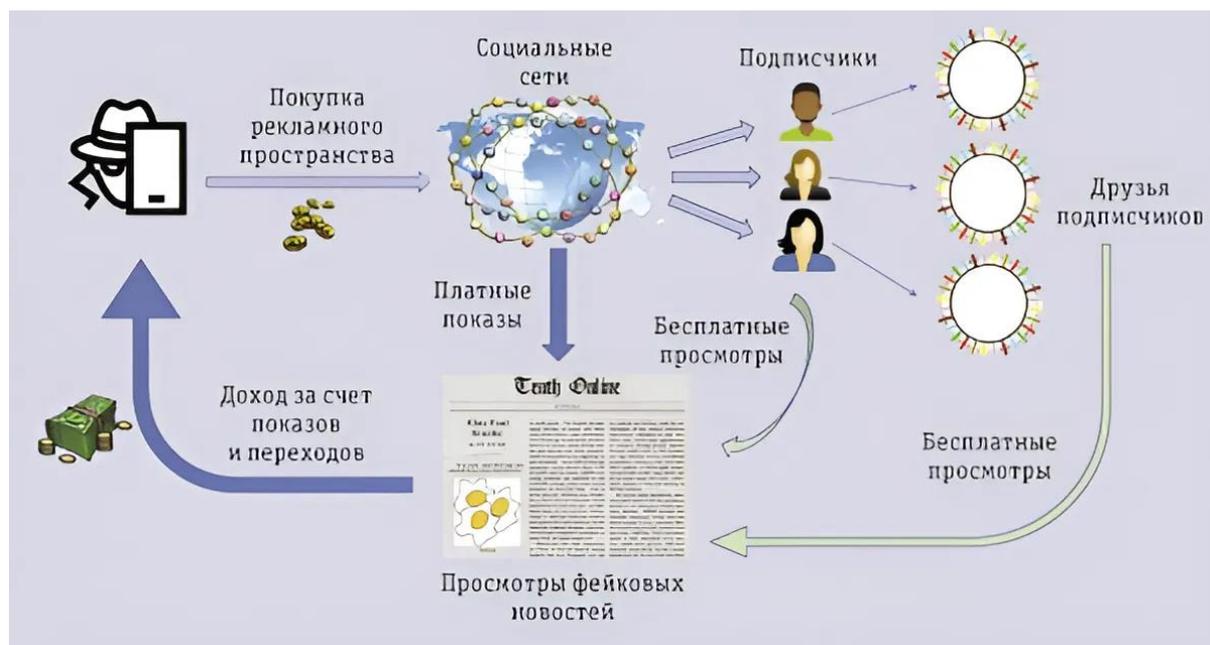


Рис. 1. Пример цифровой экосистемы и взаимосвязь с фейковыми новостями

Так же можно предложить разработку программы, которая будет после нахождения на различных площадках и мессенджерах запрещать пользователю копировать, пересылать эту новость или ставить под новостью предупреждение о возможной ложности этой информации (рис. 2). Так как после нахождения фейковой новости пройдет много времени, пока администраторы сайта или другой платформы смогут удалить или запретить распространения данной новости, или же оно вообще не захотят по тем или иным причинам скрывать новость. Но стоит помнить, что программа должна запрещать доступ только к новостям с полной уверенностью и доказательствам, что новость является фейком, например, проверяя ее на подлинность через специальный источник с уже запрещенными (фейковыми) и разрешенными (правдивыми) новостями [4]. Это поможет уменьшить распространение фейковых новостей с одной информацией. Для не подтверждённых же новостей, которые могут оказаться как правдивыми, так и ложными программа будет отсылать на оценку человеку или сохранять ее в спец. Базе до тех пор, пока она не будет определена в одну из категорий.

Другим технологическим решением является использование инструментов и сервисов проверки фактов. Эти инструменты используют методы обработки естественного языка и интеллектуального анализа данных для проверки точности новостных статей и сообщений в социальных сетях. Средства проверки фактов оценивают обоснованность утверждений путем перекрестных ссылок на информацию из авторитетных источников и выявления несоответствий или вводящих в заблуждение заявлений. То есть происходит проверка всех новостей с помощью проверки сходства с специально выбранными сайтами и источниками.



Рис.2. Пример предупреждения об фейковой новости

Предоставляя пользователям надежную информацию и прозрачные оценки новостного контента, инструменты проверки фактов дают людям возможность принимать обоснованные решения и противостоять влиянию дезинформации. Такие организации, как Snopes и FactCheck.org (рис. 3), стали пионерами в разработке таких инструментов, внося свой вклад в борьбу с фейковыми новостями.



Рис. 3. Логотип организации

Кроме того, технология блокчейн стала многообещающим решением для борьбы с фейковыми новостями за счет повышения прозрачности и прослеживаемости распространения информации. Платформы блокчейна записывают источник, содержание и временные метки новостных статей в децентрализованный реестр, предотвращая подделку и обеспечивая подлинность информации. Используя криптографические методы и механизмы консенсуса, технология блокчейн укрепляет доверие среди пользователей и снижает риск бесконтрольного распространения дезинформации. Такие проекты, как Civil и Newlines, изучают потенциал решений на основе блокчейна для продвижения честности и подотчетности в журналистике, тем самым гарантируя доступ общественности к достоверной информации [5].

В заключение, технологические решения предлагают многообещающие стратегии борьбы с распространением поддельных новостей в эпоху цифровых технологий. Используя алгоритмы, инструменты проверки фак-

тов и технологию блокчейн, мы можем коллективно смягчать распространение дезинформации и поддерживать целостность онлайн-источников информации. Решение этой сложной задачи требует многогранного подхода и множество специалистов, охватывающего технологические инновации, инициативы в области медиаграмотности и меры регулирования, направленные на формирование более информированного и жизнестойкого общества.

Список используемых источников

1. Kushnir D. Developing instrument for investigation of blockchain technology Studies in Computational Intelligence. 2022. Т. 1030. С. 123–141.

2. Аль-Нами Б. А., Афанасьев А. А., Михеев Г. Д. Актуальная информация о безопасности браузеров // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 42–45.

3. Аль-Нами Б. А., Щенникова А. В. Информационная безопасность личных данных в современном мире // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 274–277.

4. Аль-Нами Б. А., Бельский И. С. Современные методы защиты информации на серверах от атак злоумышленников // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 57–60.

5. Аль-Нами Б. А., Бордунов И. А., Минина С. А. Роль безопасности информационных данных в современном обществе // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 68–71.

Статья представлена научным руководителем, кандидатом технических наук, старшим преподавателем кафедры ИКД Аль-Нами Б. А.

УДК 621.391
ГРНТИ 81.93.29

О МАНДАТНОМ УПРАВЛЕНИИ ДОСТУПОМ

О. Б. Ильина¹, О. П. Купчиненко¹, А. В. Скоропад²

¹Военная академия связи имени Маршала Советского Союза С. М. Буденного

²Санкт-Петербургский филиал – «ЛОНИИР»

Рассмотрена реализация мандатной модели разграничения доступа в современных версиях операционной системе специального назначения «Astra Linux SE». Выполнен анализ применения специальных атрибутов мандатного управления доступом – меток. Для основных каталогов операционной системы специального назначения «Astra Linux SE» представлены примеры настроек мандатных атрибутов, уровней и категорий.

операционная система специального назначения, защита информации, права доступа, мандатная модель управления доступом, уровень, категория, метки

В современных защищенных операционных системах (ОС) может быть реализованы следующие комбинации защиты информации:

- дискреционный;
- ролевой;
- мандатный метод разграничения доступа.

Часто они реализуются в следующем порядке:

- каждый следующий настраивается после предыдущего;
- ресурс, доступный по правилам мандатного разграничения доступа, всегда доступен по правилам дискреционного доступа (не наоборот).

Система контроля доступа SELinux (Security Enhanced Linux) осуществляет принудительный контроль доступа, реализованный на уровне ядра ОС.

Вместо SELinux в операционной системе специального назначения (ОС СН) «Astra Linux SE» (начиная с версии 1.5) применяется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам, которая лишена недостатков предыдущей модели и включает дополнительные способы разграничения доступа - уровни целостности системы [1].

В отличие от классической модели мандатного управления доступом, в ДП-модели реализован мандатный контроль целостности дистрибутива и файловой системы, так же предусмотрено ролевое управление доступом [2].

В настоящее время используемая в ОС СН «Astra Linux SE» модель разграничения доступа является единственной реализованной моделью (не основанной на SELinux) в отечественных реализациях ОС СН на базе ОС Linux.

Реализация мандатного управления доступом в ОС СН «Astra Linux SE» основана на подсистеме безопасности PARSEC, которая включает:

- программный интерфейс и модуль расширения ядра ОС СН;
- поддерживающую виртуальную файловую систему /parsecfs и набор системных вызовов.

Подсистема PARSEC позволяет администраторам безопасности управлять политикой безопасности в ОС СН «Astra Linux SE».

Модель мандатного разграничения доступа задаёт список правил, которые ограничивают возможности доступа субъектов с определенным уровнем (контекстом) безопасности к объектам определенного типа. При каждом обращении происходит проверка – имеет ли право субъект с данным уровнем безопасности на данную операцию к объекту данного типа [3].

Контекст безопасности в ОС СН «Astra Linux SE» (начиная с версии 1.5) состоит из следующих компонентов:

- мандатный уровень;
- категория;
- уровень целостности.

Файл `/etc/parsec/mac_levels` содержит мандатные уровни, поддерживаемые в ОС СН.

В файле `/etc/parsec/mac_categories` перечислены поддерживаемые в ОС СН категории.

В локальном режиме выполнить настройку уровней и категорий можно с помощью утилиты «Локальная политика безопасности».

Утилиту можно вызвать из графического меню или командой `fly-admin-smc`.

Утилита «Локальная политика безопасности» решает задачи администрирования:

- создание учетных записей пользователей и групп пользователей;
- настройка параметров мандатного управления доступом, контроля целостности.

В ОС СН «Astra Linux SE» существуют объекты-контейнеры (например, каталоги), т. е. объекты, которые могут содержать другие объекты.

Специальные атрибуты мандатного управления доступом (метки) определяют максимальную метку вложенных объектов.

Тип метки может использоваться для того, чтобы изменять ее действие (таблица 1).

Дополнительные мандатные атрибуты управления доступом позволяют уточнять/изменять правила мандатного управления доступом для объектов ОС СН.

Перечисленные типы метки могут использоваться вместе.

ТАБЛИЦА 1. Метки объектов

Тип метки	Применение
ehole	Объекты-контейнеры, простые объекты (файлы). Игнорируются все мандатные правила разграничения доступа
ccnr	Объекты-контейнеры. Устанавливается правило: объект контейнер может содержать объекты с разными мандатными уровнями, но не выше уровня объекта-контейнера
ccnri	Объекты-контейнеры. Устанавливается правило: объект контейнер может содержать объекты с разными уровнями целостности, но не выше уровня целостности объекта-контейнера

В ОС СН «Astra Linux SE» (начиная с версии 1.4) возможно возникновение ситуации: при попытке изменения уровня объекта может возникнуть блокировка внесения изменений:

- на файловый объект установить мандатный уровень, выше уровня каталога, содержащего данный файловый объект запрещено;
- на каталог установить более высокий уровень не разрешено, так как каталог содержит файловые объекты с уровнями, меньше уровня, необходимого для установки.

Для устранения этих проблем используется метка `ccnr`.

Например, рекурсивно (флаг `-R` команды `pdpl-file`) изменить мандатные уровни на каталогах и добавить метку `ccnr` на каталог `test` можно командой:

```
pdpl-file -R 1:0:0:ccnr /test
```

Объект-контейнер может иметь тип: `ccnr,ccnri,ehole`.

Для каталогов ОС СН «Astra Linux SE» существуют типовые наборы мандатных уровней, категорий и меток, которые позволяют построить надежную и многофункциональную систему защиты информации в ОС (таблица 2).

Набор настроек корневого каталога указывает, что в файловой системе ОС СН могут храниться любые объекты с любыми мандатными метками. Но при этом есть следующие ограничения:

- мандатный уровень объектов не может быть выше максимально возможного значения корневого каталога;
- при этом процесс с любым уровнем доступа, например, минимальным, может обращаться внутрь корневого каталога.

Настройки каталога `/dev` разрешают создавать в ОС СН «Astra Linux SE» устройства (USB-порты), через которые можно вывести из системы конфиденциальные данные. Такая возможность может нарушить

безопасность информации и не применяется по умолчанию. Для того чтобы использовать эту возможность необходимо работать в системе с правами root (суперпользователя) и включить привилегию parsec_cap_chmac (менять мандатные метки файлов).

ТАБЛИЦА 2. Мандатные уровни, категории и метки каталогов

Каталог	Мандатный уровень, категория	Метки
/	Максимальный мандатный уровень, поддерживаемый в ОС СН	ccnr и csnri
/bin, /boot, /etc, /lib, /lib32, /lib64, /lost+found, /media, /mnt, /opt, /proc, /root, /sbin, /selinux, /srv, /sys, /usr	Нулевой мандатный уровень, нулевая маска категорий	Нет
/dev	Максимальный мандатный уровень, все мандатные категории.	ccnr
/run /var	Максимальный мандатный уровень, все мандатные категории	ccnr
/parsecfs	Нулевой мандатный уровень, нулевая маска категорий	ehole
/tmp	Максимальный мандатный уровень, все мандатные категории	ccnr ehole
/home	Максимальный мандатный уровень, все мандатные категории	ccnr
/home/pdp	Максимальный мандатный уровень, все мандатные категории	ccnr

ОС СН «Astra Linux SE» считает одного и того же пользователя с различными мандатными уровнями и категориями, как разных пользователей, создает для них разные домашние каталоги. Поэтому одновременно доступ пользователя к ним не допускается.

Домашние каталоги пользователей подвергаются процессу виртуализации в зависимости от параметров сеанса пользователя. В каталоге /home/.pdp создаются каталоги /home/.pdp/<имя пользователя>.

При инициализации сеанса пользователя в ОС СН происходит обращение к тому подкаталогу каталога /home/.pdp/<имя пользователя>, который соответствует мандатным атрибутам сеанса пользователя.

Пользователь в каждом сеансе работы с ОС СН видит в своём домашнем каталоге только те файлы и каталоги, мандатные атрибуты которых соответствуют мандатным атрибутам его сеанса.

Указанные настройки позволяют защитить данные пользователя от несанкционированного доступа.

С помощью специальных атрибутов мандатного управления доступом (меток) администратор безопасности может быстро решать задачи смены мандатного уровня на файловой системе ОС СН «Astra Linux SE».

Список используемых источников

1. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие. М.: Горячая линия – Телеком, 2018. 311 с.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу об изменениях в системе защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. Т. 2. С. 251–254.

3. Гринь Д В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

УДК 621.391
ГРНТИ 81.93.29

СЕТЕВАЯ ЗАЩИЩЕННАЯ ФАЙЛОВАЯ СИСТЕМА

О. Б. Ильина¹, О. П. Купчиненко¹, А. В. Скоропад²

¹Военная академия связи имени Маршала Советского Союза С. М. Буденного

²Санкт-Петербургский филиал – «ЛОНИИР»

Рассмотрен состав сетевой защищенной файловой системы, ее основные задачи и базовые возможности, а также представление и задачи защищенного файлового сервера и клиента сетевой защищенной файловой системы, особенности настройки файлового сервера и доступа к общему сетевому ресурсу. Проведен анализ возможностей защищенного файлового сервера и сформулированы его преимущества перед другими файловыми серверами.

сетевая защищенная файловая система, разделяемые сетевые ресурсы, файловое хранилище, монтирование сетевых ресурсов, защищенный файловый сервер

Стремительное развитие и совершенствование сетевых технологий, использование новых сетевых протоколов и увеличение объема передаваемых по локальной вычислительной сети (ЛВС) данных создают основу для организации единого пространства пользователей и ресурсов в автоматизированных системах под управлением операционной системы специального назначения в соответствии с целями, задачами и потребностями пользователей и требуют постоянного внимания к вопросам обеспечения безопасности информации.

В ЛВС могут работать компьютеры под управлением разных операционных систем таких, например, как Linux и Windows, у которых разные принципы организации сетевых ресурсов, несовместимые между собой, поэтому их нельзя просто подключить в сеть.

Для взаимодействия в ЛВС под управлением операционной системы Windows применяется клиент-серверный протокол SMB (Server Message Block). Он используется для подключения к серверам, чтобы получить доступ к файлам, каталогам и сетевым ресурсам, и для обмена информацией по межсистемным процессам.

CIFS (Common Internet File System) – это часть протокола SMB, который используется для удаленного подключения нескольких компьютеров с разными программными платформами (например, Windows и UNIX) в ЛВС. Он может идентифицировать и читать файлы, созданные в файловой системе NTFS, что позволяет использовать их между машинами с разными программными платформами, а также позволяет работать с файлами больших размеров и поддерживает символические и жесткие ссылки.

Сетевая защищенная файловая система (СЗФС), которая работает по протоколу SMB/CIFS предназначена для организации защищенных файловых серверов. По протоколу SMB/CIFS передаются сообщения, содержащие информацию о мандатной метке субъекта доступа и атрибутах безопасности (стандартных и расширенных).

Для безошибочного функционирования СЗФС в ЛВС необходимо:

- применять механизм единого пространства пользователей [1], который обеспечит однозначное соответствие между логическим именем пользователя (группы) и его идентификатором на всех серверах и рабочих станциях, используемых пользователем;
- синхронизировать UID/GID на клиенте и сервере, так как данные о группах и пользователях передаются по сети в числовом виде.

СЗФС представляет собой стандартную файловую систему, которая может работать с удаленной файловой системой, поддерживает все механизмы защиты операционной системы [2], а также позволяет разделять сетевые ресурсы (каталоги, файлы, принтеры) между пользователями сети и предоставлять общий доступ к ним.

СЗФС состоит из сервера, который представляет собой расширенный сервер Samba, и клиента, представляющего сетевую файловую систему в составе системы управления файлами ядра операционной системы и реализующего интерфейс между сервером СЗФС и виртуальной файловой системой ядра.

Сервер управляет разделяемыми ресурсами и контролирует доступ к ним. Мандатный контроль доступа к разделяемым ресурсам на стороне сервера обеспечивается тем, что при подключении клиента сервер устанавливает мандатную метку процесса в соответствии с мандатной меткой клиента. Клиент СЗФС передает на сервер информацию о классификационной метке пользователя (процесса), работающего с разделяемым ресурсом и отображает каталоги (файлы) смонтированного сетевого ресурса.

СЗФС состоит из компонентов, представленных в таблице 1. В операционной системе Astra Linux SE общий доступ к ресурсам предоставляется с помощью конфигурирования службы Samba.

Процесс настройки Samba-сервера в операционной системе Astra Linux SE состоит из следующих этапов [3]:

- проверка наличия установленных пакетов Samba-сервера;
- конфигурирование Samba-сервера;
- запуск Samba-сервера.

СЗФС не требует дополнительной установки компонентов, так как пакеты Samba-сервера и Samba-клиента в процессе установки операционной системы включается в состав устанавливаемых пакетов по умолчанию, а ее настройка осуществляется с помощью настройки параметров конфигурационного файла `/etc/samba/smb.conf`.

ТАБЛИЦА 1. Компоненты СЗФС

Название	Назначение
smbd	Сервисная служба, обеспечивающая работу службы печати и разделения файлов для пользователей операционной системы Windows. Конфигурационные параметры службы находятся в файле smb.conf.
nmbd	Сервисная служба, обеспечивающая работу службы имен NetBIOS. Может использоваться для запроса других сервисных служб имен.
smbclient	Сервисная служба, реализующая клиента для доступа к другим серверам
testparm	Команда для тестирования файла smb.conf.
smbstatus	Команда, которая сообщает, кто в настоящее время пользуется сервером smbd.
fly-admin-samba	Графическая утилита, которая позволяет настроить пользовательский доступ к ресурсам СЗФС.

Файл конфигурации smb.conf разделен на две большие секции Global Settings и Share Definitions, и состоит из трех специальных разделов [global], [homes], [printers] и нескольких пользовательских, представленных в таблице 2. Все разделы начинаются с имени раздела в квадратных скобках (например, [public]). Внутри каждого раздела представлен ряд параметров в виде строк key = value (имя = значение).

ТАБЛИЦА 2. Специальные разделы конфигурационного файла smb.conf

Раздел	Описание
[global]	В разделе описаны параметры, управляющие сервером smb в целом, а также находятся значения параметров по умолчанию для других разделов.
[homes]	Раздел позволяет подключаться к рабочим каталогам пользователей без их явного описания. При запросе клиентом определенной службы ищется соответствующее ей описание в файле и, если его нет, просматривается раздел [homes]. Если этот раздел существует, просматривается файл паролей для поиска рабочего каталога пользователя, сделавшего запрос, и, найдя его, он становится доступным по сети.
[printers]	В разделе описаны параметры управления печатью при отсутствии иного явного описания. Используется для предоставления доступа к принтерам.
[public]	В пользовательском разделе описаны настройки каталогов общего доступа
[private]	В пользовательском разделе описаны настройки каталогов общего доступа

Для проверки наличия в конфигурационном файле `/etc/samba/smb.conf` несоответствий и внутренних противоречий нужно протестировать его корректность с помощью команды `testparm`. При отсутствии ошибок, демон `smbd` выведет на экран файл основных настроек Samba-сервера, а если при тестировании будут обнаружены ошибки, то о них будет выдана полная информация. Использование команды `testparm` не гарантирует доступность и корректность работы всех и ресурсов, и сервисов.

После завершения настройки Samba-сервера, который состоит из сервисных служб `smbd` и `nmbd`, нужно запустить или перезапустить обе службы, если они были запущены до этого.

Перед настройкой службы `smbclient` нужно создать разделяемые каталоги, доступ к которым получают все пользователи или определенные пользователи и группы пользователей.

Файловый сервер Samba позволяет настроить общий ресурс с гостевым (для любого пользователя), паролем (для определенного пользователя) или смешанным доступом (например, общий ресурс с пакетами программ, которые может запустить любой пользователь, но не может что-либо изменить в их содержимом), а также в административных целях для служебного ресурса - скрытый общий ресурс.

Для подключения компьютера с операционной системой Astra Linux SE к локальным сетям Windows существуют клиентские функции Samba. Клиентские функции Samba представлены средствами просмотра сетевого окружения и монтирования файловых систем `smbclient` и `mount` соответственно. При запуске эти программы считывают текущую конфигурацию из файла `/etc/samba/smb.conf` и используют доменные функции в случае, если машина подключена к домену Windows.

Для доступа пользователей к ресурсам сервера выполняется монтирование СЗФС или используется графическая утилита `fly-admin-samba`. Получить список доступных общих ресурсов примонтированной машины, можно, используя Midnight Commander, команды командной строки или с помощью менеджера файлов. Кроме того, программа `smbclient` может работать в интерактивном режиме, позволяя выполнять следующие действия:

- создавать каталоги и перемещаться по ним;
- просматривать содержимое файлов;
- копировать и перемещать файлы между локальным компьютером и общим ресурсом;
- удалять каталоги и файлы;
- выполнять другие действия в общей сетевой папке.

Преимуществом файлового сервера Samba является наличие корзины на сетевых дисках (скрытый каталог, в который перемещаются удаляемые с

файлового сервера Samba объекты), что дает возможность сохранить удаленные файлы, так как при удалении файлов из общей папки, они удаляются навсегда.

Сетевая корзина может быть настроена, как для каждого сетевого диска, так и общая для всех сетевых дисков. При этом чтобы все файлы, которые были удалены, попадали в корзину, нужно чтобы у каждого пользователя корректно были выставлены права доступа к этой корзине.

Таким образом, файловый сервер Samba обеспечивает взаимодействие между разными операционными системами, с помощью контроля доступа к ресурсам и аутентификации пользователей и возможность настройки файлового хранилища различных масштабов с управлением сетевыми ресурсами в соответствии с потребностями пользователей, а также поддерживает другие дополнительные функции (монтирование сетевых ресурсов, синхронизацию каталогов и файлов и др.). Кроме того, сетевые ресурсы файлового сервера Samba могут использоваться разными приложениями, например, утилиты резервного копирования могут записывать в сетевые ресурсы резервные копии, а плеер проигрывать видео или музыку из сетевых ресурсов Samba, что делает файловый сервер Samba средством первой необходимости.

Список используемых источников

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Организация единого пространства пользователей в автоматизированных системах специального назначения Информационная безопасность регионов России: материалы XII Санкт-Петербургской международной конференции, Санкт-Петербург, 27–29 нояб. 2021 г. СПб.: СПОИСУ, 2021. С. 156–158.

2. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

3. Деньжонков К. А., Кий А. В., Пашенко В. В. и др. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: учебное пособие. СПб.: ВАС, 2019. 288 с.

УДК 621.391
ГРНТИ 81.93.29**WEB-ПРИЛОЖЕНИЯ В ЗАЩИЩЕННОЙ
ОПЕРАЦИОННОЙ СИСТЕМЕ****О. Б. Ильина¹, О. П. Купчиненко¹, А. В. Скоропад²**¹Военная академия связи имени Маршала Советского Союза С. М. Буденного²Санкт-Петербургский филиал — «ЛОНИИР»

Выполнен анализ особенности работы web-приложений в операционной системе специального назначения «Astra Linux SE». Рассмотрены состав и применение защищенного комплекса программ гипертекстовой обработки данных. Выполнено сравнение механизмов защиты и идентификации пользователей. Представлены средства повышения производительности работы web-приложений.

операционная система специального назначения, web-приложение, web-сервер, мандатное разграничение доступа, аутентификация, протокол Kerberos

В настоящее время web-технологии предоставляют широкие возможности по созданию и поддержке информационных ресурсов в сети. Работа web-приложений в операционной системе специального назначения (ОС СН) «Astra Linux SE» имеет особенности, обусловленные применением мандатной модели разграничения доступа и режимов аутентификации пользователей [1].

Разработчики web-приложений могут самостоятельно решать вопросы, связанные с идентификацией и аутентификацией пользователей в ОС СН. При разработке этих функций требуется учитывать необходимость сертификации разрабатываемого программного обеспечения (ПО) по требованиям отсутствия несанкционированного доступа (НСД) к информации.

Защищенный комплекс программ гипертекстовой обработки данных это ПО, которое осуществляет взаимодействие по протоколу HTTP (HyperText Transfer Protocol) между Web-сервером и браузерами. Комплекс программ решает следующие задачи:

- прием запросов;
- поиск файлов и передача их содержимого;
- выполнение приложений на сервере;
- передача клиенту результатов выполнения приложений.

В ОС СН «Astra Linux SE» ПО состоит из Web-севера Apache2 (начиная с версии ОС СН 1.6) и браузера Firefox. ПО обеспечивает мандатное разграничение доступа при организации удаленного доступа к информационным

ресурсам в информационных и управляющих системах, в которых осуществляется хранение, обработка и передача информации ограниченного доступа.

Сервер Apache2 это надежный и гибкий в конфигурации сервер, который позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и др.

Браузер Firefox предоставляет широкие возможности пользовательской настройки. Пользователь может устанавливать дополнительные темы, которые меняют внешний вид браузера, плагины и расширения, добавляющие новые функции.

Браузер содержит:

- интерфейс с различными вкладками;
- инструмент для проверки орфографии;
- быстрый поиск по мере набора информации;
- менеджер загрузок;
- поле для обращения к поисковым системам и др.

Новые функции браузера можно добавлять при помощи расширений.

В состав расширенного репозитория «Astra Linux SE» версии 1.7 входит ПО Web-сервер NGINX (Engine-X, «Энжин-кс») [2]. Сравнение серверов Apache2 и NGINX представлено в таблице 1. Web-сервер NGINX часто используют совместно с сервером Apache2 для ускорения обработки запросов и уменьшения нагрузки. NGINX по сравнению с Apache2 работает быстрее со статическим контентом и потребляет меньше серверных ресурсов. Для упрощения настройки ПО гипертекстовой обработки данных рекомендуется использовать встроенные механизмы аутентификации и идентификации пользователей с помощью защищённого Web-сервера.

Разработчики web-приложений и администраторы могут использовать следующие механизмы защиты и аутентификации:

- РАМ-аутентификация (использование базы локальных пользователей);
- Astra Linux Directory (ALD) (использование базы доменных пользователей) [3].

В основе РАМ-аутентификации лежит метод аутентификации протокола HTTP. Web-сервер Apache2 в условиях применения мандатного управления доступом не разрешает анонимное использование ресурсов и требует обязательной настройки авторизации пользователей. Если не требуется использовать политики управления доступом пользователей, подключаемых к определенному серверу, авторизацию можно отключить. Для этого необходимо добавить строку `AstraMode off` в конфигурационном файле `/etc/apache2/apache2.conf`. По умолчанию режим включен, а параметр `AstraMode` отсутствует, это соответствует значению `AstraMode on` (выключен).

ТАБЛИЦА 1. Отличия Apache2 и NGINX

Характеристики	Apache2	NGINX
Документация	Большое количество документации на разных языках	Преимущественно на русском языке
Метод обработки соединений с клиентами	На каждый запрос от клиента создается отдельный процесс. Для большого количества процессов необходимо очень мощное техническое обеспечение.	Состоит из master-процесса и нескольких дочерних процессов. Мастер-процесс один, Загрузка процессора и использование памяти равномерны.
Работа с модулями	Простота работы. Необходимо прописать только название модуля, чтобы сервер сразу его загрузил и приступил к использованию	Сложность работы в том, что для добавления модулей их необходимо заранее подобрать и скомпилировать вместе с ядром сервера.
Конфигурация и настройка	Управление осуществляется с помощью служебных файлов. Недостаток – необходимо тратить время на получение информации из служебных файлов.	Вся информация содержится в одном конфигурационном файле. С точки зрения безопасности настройка более эффективна.
Работа с контентом	Эффективная работа с динамическим контентом	Эффективная работа со статическим контентом

Для корректного функционирования авторизации через РАМ пользователю, от которого работает Web-сервер (по умолчанию это пользователь www-data), необходимо дать права на чтение информации из базы данных пользователей и сведения о мандатных метках. Для этого необходимо добавить учётную запись пользователя www-data в группу shadow.

Для пользователя, под которым будет осуществляться вход на Web-сервер, необходимо выполнить команду для настройки минимального и максимального набора мандатных уровней и категорий.

Для обеспечения нормальной работы пользователя с сетевыми сервисами в ОС СН «Astra Linux SE» (начиная с версии 1.6) необходимо задать диапазоны его мандатных уровней и категорий, даже если пользователю не доступны уровни и категории выше нулевых.

Для использования web-приложений в распределенных сетевых системах более надежным является метод защиты и идентификации пользователей на базе протокола GSSAPI (Generic Security Standard Application Programming Interface) с использованием механизма Kerberos [4].

После подключения пользователя Web-сервер Apache2 выполняет аутентификацию пользователя и определяет мандатные атрибуты подключения. После этого запрос обрабатывается процессом-обработчиком с UID аутентифицированного пользователя и соответствующими мандатными атрибутами.

При использовании аутентификации по протоколу Kerberos необходимо получить билеты для подключения к внутренним модулям и сервисам, скрытым от пользователя. Для каждого подключения требуется получить билет Kerberos на основе запроса, при этом происходит обращение к Kerberos KDC (центру распространения ключей). Поэтому один пользовательский запрос приводит к необходимости нескольких запросов к Kerberos из службы LDAP (Lightweight Directory Access Protocol). Увеличение числа запросов может привести к снижению производительности работы web-приложений.

Одним из способов повышения производительности работы web-приложений – использование функций кэширования, которые предоставляет библиотека Django.

Django – Python web-фреймворк высокого уровня, который позволяет создавать:

- безопасные и поддерживаемые web-сайты;
- динамические web-сайты;
- сетевые приложения, сервисы или ресурсы.

Для мандатной защиты ресурсов можно использовать модули кэширования:

- СУБД (PostgreSQL);
- файловый кэш.

В каждом случае необходимо настроить мандатные атрибуты на объект-контейнер (база данных и каталог).

При использовании для кэша СУБД PostgreSQL возможны три стратегии использования Kerberos при аутентификации в СУБД PostgreSQL:

- использование данных аутентификации (билетов) пользователя;
- делегирование полномочий web-приложения;
- авторизация пользователей в web-приложении.

При использовании домена ALD для аутентификации пользователей, авторизация в web-приложении может быть выполнена стандартными функциями приложения.

Получения идентификатора пользователя возможно двумя путями:

- получение UID процесса;
- получение учетной записи из REMOTE_USER (переменная среды из приложения Django).

Самый простой и быстрый способ авторизации пользователей – использование групп домена ALD. Такой подход дает возможность не обращаться непосредственно в базу каталога LDAP.

Использование данных функций позволяет повысить производительность работы web-приложений в ОС СН «Astra Linux SE».

Список используемых источников

1. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие. М.: Горячая линия – Телеком, 2018. 311 с.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительном программном обеспечении в современных операционных системах // Актуальные проблемы инфокоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. Т. 2. С. 705–709.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Организация единого пространства пользователей в автоматизированных системах специального назначения // Информационная безопасность регионов России. XII Санкт-Петербургская межрегиональная конференция: сб. науч. ст. СПб.: СПОИСУ, 2021. С. 156–158.

4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Сетевая служба аутентификации // Актуальные проблемы инфокоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. Т. 2. С. 263–268.

УДК 629.8
ГРНТИ 28.23.27

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМ УПРАВЛЕНИЯ СКЛАДОМ (WMS) ЗА СЧЕТ ОПТИМИЗАЦИИ РАЗМЕЩЕНИЯ ТОВАРА

Д. И. Исмаилов, В. Л. Литвинов

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

Научная статья рассматривает стратегии оптимизации времени и размещения товаров на складе в условиях дефицита трудового ресурса. С использованием данных нейросетевого анализа и имитационной модели предлагается инновационный подход, направленный на повышение эффективности складской логистики и снижение трудовых затрат, учитывающий баланс между размещением по группам товаров и ABC-анализом. Авторы предвидят практическую апробацию разработанных методов на складах, с акцентом на учет стоимости перемещения товара.

WMS, Warehouse Management System, система управления складом, складская логистика

В настоящее время становится остро вопрос с дефицитом трудового ресурса линейных специальности, в частности специалистов складского комплекса. Связано это с тремя основными факторами. Во-первых, это развитие маркетплейсов, большое количество коротких операций. Во-вторых, развитие сервисов курьерских доставок. В-третьих, отток трудовых мигрантов в связи с изменением курса валют и политической ситуацией в стране. Дефицит трудовых ресурсов побуждает работодателей повышать заработные платы специалистам, тем самым увеличивая стоимость складской логистики.

Безусловно, у данной ситуации есть не только минусы, но и плюсы. Если раньше дешевая рабочая сила отодвигала автоматизацию складов и использование новых передовых технологий на долгие годы в будущее в связи с долгим сроком окупаемости, то сейчас намечается положительный тренд. К сожалению, с точки зрения роботизации выросла и стоимость оборудования автоматизации в связи с ростом потребности в автоматизации, из-за сокращения предложения в связи с санкциями большинства крупных развитых стран и из-за роста курса валют. Поэтому в данной статье будет рассматриваться второй вариант сокращения затрат, а именно оптимизация времени, затрачиваемого персоналом на одну операцию.

Эффективная работа на складе требует тщательного управления временем, чтобы обеспечить эффективность операций и минимизировать потери.

Весьма полезным инструментом для анализа использования времени является разделение рабочего времени на три основные категории: полезное, бесполезное и обязательное.

Полезное время – это тот период, в течение которого сотрудники на складе занимаются действиями, направленными на достижение основных целей и задач складской деятельности. К таким действиям можно отнести:

- приемка и размещение товаров (процессы, связанные с приемкой поставок, проверкой качества товаров и их последующим размещением на складе);
- сборка и упаковка заказов (эффективная сборка и упаковка заказов перед отправкой клиентам);
- инвентаризация и учет: проведение регулярных инвентаризаций и аккуратное ведение учета товаров на складе и т. п.

Бесполезное время – это тот период, в течение которого сотрудники тратят энергию и ресурсы на действия, которые не приносят реальной пользы складской деятельности. К таким действиям можно отнести:

- лишние перемещения: ненужные перемещения по складу из-за неорганизованности или неоптимальности размещения товара;
- ожидание (задержки в ожидании поставок или отгрузок);
- избыточные процессы (лишние шаги в процессах, которые могут быть упрощены или оптимизированы).

Обязательное время – это тот период, в течение которого сотрудники заняты выполнением обязанностей, необходимых для соблюдения нормативов, законов и стандартов безопасности. К таким обязанностям можно отнести:

- соблюдение стандартов безопасности (работа в соответствии с правилами и инструкциями по обеспечению безопасности);
- обучение и тренинги (прохождение необходимых курсов обучения и тренингов для повышения квалификации);
- фиксация действий в системе.

Разделение рабочего времени на эти три категории помогает выделить приоритеты, идентифицировать узкие места в процессах и направить усилия на оптимизацию тех аспектов работы на складе, которые могут приносить максимальную пользу.

По статистике, при комплектовании заказа, 50% времени сборщик тратит именно на перемещение по складу [1]. Оптимизация данного показателя на несколько процентов может сократить затраты крупного склада на миллионы.

Время на перемещение по складу зависит от четырех составляющих: размещения товара на этом складе, маршрута обхода ячеек, используемых технологий сборки, инфраструктуры склада.

Инфраструктуру склада быстро не поменяешь, это затратный вопрос, поэтому его в данной статье рассматривать не будем.

Использование технологии мультипикинг (сборка нескольких заказов параллельно) позволяет значительно сократить перемещения персонала, но уже решена в подавляющем большинстве систем управления складом (WMS – *warehouse management system*). Другие технологии либо требуют инвестиций в оборудование, либо не дают такого большого прироста.

Значительную оптимизацию перемещения по складу можно достичь, используя построения маршрута обхода склада змейкой (рис. 1) [2], который реализован практически во всех WMS.

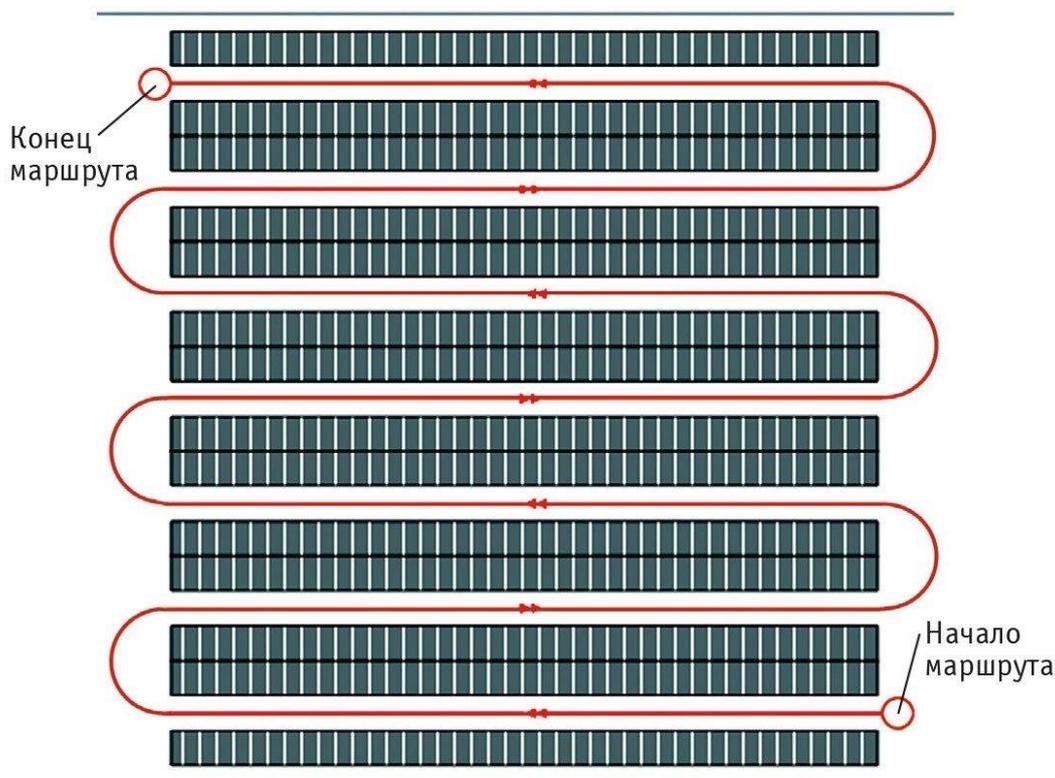


Рис. 1. Варианты обхода склада

Маршрут можно задавать в системах практически какой угодно, исходя из целей и задач руководителя склада, но там уже будет экономия не на рассматриваемом времени перемещения по складу, а на других показателях, например, на комплектацию сборных паллет на отгрузку.

В рассматриваемой статье мы сфокусируем внимание на размещении товара.

На неавтоматизированных складах с невысокими компетенциями в складской логистике, товар, как правило, расставляется по категориям, так как он приходит от поставщика. Например, для строительных материалов, в первых пяти строках ассортимента представлены смесители и прочие сантехнические изделия, в следующих пяти – валики и кисти, с одиннадцатого

по пятнадцатый ряды – саморезы и болты и так далее. Подобное упорядоченное размещение товаров обеспечивает удобство их складирования: привезенный от поставщика паллет размещается в центре, и все товары из одной категории находятся в одной области. Кроме того, при сборке конструкции, как правило, приходится перемещаться по всему складу. Существуют исключения, например, когда берутся комплектующие строго одного поставщика. Отличительной особенностью таких складов бывает минимальный штат персонала на приёмке и размещении товара и очень большая доля сборщиков. А с учётом того, что поставщики обычно привозят крупные партии паллет или коробки, а контрагенты забирают товар коробками или штуками, то, анализируя процессы склада, становится понятно, что надо оптимизировать.

Полярная ситуация может возникнуть на складах с WMS, которые могут отдать размещение на откуп системе управления складом исходя из ABC анализа – это классический метод ранжирования товарных запасов (или других активов компании) по заданным факторам [3]. В случае со складом ранжируют товар по количеству обращений к товару. В итоге получают А – ходовой товар, В – средний, С – неходовой. В данном случае система перемещает товар на складе подобно блендеру. С точки зрения сборки ситуация улучшится, пробеги персонала сократятся. Дополнительной опцией сократится количество пересортов, за счёт того, что в соседних ячейках будут лежать очень разные товары, и при отгрузке или контроле вероятность обнаружения ошибки становится в разы выше. Но при размещении товара будет тяжело, особенно если зона размещения – несколько тысяч квадратных метров. Если при размещении товар был бы существенно разный, то на терминале сбора данных (ТСД), можно было бы построить маршрут отбора, оптимальный исходя из размещения товара, но, как правило, поставщики привозят однотипный товар, который тяжело визуально отличить друг от друга.

Если размещение товаров происходит в области мелкоячеистого хранения, обычно использующей паллеты с десятками или сотнями единиц товара, то даже при наличии информации о конкретном товаре от ТСД (терминала сбора данных), сотруднику будет сложно найти его на паллете, так как их визуально много. Следовательно, для упрощения процесса размещения товара необходимо его предварительно просканировать, что, однако, затрудняет определение оптимального маршрута обхода склада. В качестве альтернативы можно не перемещать паллет по складу, а организовать его обработку на месте, то есть последовательно брать с него товар, перемещаться в зону размещения и возвращаться к паллету за следующей единицей товара. Такой подход оптимизирует процесс сборки товара, но не позволяет обеспечить оптимальное размещение товара на складе.

Получается лучший сценарий размещения где-то посередине, нужно найти баланс между размещением и по группам товара, и по ABC анализу. Если количество размещаемых позиций измеряется сотнями или даже несколькими тысячами, а поставщиков не более десятка, вопрос не такой сложный, и зачастую может решиться экспертным путем. Другой случай, если ассортимент товара измеряется десятками тысяч, а количество поставщиков измеряется сотнями или приближается к тысячам.

Данную задачу невозможно решить, используя стандартные инструменты систем управления складом, поэтому предлагается в системе записывать время совершения транзакции, которое в свою очередь состоит из времени сборки товара и времени перемещения. При этом какое именно время составляет полезное, а какое – бесполезное, не ясно.

Время сборки одного и того же товара может быть разным в зависимости от яруса размещения. При этом, на разные товары разный ярус будет влиять по-разному, поэтому стоит определить от чего зависит скорость сборки. Для этого весь массив данных предлагается подвергнуть нейросетевому анализу, чтобы определить от каких параметров товара зависит размещение. За основу будут взяты мастер-данные товаров, данные по транзакциям из системы управления складом и данные по входящим и исходящим товарным потокам.

Используя полученные данные, можно составить имитационную модель, и определить наиболее оптимальный сценарий размещения товара, в результате которого можно сократить общую трудоёмкость работы на складе. Помимо роста эффективности склада, доли фонда оплаты труда к обороту, планируется, что вырастет и общая удовлетворенность персонала, ведь всегда приятнее заниматься полезным действием, а не бесполезным.

В дальнейшем планируется апробация данной системы на складах системообразующего предприятия ООО «СТД «Петрович». При внедрении важно будет учесть не просто перемещение всего товара, что может стоить компании немалую сумму денег, но и стоимость самого перемещения товара. Важно найти точку, при которой будет максимальная выгода для компании за счёт разницы между стоимостью размещения товара и стоимостью перемещения товара.

Список используемых источников

1. Складская логистика. Retail.ru – портал для ритейлеров и поставщиков. 2010. URL: <https://www.retail.ru/articles/skladskaya-logistika/> (дата обращения 30.12.2023)
2. Как ходить будем? Звездочкой! Дзен. 2022. URL: <https://dzen.ru/a/Y6vPurm-ejzhATcR> (дата обращения 30.12.2023)
3. ABC-анализ товарных запасов. Бизнес-анализ: готовые решения в Excel и Power BI на основе данных из 1С. URL: <https://bestsaldo.ru/blog/upravlenie-zapasami/abc-analiz-tovarnykh-zapasov> (дата обращения 30.12.2023)

УДК 004.652
ГРНТИ 20.53.17

СРАВНЕНИЕ SQL И NoSQL БАЗ ДАННЫХ

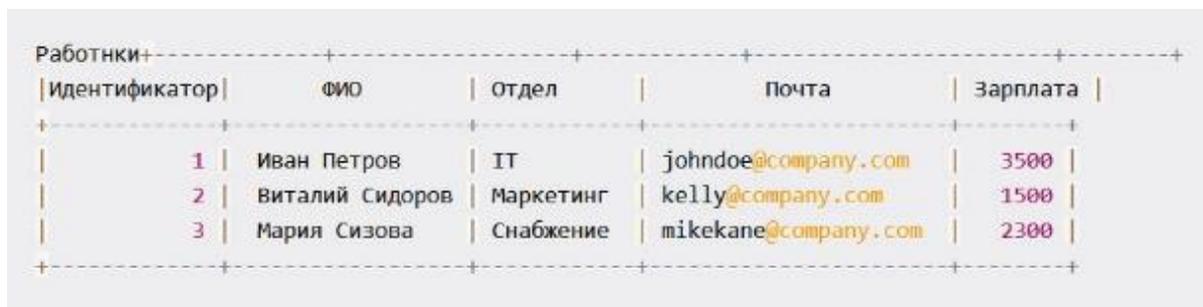
А. О. Калинюк, С. А. Константинов

Военная академия связи имени маршала советского союза С. М. Буденного

Производительность клиент-серверных приложений во многом зависит от выбора архитектуры хранения данных. В настоящее время существуют две основные модели баз данных: реляционная и не реляционная. Реляционная модель обеспечивает однозначную целостность данных и позволяет создавать сложные запросы и транзакции, кроме того, язык SQL имеет широкие возможности для создания скриптов. В не реляционной модели данные хранятся в формате «ключ-значение», что дает возможности создавать более удобные программные интерфейсы (API) и быстрые вычисления при малых объемах данных.

Архитектуры баз данных, SQL, NoSQL, БД, СУБД

В реляционной модели данных информация хранится в структурированном и табличном виде, что позволяет организовать данные в таблицах. Подобным образом можно представить организацию данных о сотрудниках в компании в виде таблицы. Реляционные базы данных имеют четкую, статичную и заранее определенную логическую структуру, которую можно рассматривать как организационный план или набор правил для хранения данных. В таблице содержатся строки или записи, которые представляют собой набор значений данных, соответствующих определенной схеме. Таким образом, реляционная модель предоставляет удобный способ хранения и управления данными, а таблицы и записи позволяют структурировать информацию для эффективного доступа и обработки. Реляционная модель представлена на рис. 1.



Идентификатор	ФИО	Отдел	Почта	Зарплата
1	Иван Петров	IT	john.doe@company.com	3500
2	Виталий Сидоров	Маркетинг	kelly@company.com	1500
3	Мария Сизова	Снабжение	mike.kane@company.com	2300

Рис. 1. Реляционная модель хранения данных

Реляционные базы данных основаны на языке SQL, позволяющим выполнять запросы. Например, если пользователю нужно просмотреть имена

сотрудников, чья ежемесячная зарплата превышает 2000 денежных единиц, то следует написать SQL-запрос (рис. 2).

```
SELECT ФИО FROM Работники  
WHERE Зарплата > 2000;
```

Рис. 2. SQL-запрос

Из приведенного выше запроса пользователь получил бы следующий результат (рис. 3):

ФИО
Иван Петров
Мария Сизова

Рис. 3. Результат запроса

Реляционная база данных состоит из нескольких связанных между собой таблиц, и ключевая особенность этой модели данных заключается в использовании первичных и внешних ключей. Первичный ключ является уникальным идентификатором записей в таблице, а внешний ключ обеспечивает связывание нескольких таблиц.

Однако с ростом размеров баз данных возникает проблема выполнения запросов, которые могут занимать много времени. Именно поэтому строение и использование реляционных баз данных являются актуальными и важными. Они позволяют эффективно организовывать и обрабатывать данные при соблюдении требований ACID:

- атомарность (Atomicity) – каждая транзакция рассматривается как неделимая и непрерываемая операция;
- согласованность (Consistency) – требование, подразумевающее, что в таблицах и транзакциях данные будут допустимыми;
- изолированность (Isolation) – Во время выполнения транзакции другие транзакции не должны оказывать влияния на её результат;
- надежность (Durability) – это принцип, согласно которому все изменения, в случае проектной аварии на нижних уровнях или других неисправностях состоянии транзакции должно сохраняться, кроме того, должно быть обеспечено сохранение выполненных транзакций.

Распределенные системы реляционных баз данных могут столкнуться с проблемой, связанной с требованиями ACID (атомарности, согласованно-

сти, изолированности и долговечности), особенно в отношении централизованного управления блокировками. Это означает, что в случае, когда несколько приложений пытаются получить доступ к данным, обрабатываемым другим приложением, они должны ждать завершения текущей транзакции, что может привести к узкому месту и замедлению работы всей системы.

В отличие от этого, *NoSQL* базы данных не хранят и не организуют данные в табличной форме с таблицами, строками и столбцами. Вместо этого они используют коллекции данных без жесткой структуры и с динамической схемой. *NoSQL* базы данных могут использовать различные модели данных, такие как ключ-значение, документоориентированная, столбцовая и графовая модели, что позволяет более гибко хранить и обрабатывать данные.

Примеры *NoSQL* баз данных:

1. *MongoDB*: документоориентированная СУБД, использующая *JSON*-подобные документы.

2. *Cassandra*: Это столбцовая база данных, которая обеспечивает высокую производительность и отказоустойчивость при работе с «большими данными». Она широко используется для хранения и обработки временных рядов данных и аналитики.

3. *Redis*: Это база данных ключ-значение, которая предоставляет быстрый доступ к данным в оперативной памяти. Она используется для кэширования данных, хранения сессий и реализации очередей сообщений.

4. *Neo4j*: Это графовая база данных, которая предназначена для работы с связанными данными, такими как социальные сети или рекомендательные системы. Она обеспечивает эффективный анализ и поиск данных на основе связей между узлами.

Было проведено сравнение баз данных, включая в себя 4 фундаментальных операции:

1. *Instantiate*. Создается экземпляр сегмента хранения для пар ключ-значение.

2. *Read*. Считывается значение, соответствующее данному ключу.

3. *Write*. Если данная пара ключ-значение не найдена в хранилище то объект добавляется в хранилище, в противном случае, обновляется значение данного ключа в хранилище.

4. *Delete*. Удаление записи, соответствующей данному ключу из пары ключ-значение.

В таблице 1 приведены базы данных, выбранные для сравнения. В первом эксперименте измеряется время, затраченное на создание экземпляра корзины базы данных (рисунок 2). *RavenDB*, *Hyertable*, *MongoDB* предлагают самое быстрое создание сегментов базы данных. *CouchDB*, *Couchbase* и *MS SQL* являются одними из самых медленных в создании сегментов.

ТАБЛИЦА 1. Исследуемые базы данных

База данных	Версия
<i>MongoDB</i>	1.8.5
<i>RavenDB</i>	960
<i>CouchDB</i>	1.2.0
<i>Cassandra</i>	1.1.2
<i>Hypertable</i>	0.9.6
<i>Couchbase</i>	1.8.0
Microsoft SQL Server	10.50.1600.1

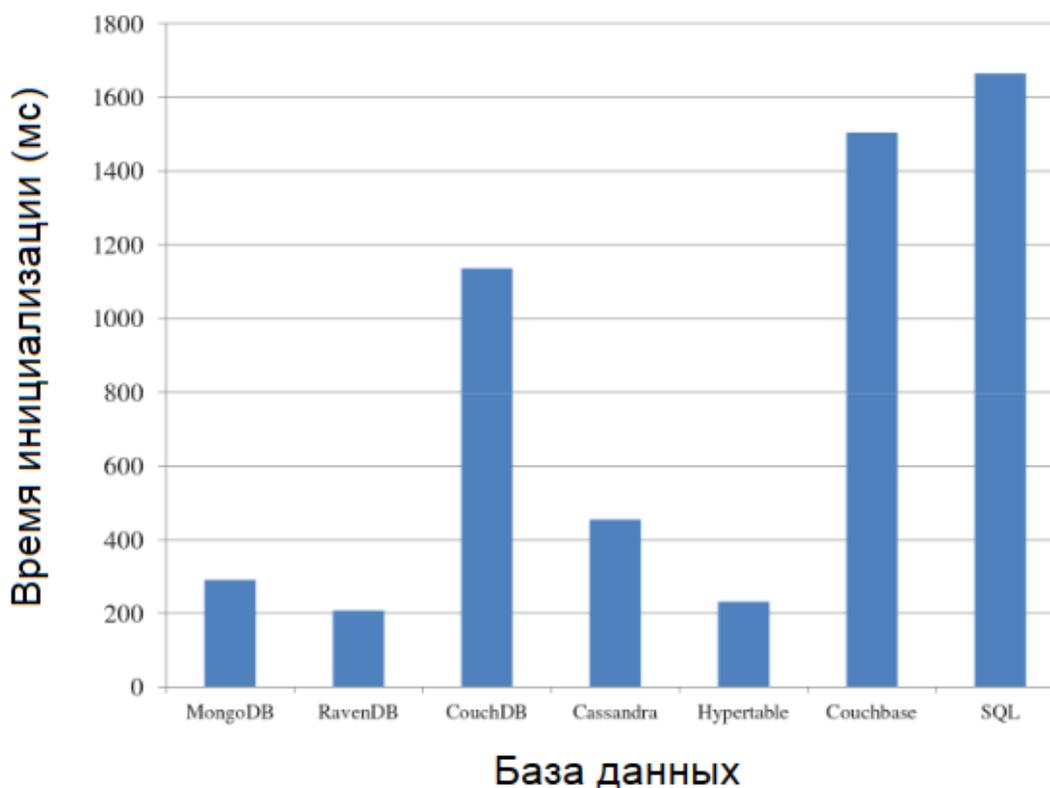


Рис. 2. Время инициализации экземпляра БД

Во втором эксперименте измеряется время, затраченное на считывание значений, соответствующих заданным ключам. В таблице 2 обобщен результат. Таким образом, получается отсортированный по производительности список: *Couchbase*, *MongoDB*, *SQL Express*, *Hypertable*, *CouchDB*, *Cassandra* и *RavenDB*. Из них *Cassandra* и *Hyper table* являются базами данных семейства столбцов; и *Couchbase*, *MongoDB*, *CouchDB* и *RavenDB* являются документоориентированными БД. Нет заметной корреляции между моделью данных и производительностью. Стоит отметить, что производительность чтения *MS SQL* лучше, чем у некоторых баз данных *NoSQL*.

ТАБЛИЦА 2. Время, затраченное на операцию чтения (мс)

БД	Количество операций чтения					
	10	50	100	1000	10000	100000
<i>MongoDB</i>	7	16	29	158	1095	10221
<i>RavenDB</i>	160	311	529	4230	47469	426525
<i>CouchDB</i>	24	121	176	1889	19528	176078
<i>Cassandra</i>	125	210	324	2355	19758	228086
<i>Hypertable</i>	61	82	113	470	3437	63036
<i>Couchbase</i>	16	21	27	88	861	7214
<i>MS SQL</i>	12	28	42	267	1958	17294

В третьем эксперименте измеряется время, затраченное на запись пар ключ-значение в корзину. Если пара ключ-значение уже существует в корзине, это равносильно обновлению существующего значения. В противном случае это равносильно добавлению пары ключ-значение в базу данных. В таблице 3 продемонстрирован результат.

ТАБЛИЦА 3. Время, затраченное на операцию записей (мс)

БД	Количество операций записи					
	10	50	100	1000	10000	100000
<i>MongoDB</i>	62	72	88	389	2793	23554
<i>RavenDB</i>	550	838	1113	6949	71443	741450
<i>CouchDB</i>	98	324	626	6231	67316	933038
<i>Cassandra</i>	127	150	222	1250	9811	86197
<i>Hypertable</i>	51	91	154	1135	10958	118872
<i>Couchbase</i>	80	71	62	122	916	8192
<i>MS SQL</i>	40	92	119	1720	15288	212479

Таким образом наблюдается, что производительность записи *RavenDB* и *CouchDB* хуже, чем у *MS SQL*. Но другие базы данных NoSQL работают лучше, чем *MS SQL*.

В четвертом эксперименте измеряется время, затраченное на удаление пар ключ-значение из БД. В таблице 4 обобщен результат. Видно, что производительность *MS SQL* при удалении лучше, чем у всех баз данных NoSQL.

ТАБЛИЦА 4. Время, затраченное на удаление (мс)

БД	Количество операций удаления					
	10	50	100	1000	10000	100000
<i>MongoDB</i>	6	13	29	275	2185	18688
<i>RavenDB</i>	70	499	819	8242	87522	799609
<i>CouchDB</i>	73	260	527	5545	67912	705284
<i>Cassandra</i>	32	95	140	1161	9270	83634
<i>Hypertable</i>	12	63	150	1801	10424	130258
<i>Couchbase</i>	7	12	16	88	835	7134
<i>MS SQL</i>	10	32	58	350	3871	33741

NoSQL-базы данных оптимизированы для хранения данных в формате ключ-значение, *SQL*-базы данных таковыми не являются. Однако не все *NoSQL* базы данных показывают лучшую производительность по сравнению с тестируемой *SQL* базой данных. Также наблюдается, что даже внутри группы *NoSQL* баз данных производительность сильно варьируется в зависимости от типа операции (например, чтение и запись). Имеется малая корреляция между производительностью и моделью данных, используемой каждой базой данных.

Базы данных *NoSQL RavenDB* и *CouchDB* плохо справляются с операциями чтения, записи и удаления. *Cassandra* имеет проблемы с операциями чтения, но хорошо справляется с записью и удалением данных. *Couchbase* и *MongoDB*, с другой стороны, обычно обеспечивают хорошую производительность при операциях чтения, записи и удаления. Однако стоит помнить, что *Couchbase* не поддерживает операцию выборки всех ключей. *MongoDB* занимает второе место после *Couchbase* в операциях чтения, записи и удаления.

Одним из основных преимуществ *NoSQL* баз данных является горизонтальное масштабирование. Это означает, что можно добавлять новые серверы или узлы к существующей инфраструктуре без необходимости изменения схемы базы данных. Такой подход позволяет распределить нагрузку на несколько серверов и обеспечить более высокую производительность и доступность данных.

Еще одним преимуществом *NoSQL* баз данных является их гибкость и адаптивность к различным типам данных. В отличие от *SQL* баз данных, которые используют строго определенные схемы и таблицы, *NoSQL* базы данных могут хранить неструктурированные данные, например, документы, графы или ключ-значение пары. Это позволяет более эффективно работать с большим объемом данных разной природы и формата.

Однако *NoSQL* базы данных также имеют свои недостатки. Они обычно не гарантируют полную согласованность и целостность данных. Это означает, что при параллельных операциях между разными узлами базы данных могут возникать конфликты и несогласованность данных. Однако существуют различные стратегии и подходы к управлению этими проблемами, такие как конфликтное разрешение и репликация данных, которые позволяют обеспечить достаточную степень целостности и согласованности данных для конкретных задач.

Список используемых источников

1. Tudorica B., Bucur C. A comparison between several NoSQL databases with comments and notes // 10th Roedunet International Conference, Iasi, Romania, 2011. PP. 1–5. DOI:10.1109/RoEduNet.2011.5993686
2. Волк В. К. Базы данных. Проектирование, программирование, управление и администрирование. СПб.: Лань, 2020. 244 с.
3. Date С. Введение в системы баз данных. 2011. 213 с.
4. Эльмарси Рамез. Основы системы баз данных. 2017. 280 с.
5. Chodorow K., Dirolf M. MongoDB: The Definitive Guide. O'Reilly Media, September 2010. 213 с.
6. Indrawan-Santiago M., Database research: Are we at a crossroad? Reflection on NoSQL, in Network-Based Information Systems (NBiS). 2012. PP. 45 –51.
7. Таненбаум Э. Распределенные операционные системы. 2011. 213 с.

УДК 004.56
ГРНТИ 50.43.19

ОБЩИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ УЗЛОВ МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

И. С. Ковалев, С. Б. Ногин, О.И. Пантюхин, В. В. Пашенко

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

Поддержание работоспособности компьютерных сетей остается актуальной проблемой. Одним из способов решения этой проблемы является мониторинг различных параметров сети. Выбор соответствующих параметров и мест их мониторинга во многом определяется целями мониторинга.

компьютерные сети, мониторинг, узел мониторинга, параметры мониторинга, выбор узла мониторинга

Мониторинг вычислительной сети – проведение измерений соответствующих параметров сети и ее элементов в контрольных точках с целью своевременного обнаружения выхода текущих значений параметров за предельные (допустимые) значения и получения необходимой информации для выработки предупреждающих действий.

Узел мониторинга – это контрольная точка, в которой осуществляются измерения соответствующих параметров сети либо ее элементов.

Существует огромное количество средств и методов мониторинга вычислительных сетей. Обоснованность их применения зависит от многих факторов: целей мониторинга, объекта мониторинга, архитектуры и конфигурации сети, режимов работы сети в целом и ее элементов, характера обработки информации в сети и т. д.

Основные шаги в процессе выбора узлов мониторинга:

- выделение объекта мониторинга;
- определение целей мониторинга;
- определение архитектуры и конфигурации сети;
- определение топологии сети;
- определение источников и потребителей информации;
- определение направлений движения данных и точек их консолидации;
- определение угроз безопасности (для мониторинга безопасности информационного процесса и данных);
- выделение узлов мониторинга.

Следует отметить, что выполнение отдельных шагов выбора узлов мониторинга определяется в первую очередь целью мониторинга.

Выделение объекта мониторинга

В качестве объекта мониторинга могут выступать различные сущности, использующие вычислительные сети в процессе их функционирования (центры обработки данных, локальные вычислительные сети (ЛВС) организаций, автоматизированные системы на базе вычислительных сетей, региональные вычислительные сети и их части и т. д.). Выбор конкретного объекта накладывает соответствующие ограничения на архитектуру сети, ее конфигурацию, состав элементов, протекающие информационные процессы, элементы системы жизнеобеспечения, что в свою очередь будет сказываться на организацию процесса мониторинга.

Определение целей мониторинга

Ключевым элементом при организации мониторинга являются его цели. В зависимости от целевой установки определяются характер мониторинга, анализируемые параметры объекта мониторинга [1], допустимые значения соответствующих параметров, правила интерпретации полученных данных и многое другое. В свою очередь, все это существенно сказывается на выборе узлов мониторинга.

Например, мониторинг технического состояния сети предполагает контроль состояния элементов сети на предмет обеспечения их работоспособности и предотвращения выхода соответствующих элементов из строя, мониторинг производительности сети обеспечивает контроль информационного процесса в сети с целью обеспечения требуемых временных параметров обработки информации и предотвращения отказов в обслуживании соответствующих пользователей и сервисов, мониторинг информационной безопасности (ИБ) предназначен для контроля событий, соответствующих различным угрозам ИБ, таким как доступ к защищаемым данным с целью их копирования, удаления, модификации, нарушения информационного процесса, отказов в обслуживании и т. д. [2].

Определение архитектуры и конфигурации сети

Архитектура сети определяет характер связей и взаимодействия элементов сети, способы обмена информацией и другие параметры. Например, использование трехуровневой схемы построения сети (ядро, уровень агрегации, уровень доступа).

Определение топологии сети

Топология сети позволяет получить данные о количестве сетевого, серверного, оконечного оборудования, его расположении, что в свою очередь будет сказываться на определении числа и мест расположения узлов мониторинга.

Для поиска устройств в сети можно использовать программы для сканирования сети. При этом надо учитывать, что в сети могут быть устройства, не имеющие собственных IP-адресов (например, коммутаторы 2 уровня). Информация о таких устройствах нужно фиксировать вручную.

Список используемых устройств включается в перечень возможных узлов мониторинга.

Определение источников и потребителей информации.

Источниками и потребителями информации в сети являются: оконечное и серверное оборудование, внешние сети. К оконечным устройствам относятся: персональные устройства пользователей, стационарное оборудование, МФУ, принтеры и т.д., которые генерируют как пользовательский, так и технологический трафик. На серверном оборудовании выполняются программы, реализующие различные сервисы и услуги, результаты которых предоставляются внешним и внутренним пользователям.

Определение направлений движения данных и точек их консолидации.

Как правило в сети выделить несколько основных маршрутов перемещения данных:

- между оконечными устройствами локальной вычислительной сети;
- между оконечным устройством локальной сети и сервисами локальной/внешней сети
- между сервисами локальной сети и внешней сетью (внешними пользователями).

Необходимо определить указанные маршруты для всех элементов сети и найти общие точки и участки маршрутов.

Полученные элементы будут точками консолидации направлений движения данных. Такими точками может быть серверное оборудование, активное сетевое оборудование и каналы, связывающие различные сегменты и уровни вычислительной сети. Подобные точки являются кандидатами на их использование в качестве узлов мониторинга.

Выделение узлов мониторинга.

Полученный список возможных узлов рассматривается исходя из целей мониторинга с учетом возможности использования различных способов передачи данных мониторинга.

Если нас интересует техническое состояние оборудования, то за основу берется общий список устройств сети.

Для анализа производительности сети в первую очередь учитываются точки консолидации направлений движения данных. Для каждого предполагаемого узла оценивается возможность выполнения на нем специальных программных агентов системы мониторинга или возможность получения

необходимых данных параметров функционирования узла, а также способа передачи необходимых данных в систему мониторинга.

Определение угроз безопасности (для мониторинга безопасности информационного процесса и данных).

Если целевой установкой мониторинга является информационная безопасность, то механизм выявления узлов мониторинга основан на построении модели угроз безопасности вычислительной сети (ЛВС, автоматизированной системы).

Общий алгоритм определения узлов мониторинга с точки зрения обеспечения ИБ заключается в следующем:

Вычислительная сеть разделяется на сегменты по функциональному признаку. Например: руководство, сегмент соответствующего отдела, административный сегмент, серверный сегмент, филиалы и т. д. Определяются взаимосвязи сегментов по телекоммуникационной сети. Определяются взаимосвязи оконечного оборудования в рамках каждого сегмента.

Для каждого сегмента определяются угрозы безопасности.

Например, сегменты руководства, отделов, административный располагаются на уровне доступа к сети и обеспечивают подключение оконечных устройств к локальной сети, их взаимодействие внутри сегмента и с другими сегментами. Оконечными устройствами могут быть персональные компьютеры, ноутбуки, офисное оборудование. Для них основными угрозами ИБ, являются:

- пассивный сбор информации о подключенных к сети устройствах (их адресах, версиях ПО и других параметрах);
- получение неправомерного удаленного доступа к сегменту (сети);
- планирование запуска вредоносных программ при запуске операционной системы;
- запуска вредоносных программ как сервисов;
- использование штатных средств удаленного доступа и управления операционной системой.

Для каждой угрозы определяются возможные способы ее выявления с помощью программных и технических средств.

При выборе узлов мониторинга учитываются:

- степень критичности обрабатываемой в сети информации;
- угрозы ИБ и наиболее уязвимые места;
- способ получения данных мониторинга.

Список используемых источников

1. Олифер Н. А., Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов: 4-е изд. СПб.: Питер, 2010. 944 с.
2. Ногин С. Б. Некоторые аспекты построения системы мониторинга функционирования вычислительных инфраструктур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2022. Т. 2. С. 638–643.

УДК 004.05
ГРНТИ 81.93.29

ПРОБЛЕМА ПРИМЕНЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ДОКУМЕНТО-ОРИЕНТИРОВАННЫМИ БАЗАМИ ДАННЫХ

Р. М. Ковалёв, А. В. Салтанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Научно-исследовательский институт «Рубин»

В работе рассматривается вопрос проблемы выбора и применения систем управления документо-ориентированными базами данных. Данная проблема является причинно-следственной связью в постановке задачи разработки программно-алгоритмического обеспечения по управлению документо-ориентированными базами данных, используемых на различных этапах жизненного цикла продукции. Популяризация нереляционных СУБД требует углубленного изучения их качественных свойств, достоинств и недостатков при управлении документо-ориентированными базами данных, предполагаемых к использованию в смежных сферах деятельности предприятия, или при производстве продукции двойного назначения.

система управления базами данных, документо-ориентированные базы данных, реляционные базы данных, нереляционные базы данных

В современном информационном пространстве проблема управления документо-ориентированными базами данных (ДОБД) становится все более актуальной и значимой. Модель ДОБД может быть построена в реляционном формате, в нереляционном формате, а также в смешанном реляционно-нереляционном формате. При трансформации модели предназначение ДОБД не изменяется, но сама по себе трансформация направлена на оптимизацию быстродействия объемного клиент-серверного взаимодействия, в специализированной информационной среде. По мере заполнения ДОБД информацией содержательного характера, количество и запросов различного характера пропорционально возрастает.

Несмотря на то что ДОБД это объект группового использования, каждый запрос к ней является индивидуальным и выражает персональное представление пользователей о структуре информации моделируемой специализированной информационной среды [1].

Одной из ключевых проблем при применении систем управления ДОБД является эффективное управление структурой документов и их связями. Недостаточное внимание к структурированию данных может привести к сложностям при поиске, обновлении и анализе информации, что снижает эффективность работы с ДОБД.

Другой проблемой, с которой сталкиваются организации при использовании систем управления ДОБД, является разработка политики информационной безопасности направленной на выполнение комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагирование на компьютерные инциденты. Эксплуатация ДОБД в современной распределенной среде с использованием облачных технологий допускает возникновение новых уязвимостей, несущих деструктивное воздействие на её функционирование и требует дополнительного анализа и принятия эффективных мер по защите данных.

Для работы с ДОБД, широко используется Structured Query Language (SQL). Одним из главных преимуществ SQL является их более длительное время существования и широкое распространение по сравнению с NoSQL. SQL базы данных обладают строгой схемой данных, что обеспечивает четкую структуру и возможность выполнения сложных запросов с использованием стандартизированного языка запросов SQL (см. рисунок 1). Однако, в некоторых случаях, такая строгая схема может стать препятствием для гибкости и масштабируемости системы. [1, 2].

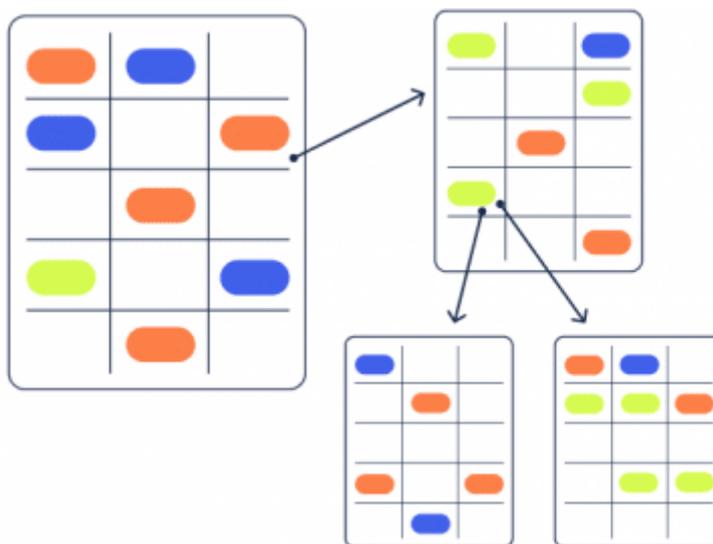


Рис. 1. Схема реляционной базы данных

Базы данных Not Only Structured Query Language (NoSQL), предлагают альтернативные модели данных и подходы к их управлению. NoSQL базы данных не требуют строгой схемы данных и позволяют горизонтальное масштабирование, что делает их оптимальными для работы с большими объемами данных и распределенными системами. Модели данных NoSQL, представленные на рисунке 2, такие как, колоночные, документо-ориентированные, ключ-значение и графовые базы данных, обладают индивидуальными особенностями по возможности хранения и обработки данных

в зависимости типа обрабатываемых данных и от персональных запросов пользователей.

Усложнение в управлении нереляционными ДОБД характеризуется несколькими показателями:

- свободное структурирование документов. Традиционные реляционные базы данных, заранее определяют фиксированную структуру хранящихся данных. ДОБД напротив, позволяют хранить документы различных типов и с произвольной структурой хранящихся данных. Это создает сложности при поиске, фильтрации и анализе данных внутри документа.
- сложность запросов и манипуляций с данными. Методы запросов и обработки данных, применяемые в нереляционных базах данных, не всегда эффективны или достаточно гибки для работы с документами, имеющими различную структуру и формат. Возникают сложности в поиске конкретных данных, иерархическом анализе информации и манипуляциях с вложенными объектами и массивами данных.

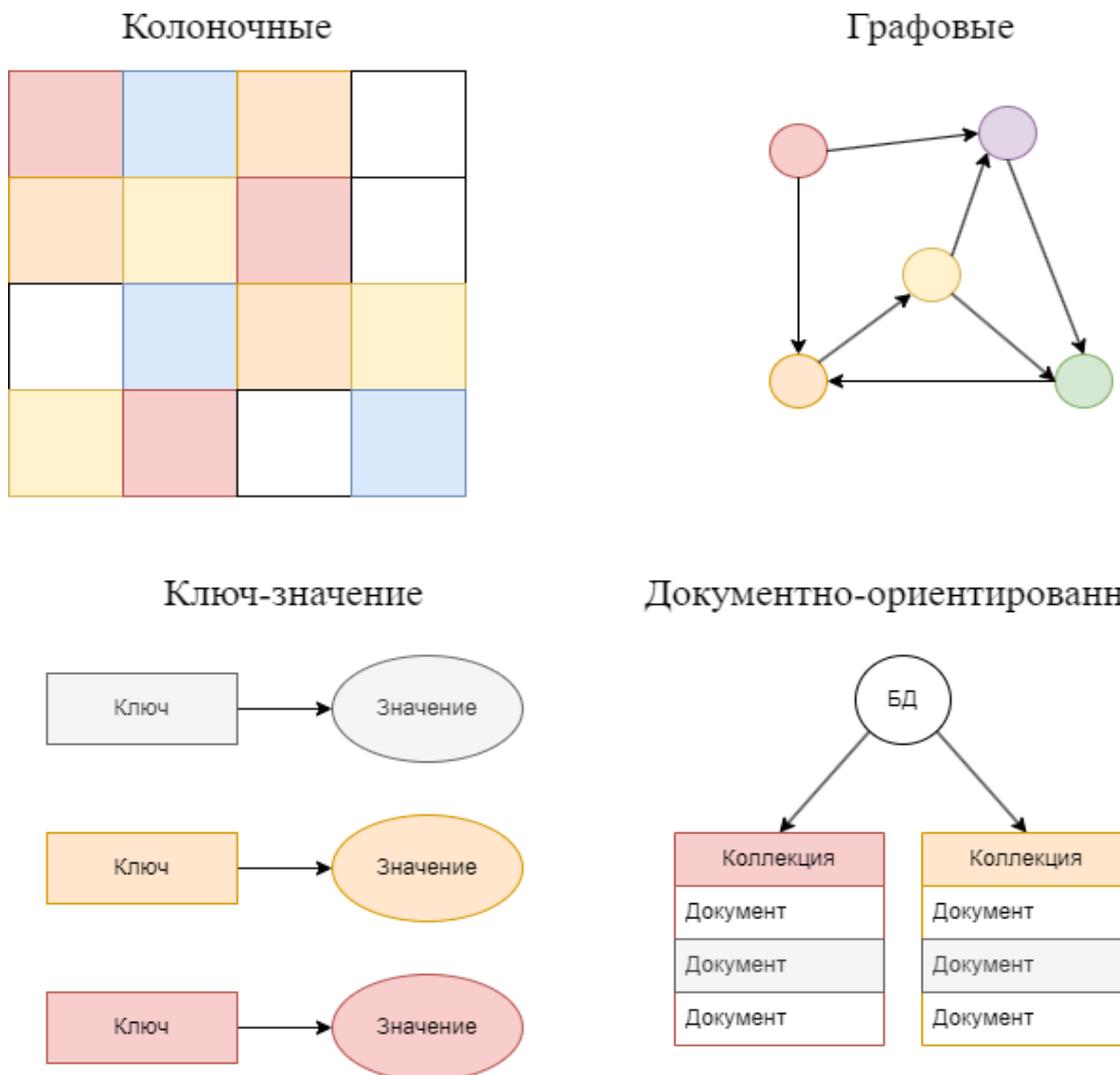


Рис. 2. Модели нереляционных баз данных

– изменение структуры и эволюция документов. Документы могут подвергаться добавлению, удалению или изменению своих полей и структуры по мере развития организации или изменения требований. В контексте реляционных баз данных это представляет незначительные проблемы, так как схема данных статична. Однако, для ДОБД необходимы расширяемые и гибкие схемы, которые позволяют эволюционировать и адаптироваться к изменяющимся потребностям без серьезных последствий [3].

Предложения по решению проблемы применения систем управления ДОБД:

1. Гибридный подход:

– сочетание SQL и NoSQL для достижения оптимального баланса между структурой, гибкостью и масштабируемостью;
– использование SQL для структурированных данных, требующих транзакционной согласованности, и NoSQL для неструктурированных данных, требующих гибкости и масштабируемости.

2. Выбор правильного NoSQL-решения:

– оценка различных NoSQL-решений (MongoDB, Cassandra, CouchDB и т. д.) на основе конкретных требований к данным и приложениям;
– необходимо учитывать такие факторы, как масштабируемость, согласованность, доступность, производительность и простота использования.

Заключение

Применение систем управления ДОБД может быть сложной задачей, но при правильном подходе она может принести ряд преимуществ.

Гибридный подход, сочетающий SQL и NoSQL, может стать оптимальным решением для многих приложений.

Выбор правильного NoSQL-решения, оптимизация схемы данных, интеграция с другими системами, обеспечение безопасности, а также обучение и поддержка пользователей – все это играет важную роль в успешном применении ДОБД.

Документо-ориентированные базы данных могут стать ключом к успеху для приложений, которым требуется высокая масштабируемость, гибкость и производительность.

Список используемых источников

1. Кара-Ушанов В. Ю. SQL – язык реляционных баз данных: учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2016. 156 с.
2. Баранов Ю. К. SQL-запросы для решения задач. М.: СОЛОН-Р, 2016. 100 с.
3. Васильев С. В., Воротникова О. В. Реляционные базы данных. М.: Инфра-М, 2016. 500 с.

УДК 004.946
ГРНТИ 20.01

СРАВНЕНИЕ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СОЗДАНИЯ ИГРОВОГО КОНТЕНТА С ЗАРУБЕЖНЫМИ АНАЛОГАМИ

Е. В. Козин¹, В. Д. Лукьянов², Т. В. Петрова¹, С. Л. Хомутовский¹

¹Военная академия связи имени маршала советского союза С. М. Буденного

²Национальный исследовательский университет ИТМО

В статье авторы рассматривают функциональные возможности игровых движков зарубежного и отечественного производства. В статье представлено сравнение основных характеристик наиболее часто используемых игровых движков в современной GameDev индустрии. Авторы акцентируют внимание на необходимости развития отечественного программного обеспечения для создания игрового контента, так как на данном этапе наблюдается отставание от зарубежного по функционалу и простоте освоения. Авторами делается вывод о том, что несмотря на высокий порог вхождения в отечественный игровой движок Unigine, он имеет широкий функционал разработки в области дополненной и виртуальной реальности, однако ему также требуется развитие и в других областях.

игровой движок, GameDev, Unreal Engine, Unity, Unigine

В современных реалиях существует большое количество разных способов передачи информации. Одной из самых перспективных и наиболее быстро развивающихся является игровая форма предоставления информации [1]. Для создания игрового контента используется специализированное программное обеспечение – игровые движки.

Игровой движок – это программное обеспечение, предоставляющее разработчикам компьютерных игр библиотеки, модули, функции, ассеты (игровые объекты), плагины и множество другого программного обеспечения для разработки. Рассмотрим два наиболее популярных зарубежных игровых движков и один отечественного производства.

Unreal Engine (UE) – игровой движок с высокой производительностью для создания игр от компании Epic Games. UE предоставляет широкий набор инструментов для 3D-графики, светового и звукового сопровождения, а также реалистичной физики происходящего в игре. К достоинствам UE также можно отнести кроссплатформенность: проекты, сделанные на Unreal Engine, поддерживаются на большинстве доступных на данный момент платформах: Windows, macOS, Linux, iOS, Android, Xbox, PlayStation, Switch, в том числе и на отечественных аппаратных платформах, таких как Astra Linux [2].

Наверное, главное достоинство UE – язык программирования Blueprint, он же визуальное программирование, с которым можно работать без написания кода – вместо этого используются так называемые ноды, представляющие собой простейшие фрагменты кода, при соединении которых формируются функции, а для более опытных и продвинутых разработчиков имеется поддержка C++.

Также к преимуществам и особенностям последней версии UE можно отнести наличие следующих технологий:

Nanite – технология, которая дает возможность внедрения и визуализации высокополигональных моделей в свои проекты, при этом не теряя качества. Используя эту технологию, проекты наполняются реалистичными объектами из разных источников, при этом разработчик может не беспокоиться об оптимизации. В состав данной утилиты также входят библиотеки для работы со светом, анимирование и разрушение объектов;

Lumen – утилита для работы со светом, реагирующая на изменения происходящей в игре сцене, а, следовательно, и света в режиме реального времени. Это позволяет разработчикам не тратить время на расчеты для динамической освещенности или не использовать в своих проектах световые карты, а использовать готовые фотореалистичные эффекты освещения: отражения света, преломления света и множество других эффектов. Данная технология поддерживает имитацию естественных источников света такие как солнечный, лунный, звездный свет, а также свет огня;

MetaSounds – технология, работающая со звуковым сопровождением. Используя ее, разработчик имеет возможность создания интерактивного звукового сопровождения, которое создается через графический интерфейс. Это позволяет разработчику контролировать все звуковые характеристики: частота и амплитуда звуковых волн, различные звуковые эффекты, такие как эффект пространственности или эха.

Обобщив все достоинства UE можно сказать, что данное ПО предназначено для крупных и нагруженных игровых проектов на разных платформах. UE содержит большое количество библиотек и функций для реализации таковых проектов, но также имеется ряд недостатков, в особенности, для начинающих игровых разработчиков:

- разработка в Unreal Engine требует знания C++, который считается производительным и быстрым языком, однако не самым простым для новичков;

- наличие большого количества функций, библиотек и прочего ПО требует большого количества памяти, занимаемого на носителе для установки и оперативной памяти непосредственно для работы;

- движок не оптимизирован для работы с мобильными платформами и несмотря на то, что есть возможность разработки игр для мобильных платформ (iOS и Android), UE предназначен для разработки высококачественных игр, что требует большого количества ресурсов устройства, на котором

запускается игра, а значит производительность на мобильных платформах будет намного меньше.

– несмотря на существующую базу объектов *Unreal Engine* для развития проектов, многие из них являются либо платными, либо их использование требует авторских отчислений разработчикам.

Следующее ПО, которое мы рассмотрим это *unity*. *Unity* – это кроссплатформенный игровой движок для создания игровых проектов различных жанров. Ниже представлен список преимуществ движка *Unity*:

– в сравнении с другими игровыми движками *Unity* имеет весьма низкий порог вхождения, т.к. для работы в нем можно использовать графический язык программирования *Visual Scripting*, который значительно проще сложного *C++* [3]. Для более гибкой настройки можно воспользоваться языком *C#*, который также считается проще чем *C++*;

– *Unity* также имеет поддержку кроссплатформенности, что позволяет разрабатывать проекты, поддерживаемые на большинстве современных платформ: *Windows*, *Mac*, *Linux*, *iOS*, *Android*, *PlayStation*, *Xbox*, *Nintendo Switch* и др.;

– наличие магазина с большим выбором объектов и ресурсов. *Asset Store* – онлайн-магазин, содержащий большую базу. В нем находятся как платные, так и бесплатные объекты, и ресурсы, для разрабатываемых проектов.

Однако у *Unity* имеются недостатки:

– движок слабо оптимизирован под нагруженные проекты и в большей степени заточен под разработку игр для мобильных платформ. Для высококачественных проектов с реалистичной физикой, качественным звуком и красивой графикой ресурсов *Unity* может не хватить;

– *Unity* является проприетарным программным обеспечением с закрытым программным кодом, что означает, что изменить его для своих нужд не получится;

– исходя из преимуществ и недостатков можно увидеть, что *Unity* обладает теми же преимуществами, что и *UE*, в виде кроссплатформенности и более простым порогом вхождения, однако он не подходит для разработки крупных и масштабных проектов.

Теперь поговорим об отечественной разработке: *Unigine* – кроссплатформенное программное обеспечение для разработки игр, которое было разработано компанией *Unigine*, находящейся в Томске. С его помощью создаются *AR/VR* проекты, игровые и не только [4]. Движок также использует в работе разные графические программируемые интерфейсы приложения (*DirectX11*, *DirectX12*, *OpenGL*). Этой компанией также были разработаны тесты производительности, позволяющий быстро измерить мощность видеокарты (бенчмарки): *Heaven*, *Valley*, *Sanctuary*, *Tropics*, *Superposition*.

Ниже представлен список преимуществ использования разработчиками движка *Unigine*:

– данный движок поддерживает технологию кроссплатформенности и адаптирован под использование на ПК, игровых консолях и шлемах виртуальной реальности.

– работа с высоконагруженными мирами благодаря использованию двойной точности координат. Данная технология используется при создании авиасимуляторов, судоводных симуляторов, симуляций открытого космоса и других областях, то есть в проектах с перемещением на длинные расстояния.

– компания предоставляет бесплатную нелицензируемую версию движка (Unigine Community Software Development Kit) для проектов, не приносящих прибыль, что позволяет его использовать в учебных и некоммерческих целях.

Также у отечественного движка есть и недостатки, которые не позволяют его использовать в некоторых проектах:

– работа с данным движком может потребовать от разработчика глубоких знаний и навыков в сфере 3D-графики, программирования на языке C++, а также знания проприетарного скриптового языка программирования UnigineScript, что усложняет его освоение и устанавливает довольно высокий порог вхождения.

– отечественный движок не так распространен, как движки, описанные выше, вследствие чего наблюдается дефицит материалов для обучения, ресурсов, форумов, где можно получить ответ на интересующий разработчика вопрос от других разработчиков.

– использование движка в коммерческих проектах обязывает разработчика платить авторские отчисления компании-разработчику. Это относится к проектам, приносящим прибыль, то есть коммерческим. Стоимость лицензии может составлять от 10000 до 20000 долларов в год, что для индивидуальных разработчиков, инди-компаний или малых/средних компаний может быть слишком затратно.

Подводя итог, можно заключить, что движок Unreal Engine является мощным инструментом разработки высококачественных игр, но обладает более высоким порогом вхождения. Unity более лоялен к новичкам в разработке игр, однако и его возможности весьма ограничены – движок в основном подходит для разработки под мобильные платформы. Unigine предоставляет широкий функционал разработки в области виртуальной/дополненной реальности, но также может быть сложным в освоении разработчиками.

Список используемой литературы

1. Григорьева К., Васильев Н., Корчевой П., Комаров Р. Применение компьютерных игр в образовании // САПР и графика. 2000. №8 (286). С. 68–72.
2. Unity. URL: unity3d.com/ru/
3. Unreal Engine 5. URL: <https://www.unrealengine.com/en-US/unreal-engine-5>
4. Островский Ю. Н., Измайлов Н. С., Хомутовский С.Л. Технология «расширенной реальности» в вооруженных силах // Развитие военной педагогики в XXI веке. 2023. С 84–89.

УДК 004.81
ГРНТИ 28.23.29

РАЗРАБОТКА ПРОТОТИПА ПРОГРАММНОГО МОДУЛЯ РЕАЛИЗАЦИИ РЕАЛИСТИЧНОГО ПОВЕДЕНИЯ ВИРТУАЛЬНЫХ АГЕНТОВ В UNREAL ENGINE 5 ПОСРЕДСТВОМ СИСТЕМЫ ЗАПРОСОВ СРЕДЫ (EQS)

А. Е. Колмаков, В. Л. Литвинов

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

Изучены технологии реализации интеллектуального поведения виртуальных агентов встроенного инструментария Unreal Engine 5. Среди них выделены основные пять компонентов: контроллер агента, дерево поведения, органы чувств, система запросов среды и анимационный монтаж. Эти технологии использованы для решения задачи обхода препятствий агентами с разными значениями входных параметров EQS - при большей точности поведения агента постепенно повышается нагрузка на вычислительный ресурс, что приводит к низким значениям показателя FPS. Это говорит о том, что решение задачи увеличения реалистичности путём увеличения количества точек и уменьшения расстояния между точками системы пространственных запросов приводит к едва заметным результатам и неоправданным потерям производительности.

виртуальный агент, пространственный запрос, FPS, задача обхода препятствий

Виртуальные агенты используются не только в компьютерных играх, но и в медиа-сфере, в виртуальных симуляторах, в рекламе, в маркетинге, в технологиях дополненной и виртуальной реальности.

Повышение реалистичности поведения виртуальных агентов позволит создавать не только более реалистичные продукты развлекательного и рекламного характера, но и более реалистичное моделирование сценариев с участием виртуальных агентов.

Улучшение качества изображений и звука, а также разработка алгоритмов обработки данных могут привести к созданию виртуальных агентов, которые будут неотличимы от реальных людей.

Еще одной перспективной областью является разработка технологий виртуальной реальности, которые могут позволить пользователям взаимодействовать друг с другом посредством виртуальных агентов в режиме реального времени.

Более реалистичное поведение может включать в себя более естественные движения, мимику и жесты, а также более точные реакции на действия пользователя.

Задача распознавания препятствий является одной из самых сложных и важных задач моделирования реалистичного поведения виртуальных агентов [1].

Система запросов к среде (EQS) – это функция в системе искусственного интеллекта в Unreal Engine, которая позволяет собирать данные из среды и принимать решения на основе результатов различных тестов. Ее можно использовать для поиска наилучших локаций или действующих лиц на основе определённых пользователем тестов, таких как поиск ближайшего источника угрозы или определение прямой видимости агента [2, 3].

В данном тесте агенту нужно было как можно быстрее скрыться от глаз наблюдателя за ближайшим препятствием (рисунок 1). Сцена, начальное положение наблюдателя идентичны. Когда наблюдатель теряет цель из вида – тест останавливается. (угол обзора наблюдателя – 30 гр.)

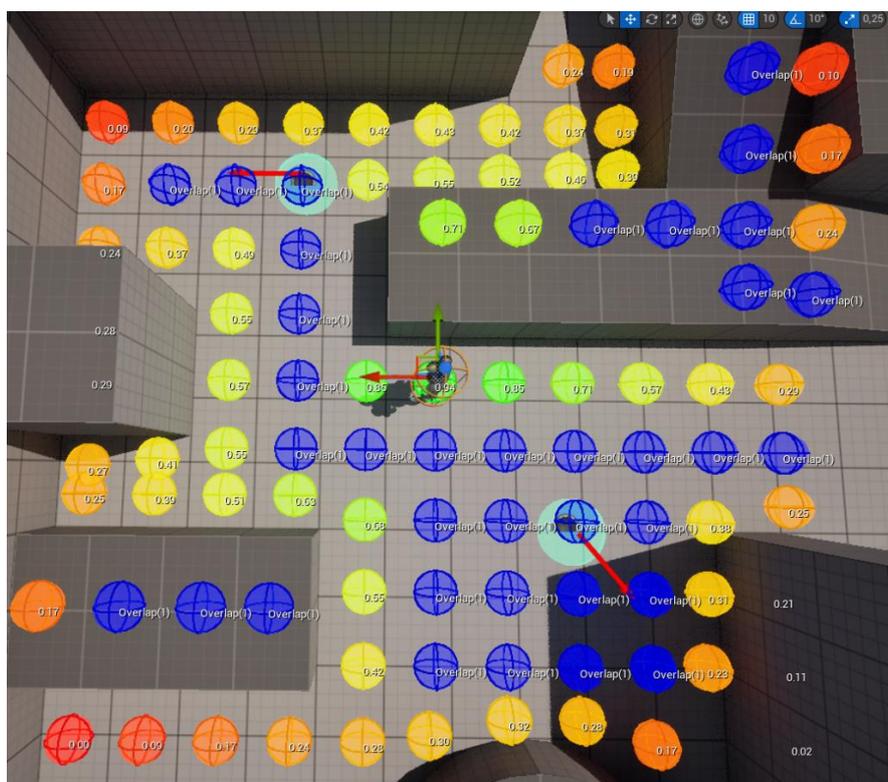


Рис. 1. Имитация сети EQS для решения задачи поиска укрытия вне зависимости от обзора наблюдателя. Агент уже «знает» точки потенциального укрытия, они отмечены красным, синий – не является укрытием

Анализ таблицы 1 подтверждает, что большое количество узлов сетки EQS приводит к резкому падению производительности при том, что время нахождения укрытия виртуальным агентом уже на значении параметра, характеризующего половину длины сетки EQS, равном 800 перестаёт гарантировано быть минимальным.

Для большей наглядности падение производительности при повышении нагрузки на вычислительный ресурс отображено на рисунке 2.

ТАБЛИЦА 1. Результаты теста на индивидуальном средстве информатизации со средними характеристиками

Grid half size	Finish time с.	Memory Мб.	FPS ср.
200	5,37	0,37	57,49
300	4,89	0,41	54,28
450	4,52	0,49	49,03
500	4,43	0,53	47,93
550	4,39	0,54	41,26
800	4,45	0,59	34,58
1000	4,42	0,68	20,17
1100	4,51	0,76	17,26
1200	4,42	0,77	13,81
3000	-	-	-

FPS ср. относительно параметра "Grid half size"

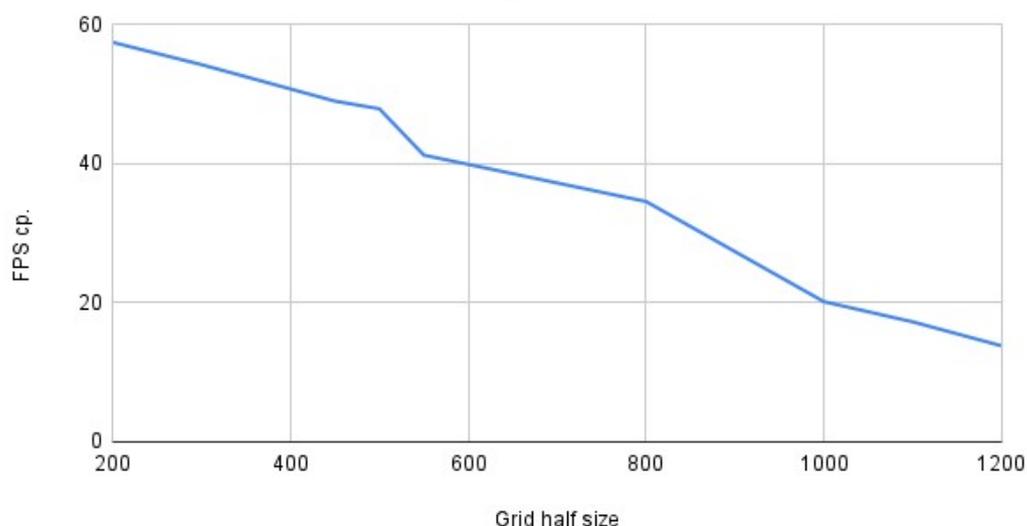


Рис. 2. Демонстрация закономерного падения производительности по мере увеличения количества узлов сетки EQS

Список используемых источников

1. Millington I. Artificial intelligence for games / Ian Millington, John Funge. 2nd ed. p. см. Includes index. ISBN 978-0-12-374731-0
2. Максименкова О. В. Программирование в Unreal Engine 5 для начинающего игроде-ла: основы визуального языка Blueprint / Ольга Максименкова, Никита Веселко. М.: Эксмо, 2023. 320 с. ISBN 978-5-04-164196-2
3. Jason G., Game Engine Architecture. Programming and internal structure. The third edition. SPb., 2021. 1136 p. ISBN 978-5-4461-1134-3
4. Russell S., & Norvig, P. Artificial intelligence: A modern approach (2nd ed.). Upper Saddle River, NJ: Prentice Hall, 2018. P. 1151.

УДК 004.75
ГРНТИ50.41.01

КЛАСТЕРИЗАЦИЯ НТТР-ЗАПРОСОВ МЕТОДОМ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ КОХОНЕНА

Т. В. Комашинский, Н. В. Чикалов

НПП «Радар ММС», Научно-исследовательский институт «Рубин»

В статье представлен подход к решению задачи поиска целевых компьютерных атак на прикладном уровне, основанный на самоорганизующихся нейронных сетях Кохонена. Цель исследования – повышение эффективности обнаружения аномалий атак в веб-трафике. В рамках данной статьи рассматривалось выявление SQL-инъекций посредством кластеризации сети Кохонена входящих запросов НТТР-трафика.

Сети Кохонена, кластеризация НТТР-запросов, самоорганизующиеся сети

Идентификация неизвестного типа трафика является важным требованием в методах и современных средствах мониторинга сетевого трафика на основе применения технологии DPI. В отчете OWASP Top-10 компьютерные атаки путем инъекции занимают лидирующие позиции в списке актуальных веб-угроз. Векторы атак направлены на веб-приложения, используя протокол НТТР в качестве транспортного механизма, поэтому крайне актуальна разработка научно-практических решений, которые позволят обнаружить отклонения в НТТР-запросах [1].

Достоинства самоорганизующихся нейронных сетей Кохонена: универсальность аппроксимации, обучение без учителя, самоорганизация, простота – позволили в результате анализа различных типов искусственных нейронных сетей (ИНС) обоснованно выбрать их для исследования в задачах обнаружения аномалий и сложных угроз в запросах НТТР-трафика.

Самоорганизующиеся нейронные сети Кохонена условно представимы двумя классами: слоем Кохонена и картой Кохонена. Отличие заключается в том, что слой основан на ИНС с неупорядоченными нейронами, а карта – на ИНС с упорядоченными нейронами.

В настоящей статье рассмотрена кластеризация с целью выявления SQL-инъекций среди всего набора данных [2]. Предлагается метод, который позволяет проводить кластеризацию НТТР-запросов слоем и картой Кохонена в режиме без учителя и не требует предварительной маркировки дата-сета.

Решаемая задача заключается в выявлении среди НТТР-запросов SQL-инъекций.

Сеть Кохонена является кластеризатором, а атака определяется на основе принадлежности к заданному кластеру.

Принципиальное отличие слоя Кохонена от других моделей ИНС – неконтролируемое обучение. Этот тип обучения позволяет данным обучающей выборки содержать значения только входных переменных. Сеть Кохонена учится понимать саму структуру данных и решает задачу кластеризации.

На рисунке 1 представлена архитектура слоя Кохонена.

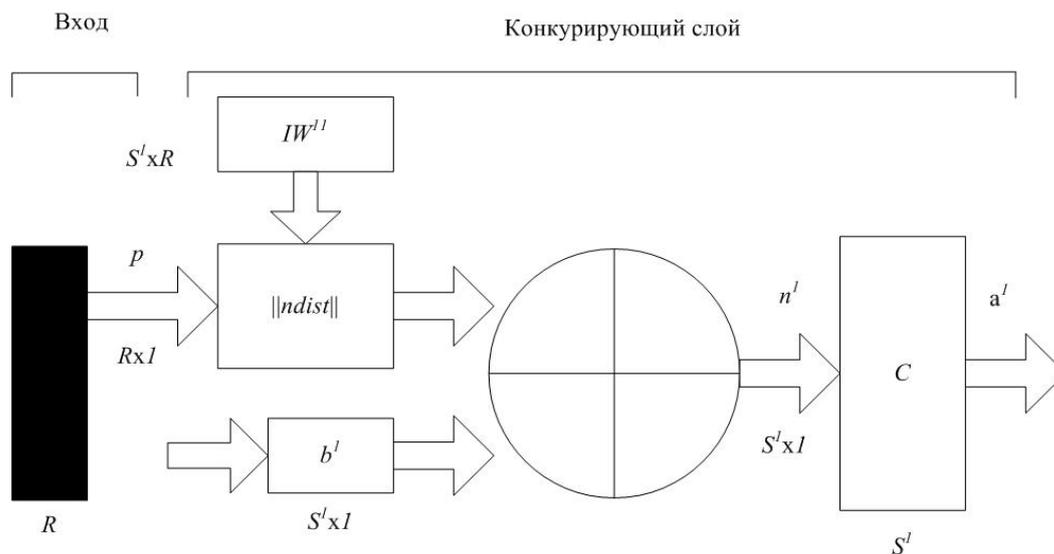


Рис. 1. Архитектура слоя Кохонена

Слой, представленный на рисунке 1, является слоем конкурирующего типа, поскольку в нем применена конкурирующая функция активации. Входом для слоя Кохонена является вектор p размером $R \times 1$. Здесь использован блок $||ndist||$ для вычисления отрицательного Евклидова расстояния между входным вектором p и строками матрицы весов IW^{l1} . Вход функции активации n^l – это результат суммирования вычисленного расстояния с вектором смещения b^l . Если все смещения нулевые, максимальное значение n^l не может превышать 0. Нулевое значение n^l возможно только тогда, когда вектор входа p оказывается равным вектору веса одного из нейронов. Если смещения отличны от 0, то возможны и положительные значения для элементов вектора n^l . Функция активации анализирует значения элементов вектора n^l и формирует выходы нейронов, равные 0 для всех нейронов, кроме одного нейрона – победителя, имеющего на входе максимальное значение. Таким образом, вектор выхода слоя a^l имеет единственный элемент, равный 1, который соответствует нейрону-победителю, а остальные равны 0. Функция активации может быть описана следующим образом:

$$a_i^1 = \begin{cases} 1, & i = i^*, i^* = \arg(\max n_i^1), \\ 0, & i \neq i^* \end{cases} \quad (1)$$

где n^1 – вход функции активации (результат суммирования вычисленного расстояния с вектором смещения b).

Эта функция распространяет свое действие на весь слой. Номер активного нейрона i^* определяет тот кластер, к которому наиболее близок входной вектор.

Для защиты веб-приложений от атак предлагается профилирование на основе кластеризации веб-трафика. Анализируя данные, полученные как искусственным путем (например, HTTPCSIC 2010), так и данные, полученные естественным способом (посредством захвата трафика с помощью Wireshark или tcpdump) посредством применения ИНС Кохонена, можно составить кластеры поведения определенных типов веб-трафика [3]. В результате экспериментальной кластеризации получено два: нормальный кластер и аномальный кластер (аномальный кластер может содержать в себе некоторое количество вложенных кластеров, принадлежащих разным типам атак).

В первом кластере агрегировались запросы, не относящиеся к SQL-инъекциям; во втором – запросы, являющиеся SQL-инъекциями.

Апробация метода осуществлялась на наборе данных HTTPCSIC 2010, содержащем 36000 записей нормального HTTP-трафика и 25065 записей аномального HTTP-трафика. В записях аномального трафика представлены следующие виды атак: SQL-инъекции, XSS, SSI, CRLF-инъекции, переполнение буфера. В таблице 1 представлены возможные атрибуты HTTP-трафика для построения кластеров.

ТАБЛИЦА 1. Атрибуты кластеризации HTTP-запросов

№	Название атрибута
1	Длина захваченного пакета
2	Длина полезных данных
3	Количество цифр в строке
4	Количество и тип специальные символы
5	Метод HTTP-запроса
6	Значение поля ContentLength
7	Значение поля ContentType

Данные атрибуты представляют собой исходный профиль запроса, представленный в числовых величинах:

$$r^i = (r_1^i, r_2^i, r_3^i, r_4^i, r_5^i, r_6^i, r_7^i), \quad (2)$$

где r_j^i – вес выбранного атрибута.

Для задачи выявления SQL-инъекций в http-трафике каждый запрос представлялся в виде одномерного вектора:

$$r^i = r_4^i. \quad (3)$$

Эксперимент проводился в среде MatlabR2022b с использованием пакета для проектирования, моделирования, разработки и визуализации нейронных сетей NeuralToolbox. В таблице 2 представлены примеры SQL-инъекций.

ТАБЛИЦА 2. Примеры SQL-инъекций

№	Пример
1	sqlinj/index1.php?id=1'
2	sqlinj/script.php?search_text=')+and+(news_id_author='1
3	sqlinj/index1.php?id=-1 UNION SELECT 4 username, password,1 FROM admin
4	sqlinj/index1.php?id=-1 UNION SELECT password FROM admin/*
5	sqlinj/index1.php?id=12;INSERT INTO admin (username, password) VALUES ('HaCkEr', 'foo');
6	sqlinj/index1.php?id=1 GROUP BY 2
7	sqlinj/index2.php?user=-1' UNION SELECT 1,2,3,4,5 INTO OUTFILE '1.php' --%20
8	sqlinj/index2.php?user=-1' UNION SELECT 1,LOAD_FILE('1.php'),3,4,5 --%20

Для обнаружения в запросах SQL-инъекций осуществлялся поиск следующих символов по их ASCII-кодировке. Выбранные для поиска символы являются характерными для данного типа атак: ', *, ;, -, %27, %2527, %2A, %252A, %3A, %253A, %2D, %252D.

Кластеризация проводилась по значению атрибута – количество и тип специальных символов в строке, характерных для SQL-инъекций.

Входной вектор был одномерный и представлял собой вес, назначенный в соответствии с количеством и типом встречаемых специальных символов. Веса для каждого запроса представлены на рисунке 2.

На рисунке 2 видно, что присвоение каждому запросу весов задействованных спецсимволов позволяет выделить SQL-инъекции. Можно заметить четкое разделение запросов по слоям, что позволяет судить о наличии определенных шаблонов SQL-инъекций.

В результате работы сети Кохонена, были получены результаты, представленные в таблице 3.

Из таблицы 3 следует, что посредством кластеризации http-трафика на основе применения ИНС Кохонена, было выявлено 92% SQL-инъекций в

GET-запросах и 90% SQL-инъекций в POST/PUT-запросах. Доля невыявленных SQL-инъекций составляет 8% и 10% соответственно.

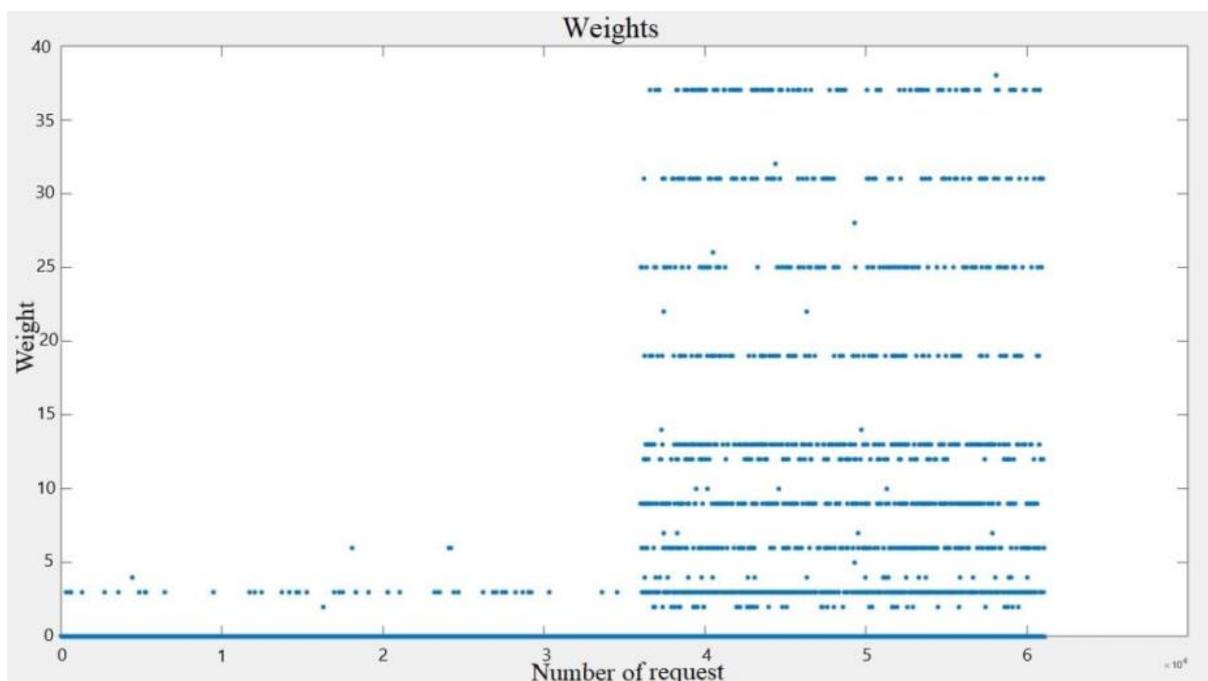


Рис. 2. Значение веса для каждого запроса

ТАБЛИЦА 3. Анализ результатов кластеризации HTTP-трафика

	HTTP-методы	
	GET	POST/PUT
Число записей, попавших во 2 кластер	1503	1509
Число записей, попавших во 2 кластер, но являющихся нормальными запросами	51	51
Число записей, попавших во 2 кластер, но не являющихся SQL-инъекциями.	87	87
Число записей, попавших во 2 кластер, являющихся SQL-инъекциями	1365	1371
Число записей, попавших в 1 кластер, являющихся SQL-инъекциями	116	150
Всего SQL-инъекций в датасете	1481	1521

Во второй части экспериментальных исследований, были построены кластеры с использованием карты Кохонена. В процессе обучения карты, в отличие от обучения слоя Кохонена, участвуют соседи нейрона-победителя, и, таким образом, топологическая карта выглядит более упорядоченной, чем области кластеризации слоя Кохонена. Принципиальных различий между

использованием слоя и карты нет, за исключением финального представления результата работы сети. Топология карты Кохонена представлена в виде гексагональной сетки размером 10x10. Результаты кластеризации представлены на рисунке 3.

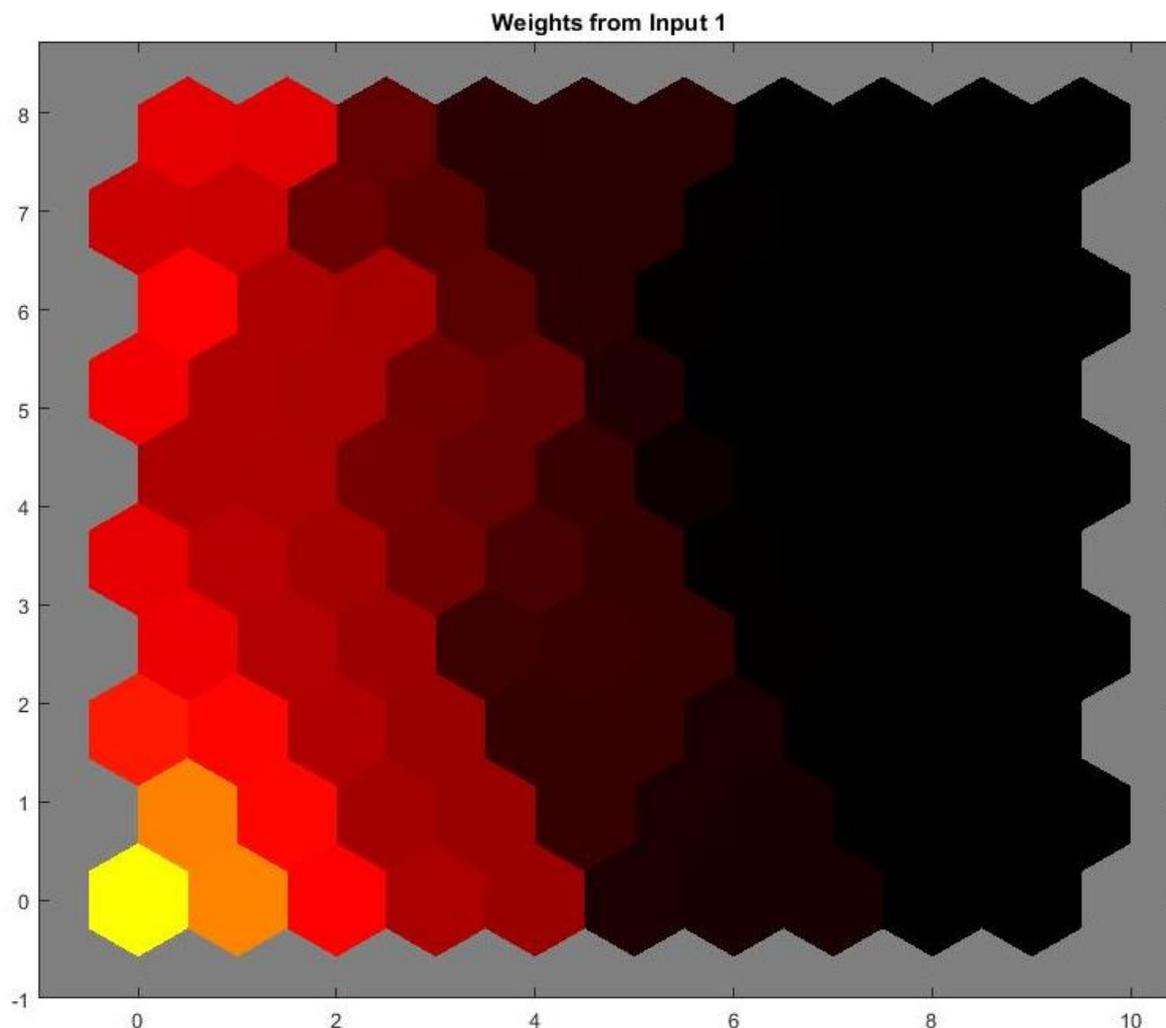


Рис. 3. Плоскость весов карты Кохонена

Рисунок 3 показывает плоскость веса для каждого нейрона. Все 100 нейронов можно укрупненно разделить на 2 кластера: первый кластер – трафик, не являющийся SQL-инъекциями, а второй – трафик, являющийся SQL-инъекциями. Более темным цветом выделена область, имеющая большой вес. Таким образом, там сосредоточены нейроны, реагирующие на нормальный трафик. Область нахождения аномальных нейронов соответствует областям, окрашенным желтым, оранжевым, красным и темно-красным цветами. Результаты, полученные в результате работы карты Кохонена аналогичны результатам работы слоя Кохонена, представленным в таблице 3.

Предложен метод анализа HTTP-трафика, использующий векторное представление HTTP-запросов и самоорганизующиеся нейронные сети Кохонена. Векторизованные HTTP-запросы имеют тенденцию группироваться

в четкие, непересекающиеся кластеры нормальных и аномальных запросов. Путем использования кластеризации получен помеченный набор данных для обучения и новые шаблоны для обнаружения атак типа SQL-инъекций.

Результатом использования сетей Кохонена является 90% эффективность обнаружения аномалий на основе SQL-инъекций.

Исследованный и апробированный подход подтверждает, что самоорганизующейся сети не нужно указывать, как выглядит аномалия. Научившись кластеризовать нормальное и аномальное поведение, ИНС готова к обнаружению любой отклоняющейся активности.

Список литературы

1. Ляшков М. А., Пчелинцев С. Ю., Ковалева О. А. Метод обнаружения и анализа аномального HTTP-трафика с помощью языковых моделей и векторного представления HTTP-запросов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2022. №04. С. 109–117. DOI: 10.37882/2223-2966.2022.04.23
2. Chaochao Luo. A novel web attack detection system for internet of things via ensemble classification. / Chaochao Luo, Zhiyuan Tan, Geyong Min, Jie Gan, Wei Shi, and Zhihong Tian // IEEE Transactions on Industrial Informatics, 2020.
3. Information Security Institute of CSIC: HTTP data set CSIC2010. URL: <https://www.isi.csic.es/dataset> (дата обращения: 01.02.2023).

Статья представлена научным руководителем, доцентом кафедры ИБ СПб ГЭТУ «ЛЭТИ», кандидатом технических наук, доцентом В. В. Комашинским.

УДК 004.75
ГРНТИ50.41.01

МОДЕЛЬ МОНИТОРИНГА ПОВЕДЕНИЯ КОРПОРАТИВНЫХ ВЕБ-ПОЛЬЗОВАТЕЛЕЙ

Т. В. Комашинский, Н. В. Чикалов

НПП «Радар ММС», Научно-исследовательский институт «Рубин»

Известно, что одной из основных причин возникновения опасности в веб-приложениях являются генерация аномального трафика, непрофильного трафика, изменения профиля поведения веб-приложения или веб-пользователя, недоверенные фреймворки и модули, которые «перенагружены» лишним функционалом т. д. Все это, создаёт ненужную нагрузку, затрудняющую доступ к веб-ресурсу. Это обстоятельство, является одним из тех событий, с которыми рано или поздно могут столкнуться корпоративные веб-приложения, неадаптированные к разным типам нагрузки. Учитывая это, для определения профиля поведения веб-приложения и веб-пользователя предлагается структурная модель виртуализированной функции мониторинга веб-приложений.

Виртуализированные сетевые функции, мониторинг веб-приложений, модель мониторинга

Предлагается модель веб-приложений в виртуализированных сетях. Отличия предлагаемого подхода от существующих:

1. Классические программно-аппаратные средства зависят от аппаратной платформы, долгие в разработке и внедрении, привязаны к конкретному производителю аппаратной платформы [1].

2. Облачные решения подходят не всем типам компаний – многие компании имеют ограничения на использование облачных сервисов информационной безопасности.

3. Существующие решения предлагается внедрять в существующие сети, что в условиях стагнации телекоммуникационных технологий с переходом на принцип All IP в скором времени будет являться «тупиковым решением». Разрабатываемые современные решения должны быть направлены на возможность встраивания в SDN-сети (Software Defined Networking).

4. Предлагаемые решения являются либо WAF-решениями (Web Application Firewall), либо WAM-решениями (Web Application Monitoring).

5. Размещение на стандартных архитектурах x86.

Структура предлагаемой виртуализированной системы веб-мониторинга представлена на рисунке 1. Разрабатываемая виртуализированная система базируется на микросервисной архитектуре – каждая служба представлена своим сервисом. Это позволит внедрять новые и модифицировать существующие контейнеры виртуализированной системы без остановки. В системе предлагается следующая компоновка по контейнерам.



Рис. 1. Структура виртуализированного веб-мониторинга

Контейнер 1 содержит в себе «подконтейнеры», ориентированные для обнаружения определенного вида атак. Это позволит повысить эффективность обнаружения атак, путем распараллеливания анализа входного веб-трафика [2].

Контейнер 2 содержит в себе средства анализа и прогнозирования. Это означает, что в данном контейнере функционирует программное средство, логика которого настроена на прогнозирование следующего состояния.

Контейнер 3 содержит средства контентно-адаптивной обработки, которые исследуют входящие/исходящие потоки в зависимости от типа (видео, аудио, передача файлов и т. д.) трафика.

Контейнер 4 содержит средства для автоматического тестирования веб-приложения на предмет доступности сервисов.

Контейнеры 5 содержит средства поведенческого анализа. Данный контейнер отвечает за анализ поведения веб-приложений.

Контейнер 6 отвечает за анализ веб-пользователей.

Контейнер 7 содержит средства подготовки отчетов для лиц, принимающих решения.

Под профилем пользователей понимается вектор интересов и тематические выборы, построенные на основе обрабатываемых веб-ресурсов. Сбор тематических профилей пользователей создаёт матрицу. В этой матрице на каждой строке указывается пользователь, а в каждом столбике показаны признаки. В зависимости от частоты обращения ресурсов, входящих в категории поведения пользователей и объёма входящего трафика, вычисляется значимость признаков. Для повышения качества модели проводится процесс нормализации свойств в интервале $[0; 1]$. После завершения процесса проектирования признаков, для построения модели выбираются более информативные и достоверные признаки. Это уменьшает объём обрабатываемой информации, создаёт условие для предотвращения повторения процесса обучения, а также, в целом, повышает качество модели. В рассматриваемом случае ресурсы группируются согласно тематической категории. Понятно, что ресурсы, которые относятся к одной тематической категории, могут быть размещены в различных источниках.

Учитывая то, что профили представляют собой многомерные векторы, удобнее всего пользоваться картами Кохонена для визуализации.

Отличительной особенностью предлагаемого решения является возможность одновременный контроля и веб-пользователя и веб-приложения (составляется профиль поведения веб-приложения компании и профиль поведения сотрудников компании, которые во время работы обращаются к сторонним веб-ресурсам).

Предлагаемое решение для веб-мониторинга:

- независимо от аппаратного обеспечения и легко интегрируется практически с любым имеющимся;
- позволит осуществлять мониторингом поведения как веб-приложения, так и веб-пользователя, и является универсальным, так как может быть встроено как в оборудование существующих сетей, так и в оборудование облачных провайдеров.

Список литературы

1. SDN и NFV: как это работает на сети оператора связи. URL: <https://shalaginov.com/2015/12/27/sdn-%D0%B8-nfv-%D0%BA%D0%B0%D0%BA-%D1%8D%D1%82%D0%BE-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B5%D1%82-%D0%BD%D0%B0-%D1%81%D0%B5%D1%82%D0%B8-%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0> (дата обращения 01.11.2023)

2. Lessons learned from the world's most notable privacy abuses and security incidents, 2017. URL: <https://www.forrester.com/report/Lessons-Learned-From-The-Worlds-Most-Notable-Privacy-Abuses-And-Security-Incidents-2017/RES137315> (дата обращения 01.11.2023)

Статья представлена научным руководителем, доцентом кафедры ИБ СПб ГЭТУ «ЛЭТИ», кандидатом технических наук, доцентом В. В. Комашинским.

УДК 004.75
ГРНТИ 50.41.01

ПРЕДЛОЖЕНИЯ ПО ФОРМИРОВАНИЮ СИСТЕМЫ МОНИТОРИНГА ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ ВИРТУАЛИЗИРОВАННЫХ СЕТЕВЫХ ФУНКЦИЙ

Т. В. Комашинский, Н. В. Чикалов

НПП «Радар ММС», Научно-исследовательский институт «Рубин»

Рост числа веб-приложений сделал мониторинг веб-ресурсов серьезной проблемой. Наличие большого числа библиотек и фреймворков увеличивает количество потенциальных уязвимостей в конечном веб-приложении. Современный мониторинг веб-приложений – это синтетическое решение для мониторинга, которое постоянно проверяет время отклика, содержимое, общую производительность веб-приложений, безопасность. В настоящей работе авторы предлагают структурную модель виртуализированной функции мониторинга веб-приложений.

Виртуализированные сетевые функции, мониторинг веб-приложений

На сегодняшний день российские компании активно внедряют подход виртуализации сетевых функций (VNF) [1].

Виртуализация сетевых функций – это концепция сетевой архитектуры, предлагающая использовать технологии для виртуализации целых классов функций сетевых узлов в виде составных элементов, которые могут быть соединены вместе или связаны в цепочку для создания веб-сервисов.

Чтобы реализовать все преимущества технологии виртуализации сетевых функций, необходимо контролировать: кто и насколько интенсивно работает с веб-приложениями, какие взаимозависимости существуют между веб-приложениями, каковы оптимальные способы их использования. Ответы на эти вопросы помогут подготовить профили веб-приложений для максимально эффективного и безопасного предоставления услуг. За последние два года SDN и VNF технологии переместились на быстрые изменения ресурсов сети и вывод новых услуг для конечных пользователей с точки зрения веб-приложений. Теперь основной задачей считается обеспечение наиболее комфортных условий для работы веб-приложений в зависимости потока и типа данных, которые они передают или получают. Следовательно, правила, профили и политики доступа в сети меняются в зависимости от требований веб-приложений и требований безопасности [2].

Преимущество VNF заключается в том, что виртуализированные сетевые функции гораздо более динамичны, чем их традиционные программно-аппаратные аналоги, так как они могут быть развернуты и удалены по требованию и масштабироваться в соответствии с изменением объема трафика.

В следствие этого возникает потребность в разработке единого средства мониторинга веб-приложений.

Учитывая тенденции развития ИКТ в сторону SDN и VNF, предполагается разумным.

Структура предлагаемого решения представлена на рисунке 1.

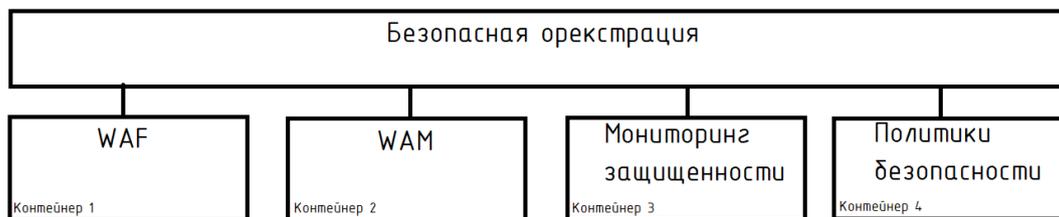


Рис. 1. Структура VNF-решения

Разрабатываемая система мониторинга представляет собой набор контейнеров с разными средствами контроля веб-приложений. Функция безопасной оркестрации позволяет управлять контейнерами с учетом требований регуляторов ИБ.

Данное решение позволит в полной мере охватить все аспекты функционирования веб-приложения и построить полный профиль «нормального» поведения.

При необходимости можно добавлять новые контейнеры.

Безопасная оркестрация позволит системе быть устойчивой в условиях внешнего деструктивного воздействия.

В целом, это решение позволит:

- защитить корпоративное веб-приложение;
- наблюдать и анализировать функционирование в WEB-приложений.

Технология VNF может обеспечить SDN инфраструктурой, на которой работает программное обеспечение SDN. Более того, цели NFV близки к целям SDN в части использования обычных стандартных серверов и коммутаторов.

Предполагается, что VNF целесообразно использовать в качестве основной архитектурой для построения систем мониторинга веб-приложений. Микросервисная архитектура позволит добавлять новые «модули» к VNF-решению без остановки работы всей системы мониторинга.

Список литературы

1. SDN и NFV: как это работает на сети оператора связи. URL: <https://shalaginov.com/2015/12/27/sdn-%D0%B8-nfv-%D0%BA%D0%B0%D0%BA-%D1%8D%D1%82%D0%BE-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B5%D1%82-%D0%BD%D0%B0-%D1%81%D0%B5%D1%82%D0%B8-%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0> (дата обращения 01.11.2023)

2. Lessons learned from the world's most notable privacy abuses and security incidents, 2017. URL: <https://www.forrester.com/report/Lessons-Learned-From-The-Worlds-Most-Notable-Privacy-Abuses-And-Security-Incidents-2017/RES137315> (дата обращения 01.11.2023)

Статья представлена научным руководителем, доцентом кафедры ИБ СПб ГЭТУ «ЛЭТИ», кандидатом технических наук, доцентом В. В. Комашинским.

УДК 004.492.3+004.93'11
ГРНТИ 50.41.27

О НЕКОТОРЫХ АСПЕКТАХ СТАТИЧЕСКИХ ПРИЗНАКОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С. А. Копылов, Е. В. Михайлова

Академия Федеральной службы охраны Российской Федерации

Вредоносное программное обеспечение остается наиболее значимой угрозой информационной безопасности конфиденциальной информации и персональных данных пользователей. Существенный рост объемов передаваемой и обрабатываемой информации показал возросшее количество случаев внедрения и последующего распространения вредоносного кода в типы данных, содержащие защищаемую информацию. Указанная особенность делает задачу по идентификации признаков пространства, характеризующего вредоносное программное обеспечение, встроенное в различные форматы файлов, актуальным направлением исследования. В работе приведен обзор статических признаков вредоносного программного обеспечения, представлено их описание и приведены отличительные особенности, присущие файлам, содержащим встроенный вредоносный код.

вредоносное программное обеспечение, статические признаки

В качестве признаков пространства вредоносного программного (ВПО) обеспечения могут выступать статические или динамические признаки (характеристики) исполняемых и текстовых файлов с расширенным функционалом. Статические признаки – характеристики файла, которые извлекаются без его выполнения или запуска. С помощью них мы пытаемся выяснить, что ВПО делает, какие команды в нём работают [1]. Статические характеристики могут быть извлечены из следующих файлов:

1. Исполняемые файлы PE. Статические характеристики исполняемых файлов Windows извлекаются из бинарного содержимого исполняемого

файла или исходного файла на языке ассемблера, полученного после декомпиляции и дизассемблирования бинарного исполняемого файла;

2. Исполняемые файлы APK. В приложениях операционной системы Android характеристики извлекаются путем дизассемблирования APK файлов;

3. Текстовые документы с расширенным функционалом (PDF, DOCX, RTF). Статические признаки выделяются из тела PDF файла посредством декомпиляции и декодирования PDF файла, а также из макросов и активного содержимого файлов DOCX и RTF.



Рис. 1. Классификация признаков вредоносного программного обеспечения

К статистическим признакам вредоносного программного обеспечения относятся:

- строки (последовательность символов);
- байты и код N-грамм (непрерывной последовательности из N элементов текста) [2];
- энтропия последовательности байт;
- визуализация контента изображениями в оттенках серого;
- операторы вызова функций;
- операторы вызова API функций;
- граф потока управления.

Содержимое строк позволяет получить информацию об особенностях функционирования анализируемой программы или файла. К полезной информации в строках, относятся: подключаемые URL-адреса, расположение или пути файлов, к которым осуществляется обращение, имена меню при-

ложения и так далее. Обнаружение ВПО, основанное на анализе строк, может быть реализовано извлечением строк, обучением модели и последующим анализом поступающих данных на основе обученной модели.

N -граммой может быть последовательность слов, букв, символов или знаков, входящих в текст. N -граммы могут быть извлечены из: последовательностей байт, представляющих бинарное содержимое программы, исходного кода на языке ассемблера и содержимого текстового документа. Байтовые N -граммы извлекаются обнаружением уникальной комбинации каждых N последовательных байт, являющейся индивидуальным признаком. При обнаружении ВПО из инструкций ассемблера в качестве N -граммы берут последовательность мнемоник инструкции вида "ADD", "MUL", "PUSH". Использование N -грамм характеризуется такими особенностями как [3]:

- количество возможных N -грамм, описывающих вредоносное программное обеспечение, может превышать количество элементов, входящих в обучающую выборку, что делает задачу обучения нерешаемой;
- ключевые N -граммы выбираются на основе частоты встречаемости N -граммы в строковом содержимом данного набора данных;
- в процессе обнаружения осуществляется сопоставление ключевой N -граммы информационным последовательностям анализируемого файла. При отсутствии ключевой N -граммы инфицированный файл будет ошибочно классифицирован как файл, без ВПО.

Энтропия или мера неопределенности системы (количество информации, приходящегося на один передаваемый символ) применяется в качестве классификационного признака в процессе обнаружения вредоносного программного обеспечения. Вредоносное программное обеспечение, как и любое программное обеспечение, может содержать средства защиты от анализа. К существующим средствам защиты от статического анализа относится применение упаковщиков (сжатие с шифрованием данных или без такового), обфускация кода, а также методы маскирования информации. Анализ энтропии файлов, содержащих вредоносные вложения сжатых или зашифрованных, показал, что энтропия оригинальных файлов в значительной степени меньше энтропии файлов с вредоносными вложениями, что позволяет использовать количественные значения энтропии в качестве классификационного признака. В контексте теории информации энтропия последовательности байт отражает ее статистическую вариацию. В частности, нулевая энтропия будет означать, что один и тот же символ повторяется в анализируемом сегменте. Такое поведение можно наблюдать в "дополненном" фрагменте кода. Напротив, высокое значение энтропии будет указывать на то, что фрагмент полностью состоит из различных значений.

В задачах обнаружения вредоносного программного обеспечения классификационный признак энтропии информационной последовательно содержимого файла может быть использован в процессе обучения модели. При этом для каждого вида вредоносного программного обеспечения, а также используемого средства защиты от анализа, необходимо формировать отдельный набор данных (обучающую выборку) и проводить обучение. Указанная особенность обусловлена наличием индивидуальных порогов срабатывания для каждого типа вредоносного программного обеспечения, что не позволяет использовать единую обученную модель для обнаружения вредоносных вложений различного типа. Кроме того, существуют методики снижения энтропии в исполняемых файлах посредством добавления инструкций определенного типа [4].

Вызовы API функций представляют собой функции интерфейса прикладного программирования для взаимодействия программных компонентов. Из-за того, что API функции и системные вызовы связаны со службами, предоставляемыми операционными системами и программным обеспечением нет другого способа получить доступ к системным ресурсам без использования функций API, вызов определенных функций API – это ключевой признак обнаружения ВПО. Для решения задачи обнаружения вредоносных программ также используют алгоритмы обучения ассоциативным правилам на основе правил ассоциации классов объектно-ориентированного программирования.

Визуализация контента изображениями в оттенках серого – техника по отображению бинарного содержимого ВПО изображением в оттенках серого. Оно достигается интерпретацией байтов в виде пикселей на изображении со значениями от 0 до 255 (0 – черный цвет, 255 – белый). Пример визуализации контента ВПО изображением в оттенках серого представлен на рисунке. 2 [5].

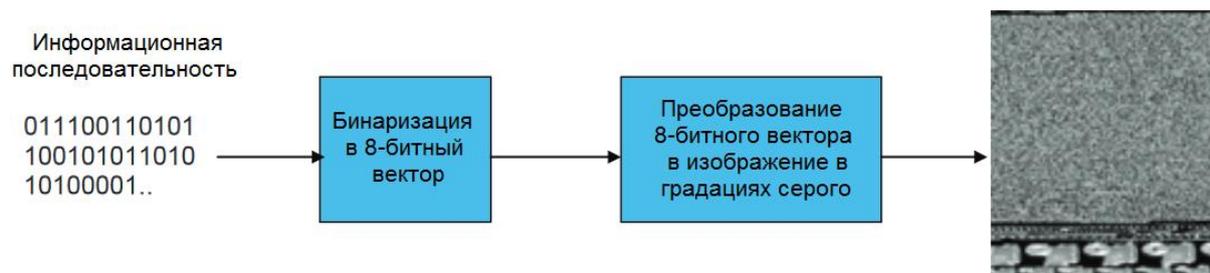


Рис. 2. Визуализация контента изображениями в оттенках серого

Часто, представляя анализируемый файл изображением в оттенках серого, можно обнаружить малые различия между образцами, принадлежащими к одному и тому же семейству встроенного ВПО. При этом изображения образцов одного семейства отличаются от изображений,

принадлежащих другому. Наличие визуального сходства применяется в процессе обнаружения (классификации) вредоносных программ.

Визуализация изображения в оттенках серого имеет недостатки, связанные с процессом формирования изображения. Так как бинарные файлы не являются двумерными изображениями, преобразование вносит в них дополнительные характеристики, влияющие на качество. Необходимо выбрать ширину изображения (новый параметр). Выбор ширины влияет на высоту изображения в зависимости от размера бинарного файла, что приводит к наложению несуществующих пространственных корреляций между пикселями в разных строках. Методы визуализации не применимы для обнаружения ВПО, защищенного от анализа упаковщиками, обфускаторами или средствами маскирования, так как указанные техники изменяют структуру байт файла, а, следовательно, и формируемое изображение.

Граф вызова функций – ориентированный граф, вершины которого представляют функции, из которых состоит программа, а ребра символизируют вызовы функций. Вершина может быть представлена одним из двух типов функций [6]:

- – локальные функции, реализованные разработчиком для выполнения конкретных задач;
- – внешние функции, предоставляемые операционной системой, системными и внешними библиотеками.

Особенностью графа в том, что только локальные функции могут вызывать внешние функции, а не наоборот. Графы вызовов функций генерируются на основе статического анализа файла дизассемблирования. В качестве подхода к обнаружению ВПО может быть использован алгоритм кластеризации, основанный на структурном сходстве графов вызовов функций. В качестве алгоритмов кластеризации выступают: метод k-medoids (версия алгоритма k-средних для анализа графов), плотностный алгоритм пространственной кластеризации с присутствием шума.

Граф потока управления – ориентированный граф, в котором узлы представляют базовые блоки, а ребра представляют пути потока управления. Базовый блок – это линейная последовательность программных инструкций, которая имеет точку входа и выхода (первая и последняя выполненная команда). Граф потока управления является представлением всех путей, которые можно пройти во время выполнения программы. Обнаружение ВПО может быть реализовано посредством алгоритмов классификации за счет преобразования разреженного графа потока управления в векторное представление и бинарной классификации полученных значений.

Список используемых источников

1. Positive Technologies. Актуальные киберугрозы: III квартал 2023 года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3> (дата обращения 30.05.2024)

2. ГОСТ Р 59163-2020. Информационные технологии. Методы и средства обеспечения безопасности. Руководство по обеспечению безопасности при внедрении серверов виртуализации. М.: Стандартинформ, 2020. 27 с.

3. Design-hero. Анализ вредоносных программ 101. Базовый статический анализ. URL: <https://design-hero.ru/articles/313698> (дата обращения 30.05.2024)

4. Shabtai A., Moskovitch R., Feher C., Dolev S., Elovici Y. Detecting unknown malicious code by applying classification techniques on OpCode patterns // Security Informatics. 2012. Т. 1. № 1. С. 1–22.

5. Саттон М., Грин А., Амини П. Fuzzing. Исследование уязвимостей методом грубой силы. Пер. с англ. СПб.: Символ-Плюс, 2009. 560 с.

6. Бегаев А. Н., Кашин С. В., Маркевич Н. А., Марченко А. А. Выявление уязвимостей и недеklarированных возможностей в программном обеспечении: Учебно-методическое пособие. СПб.: Университет ИТМО, 2020. 38 с.

УДК 004.492.3+001.891.572
ГРНТИ 50.41.27

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ВНЕДРЕНИЯ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СОДЕРЖАЩЕГО СРЕДСТВА ЗАЩИТЫ ОТ АНАЛИЗА, В ФАЙЛЫ ФОРМАТА PDF

С. А. Копылов, А. А. Полехин

Академия Федеральной службы охраны Российской Федерации

Обеспечение информационной безопасности информационных систем является одним из наиболее актуальных направлений реализации политики в области кибербезопасности. Стремительный рост количества инцидентов нарушения информационной безопасности делает задачу по совершенствованию средств защиты актуальным направлением исследований. Для решения указанной задачи необходимо оценивать не только существующие средства защиты и присущие им недостатки, но средства реализации компьютерных атак. В работе представлена функциональная модель внедрения вредоносного программного обеспечения, содержащего средства защиты от анализа, в файлы формата PDF. Разработанная модель учитывает особенности внедрения вредоносного кода в структурные компоненты PDF файлов и применение обфусцирующих преобразований, используемых для защиты встроенного вредоносного кода от статических методов анализа.

вредоносное программное обеспечение, файлы формата PDF, обфускация

Поддержание высокого уровня защищенности информационных систем является одной из трудновыполнимых задач ввиду постоянного совершенствования методов и средств реализации компьютерных и целевых атак. Внедрение и реализация вредоносного программного обеспечения остается одним из наиболее распространенных классов методов успешно реализуемых атак. Высокий процент успешно реализованных атак посредством использования вредоносного программного обеспечения обусловлен применением к встраиваемому вредоносному коду средств защиты от анализа.

Существующие методы защиты вредоносного программного обеспечения от анализа могут быть разделены на [1]:

– – методы защиты от статического анализа (антистатические методы защиты): использование упаковщиков (шифровальщиков); обфускация программного кода и сокрытие информации;

– – методы защиты от динамического анализа (антидинамические методы защиты): обнаружение отладчиков, обнаружение виртуальных машин, обнаружение средств мониторинга, а также другие методы защиты от отслеживания.

Исходя из особенностей построения и функционирования файлов формата PDF, использование антидинамических методов защиты вредоносного программного обеспечения, внедряемого в структурные элементы файлов формата PDF, является малоэффективным и не позволяет защитить встроенный вредоносный код от обнаружения антивирусными средствами. При этом антистатические методы защиты вредоносного программного обеспечения позволяют обходить существующие средства обнаружения. Так применение обфускирующих преобразований (обфускации) позволяет преобразовывать исходный код к виду функционально идентичному оригиналу, но существенно повышающего сложность его анализа и декомпиляции.

Методы обфускации программного кода (в том числе и вредоносного) разделяются на следующие классы [2, 3]:

– традиционные (классические) методы, реализующие вставку лишнего кода, замену регистров (адресов памяти), замену инструкций и переупорядочивание инструкций;

– метод отборных инструкций, осуществляющий внесение в исходный код или содержимое специальным образом составленных поврежденных инструкций (функций), которые нарушают работу дизассемблера;

– методы обфускации, основанные на системе обработки исключений операционной системы Windows, позволяющие осуществлять сокрытие потока управления посредством внедрения и реализации собственных механизмов обработки исключений.

Для разработки функциональной схемы внедрения вредоносного программного обеспечения, защищенного от анализа, проведено исследование структурных компонентов файлов формата PDF. К основным структурным объектам, составляющим файл формата PDF, относятся [4, 5]:

- заголовок (H), определяющий версию (спецификацию) файла PDF;
- тело (B), содержащее структурированную последовательность объектов, которые определяют итоговое представление;
- таблица перекрестных ссылок (X), содержащая информацию о каждом объекте в теле документа в виде строки описания места данного объекта;
- концевик (T), предназначенный для чтения файла PDF программой-просмотрщиком и перехода к таблице перекрестных ссылок.

Представленная структура позволяет описать файл формата PDF (F_{pdf}) выражением:

$$F_{pdf} = code(F_{dec}) = code(\{H, B, X, T\}), \quad (1)$$

где F_{pdf} – файл формата PDF ($F_{pdf} \in F$), F – множество всех файлов, $F_{dec} = \{H, B, X, T\}$ – PDF файл, состоящий из структурных элементов, $code$ – функция кодирования (формирования PDF документа).

Процесс внедрения вредоносного программного обеспечения в файл формата PDF состоит из следующих этапов:

- декодирование файла формата PDF;
- выделение позиций встраивания;
- внедрение вредоносного кода в объекты тела PDF файла;
- применение обфусцирующего преобразования;
- кодирование элементов в PDF файл.

Функциональная схема внедрения вредоносного программного обеспечения, защищенного от анализа, в структурные элементы тела файла формата PDF представлена на рисунке 1.

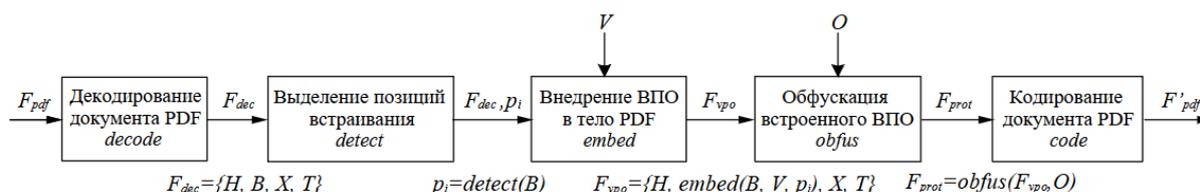


Рис. 1. Функциональная модель внедрения вредоносного программного обеспечения, защищенного от анализа в файл формата PDF

На первом этапе внедрения вредоносного кода осуществляется декодирование файла формата PDF F_{pdf} на структурные элементы функцией *decode*:

$$F_{dec} = decode(F_{pdf}) = \{H, B, X, T\}. \quad (2)$$

В процессе декодирования исходного PDF файла F_{pdf} осуществляется анализ заголовка H на предмет наличия конструкции вида "%PDF – 1.N", (где N – версия спецификации файла), однозначно характеризующий PDF документ указанной версии. Отсутствия указанной информационной последовательности позволяет сделать вывод о том, что анализируемый файл F_{pdf} не является файлом формата PDF.

На втором этапе осуществляется выделение (детектирование) позиций встраивания p_i в теле B декодированного документа F_{pdf} функцией *detect*:

$$p_i = detect(B). \quad (3)$$

В качестве позиций встраивания p_i выступает содержимое следующих объектов тела PDF документа B : логический объект, число (целое и десятичное), строка, имя, массив и прочие. Объекты тела PDF файла начинаются со специального символа "\" и располагаются между последовательностями символов вида "xxx 0 obj" и "end obj" (xxx – порядковый номер объекта, "end

obj'' – символ окончанием объекта) и описывают качественные или количественные признаки объекта

На третьем этапе осуществляется встраивание вредоносного программного обеспечения (вредоносного кода) V в выделенные позиции встраивания p_i функцией $embed$ исходного PDF файла F_{pdf} :

$$B' = embed(B, V, p_i), \quad (4)$$

где B' – модифицированное тело PDF документа F_{pdf} , $V = \{v_1, v_2 \dots v_n\}$ – вредоносное программное обеспечение (вредоносный код), n – длина (размер) встраиваемого вредоносного кода.

В результате внедрения вредоносного программного обеспечения осуществляется модификация структуры и содержимого объектов тела файла формата PDF.

На этапе применения обфусцирующего преобразования к сформированному содержимому модифицированного тела B' исходного PDF документа осуществляется одно или несколько обфусцирующих преобразований $obfus$:

$$B_{obf} = obfus(B'). \quad (5)$$

В результате наложения обфускации формируются структурные элементы $\{H, B_{obf}, X, T\}$ файл формата PDF F'_{pdf} , содержащие обфусцированное вредоносное вложение (вредоносный код).

На заключительном этапе осуществляется кодирование сформированных структурных элементов в файл формата PDF F'_{pdf} функцией $code$:

$$F'_{pdf} = code(\{H, B_{obf}, X, T\}). \quad (6)$$

Результатом кодирования является формирование электронного документа формата PDF F'_{pdf} ($F'_{pdf} \in F$), содержащего встроенное вредоносное программное обеспечение. Стоит отметить, что внешнее отображение PDF файлов F'_{pdf} и F_{pdf} остается идентичным, при существенном различии в структурном плане $F'_{pdf} \neq F_{pdf}$.

Разработанная функциональная модель внедрения вредоносного программного обеспечения, содержащего средства защиты от анализа, в файлы формата PDF позволяет: описать процесс внедрения вредоносного программного обеспечения (программного кода) в структуру PDF файла; определить потенциальные позиции внедрения вредоносного кода в структуру PDF файла; а также учесть применение обфусцирующих преобразований,

направленных на защиту (сокрытие) встроенного вредоносного кода от обнаружения используемыми средствами защиты. Реализация разработанной модели на практике и экспериментальная оценка разработанной модели являются направлением дальнейших исследований.

Список используемых источников

1. Afianian A., Niksefat S., Sadeghiyan B., Baptiste D. Malware Dynamic Analysis Evasion Techniques: a Survey // ACM Computing Surveys. 2019. Т. 52. №. 6. С. 1–28.
2. Бутин А. А. Технологии защиты программного обеспечения // Информационные технологии и математическое моделирование в управлении сложными системами: электрон. научн. журн. 2019. № 2. С. 53–63. URL: <http://ismm. irgups.ru/tehnologii-zashchity-programmnogo-obespecheniya> (дата обращения: 19.06.2019)
3. Салахутдинова К. И., Малков В. В., Кривцова И. Е. Сравнительный анализ подходов к идентификации программного обеспечения // Безопасность информационных технологий. 2019. Т. 26. № 2. С. 58–66.
4. ISO 32000–1:2008. Document management. Portable document format. Part 1: PDF 1.7. First edition. Женева, Швейцария: International Standard, 2008. 756 с.
5. ISO 32000–2:2020. Document management. Portable document format. Part 2: PDF 2.0. Second edition. Женева, Швейцария: International Standard, 2017. 1004 с.

УДК 004.492.3
ГРНТИ 50.41.27

ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ФАЙЛАХ ФОРМАТА PDF ПОСРЕДСТВОМ АНАЛИЗА ПОКРЫТИЯ КОДА ПРОСМОТРИЩА

С. А. Копылов, Н. А. Цапков

Академия Федеральной службы охраны Российской Федерации

Последние годы отмечаются значительным увеличением доли электронного документооборота в различных сферах информационного взаимодействия. Электронные документы являются неотъемлемой частью работы многих организаций, упрощая процессы обмена информацией и управления данными. При этом с ростом использования электронных документов, наблюдается увеличение количества нарушений информационной безопасности, связанных с внедрением вредоносного программного обеспечения. Наиболее распространенным типом данных, содержащим вредоносное программное обеспечение, является формат PDF. Из-за популярности данного формата отмечается значительный рост нарушений информационной безопасности. Для снижения числа инцидентов нарушений информационной безопасности при работе с PDF-документами необходимо разрабатывать новые или совершенствовать существующие средства обнаружения вредоносного кода. В качестве предлагаемого подхода к обнаружению может выступать подход, основанный на динамическом анализе средств просмотра PDF документов. В работе представлено описание подхода к обнаружению вредоносного программного обеспечения посредством анализа покрытия кода просмотрщика PDF документов.

обнаружение вредоносного программного обеспечения, фаззинг-тестирование

Существующие средства обнаружения вредоносного программного обеспечения в формате PDF сталкиваются с рядом недостатков, что подтверждается как статистическими данными, так и результатами исследований. Эти недостатки делают многие PDF-просмотрщики уязвимыми для различных видов атак, включая возможность удаленного выполнения кода, возможность раскрытия конфиденциальной информации и возможность манипуляции данными. Исследования, проведенные компанией "Positive Technologies" [1] (рис. 1), показывают, что в 2023 году злоумышленники при реализации успешных атак на организации активно использовали различные методы социальной инженерии. Наиболее часто злоумышленники прибегали к использованию электронных писем для реализации злонамеренных воздействий (89%). В представленном исследовании отмечается, что для обхода средств защиты систем электронной почты (документооборота) киберпреступники все чаще используют вложения в файлы формата PDF (Portable

Document Format). Указанный факт подчеркивает необходимость совершенствования средств обнаружения и защиты от подобных угроз, вызванных внедрением и использованием вредоносного программного обеспечения в легитимных типах данных.

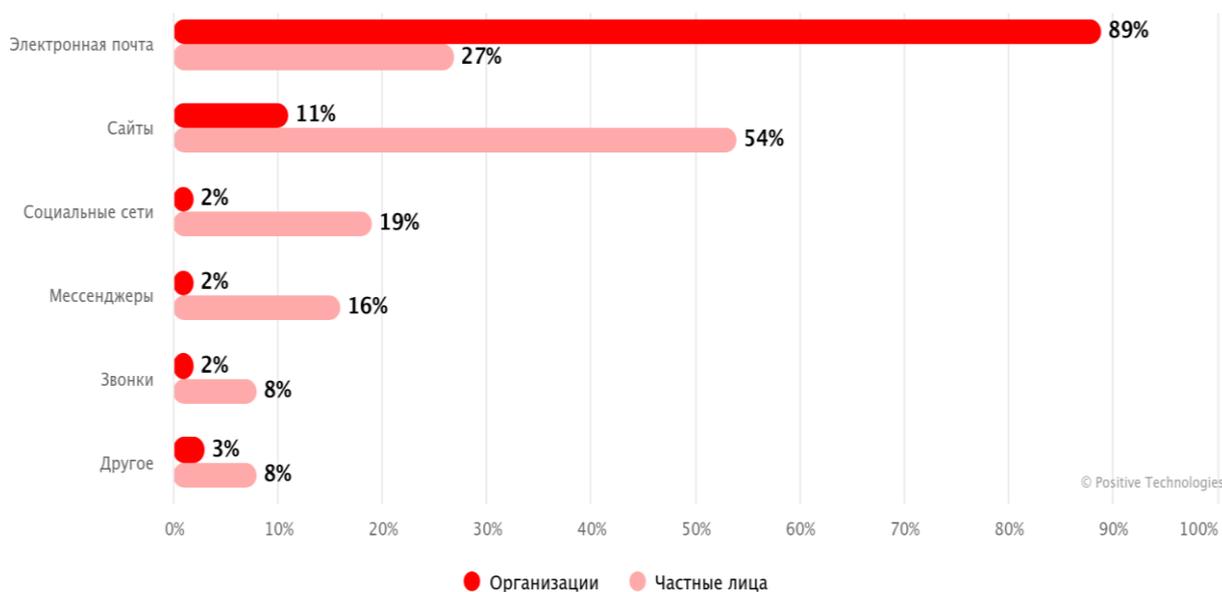


Рис. 1. Используемые злоумышленниками каналы социальной инженерии

Исследователи компании "Vipre" отмечают, что использование вредоносных PDF-файлов увеличилось в пять раз с начала года. Согласно отчету "Netskope", в течение третьего квартала, PDF-вложения занимали лидирующее положение среди всех форматов для распространения вредоносного программного обеспечения. Одним из популярных способов "заражения" PDF-файла являлось внедрение вредоносной ссылки.

В настоящее время существует два основных типа средств обнаружения вредоносного программного обеспечения: статические и динамические. Статические методы не способны обнаруживать новые угрозы, так как они ориентированы на известные сигнатуры вредоносных программ. С другой стороны, динамические методы обладают низкой вероятностью обнаружения, что связано с их ограниченной способностью к поиску неизвестных угроз. Следовательно, для повышения эффективности защиты от новых и неизвестных угроз необходимо совершенствовать динамический метод обнаружения вредоносного программного обеспечения.

В данной работе представлен инновационный подход к обнаружению вредоносного программного обеспечения в формате PDF, основанный на динамическом анализе покрытия кода просмотрщика PDF-файлов. На первом этапе разработанного подхода к обнаружению вредоносного программного обеспечения, встроенного в PDF файл, осуществляется разработка программного стенда, включающего установку и настройку средства эмуляции для имитации работы просмотрщика PDF в защищенной среде.

В качестве средства эмуляции могут быть использованы: виртуальная машина, контейнер или изолированная программная среда типа песочница (SandBox). Виртуальная машина [2] – виртуальная платформа, объединяющая виртуальные ресурсы для обработки, хранения и передачи информации, а также возможно содержащая аппаратное обеспечение и данные пользователей. Контейнер [3] представляет собой легкую форму виртуализации на уровне операционной системы, которая использует общий ядро системы хоста. В отличие от виртуальных машин, которые виртуализируют аппаратное обеспечение, контейнеры используют обобщенное пространство пользователя. Средства представляют собой стандартные программные модули, которые упаковывают код и все зависимости для быстрого и надежного запуска приложений в различных средах. Они не сохраняются, а разворачиваются из образов. Sandbox – это изолированная среда, созданная для запуска программ с целью обнаружения и предотвращения ошибок или уязвимостей их распространения. Путем эмуляции рабочей среды с использованием отдельного набора ресурсов, обеспечивает защиту критически важных систем сети, позволяя запускать подозрительные программы или код для анализа. Позволяет нейтрализовать (исключить) обнаружения программным обеспечением факта ее запуска в эмуляторе.

На втором этапе работы осуществляется конфигурирование средства осуществления фаззинг-тестирования. В качестве используемого средства фаззинг-тестирования выступает "AFL++". "AFL++" [4] представляет собой фаззер ориентированный на анализ покрытия, что означает, что он собирает информацию о покрытии для каждого измененного входа с целью обнаружения новых путей выполнения и потенциальных ошибок. Основной целью является выявление падений, зависаний, нарушений логики и проверок в коде приложения, а также утечек памяти, вызванных такими данными на входе. При наличии доступа к исходному коду, AFL может использовать инструментарий, вставляя вызовы функций в начало каждого базового блока (функции, циклы и т. д.).

На третьем этапе осуществляется загрузка исходного кода просмотрщика PDF в виртуальную машину и производится компиляция бинарного файла просмотрщика PDF с внедрением санитайзеров, которые осуществляют выявление различных типов ошибок, такие как утечки памяти, переполнения буфера и другие проблемы, позволяющие привести к уязвимостям и нестабильной работе программ. В качестве используемых санитайзеров могут выступать [5–8]:

1) AddressSanitizer (ASan) – предназначен для выявления ошибок чтения или записи в память, таких как переполнение буфера или использование освобожденной памяти (предоставляет подробную информацию об ошибках и помогает в процессе их отладки).

2) MemorySanitizer (MSan) – обеспечивает выявление участков неинициализированной памяти (обнаруживает ошибки, связанные с использованием неинициализированных данных, которые могут привести к непредсказуемому поведению программы).

3) UndefinedBehaviorSanitizer (UBSan) – выявляет неопределенное поведение в программе, такое как деление на ноль, переполнение целочисленных типов или некорректное использование указателей (предупреждает о наличии возможных ошибок указанного класса).

На четвертом этапе осуществляется построение кода покрытия просмотрщика PDF файлов посредством запуска на анализ AFL++ скомпилированного исполняемого файла просмотрщика PDF файлов, запущенного с PDF файлами, не содержащими вредоносный код ("чистые" PDF файлы), и со встроенным вредоносным программным обеспечением ("зараженные" PDF файлы). Из полученных значений покрытия кода просмотрщика PDF файлов формируются базы данных для "чистых" и "зараженных" PDF файлов. Полученные наборы данных являются входными наборами данных для средств машинного обучения, позволяющим осуществлять классификацию данных на основе проведенного обучения (алгоритмы классификации) или формировать функцию преобразования в зависимости от анализируемых пар "входные-выходные" данные (алгоритмы регрессии).

На пятом этапе из полученных наборов данных осуществляется обучение используемого алгоритма регрессии методов машинного обучения для формирования функции преобразования и получения разделяющего правила (порогового значения) разделяющего анализируемые покрытия кодов просмотрщика PDF для "чистых" и "зараженных" PDF файлов. Полученное пороговое значение представляет собой правило принятия, которое используется в процессе анализа новых PDF файлов на предмет обнаружения наличия (отсутствия) встроенного вредоносного программного обеспечения (вредоносного кода).

Разработанный подход позволяет применить методы фаззинг-тестирования в процессе динамического анализа и обнаружения встроенных в PDF документы вредоносных вложений. При этом практическая реализация предложенного подхода к вредоносного программного обеспечения является направлением дальнейших исследований, которая позволит количественно оценить точность обнаружения вредоносных вложений.

Список используемых источников

1. <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3>
2. ГОСТ Р 59163-2020 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Руководство по обеспечению безопасности при внедрении серверов виртуализации.
3. <https://www.oracle.com/cis/cloud/cloud-native/container-registry/what-is-docker>
4. <https://habr.com/ru/articles/772156>

5. Zalewski M. AFL Documentation. Release 2.53b, 2019. 95 p.
6. The LibAFL Fuzzing Library. URL: <https://aflplus.plus/libafl-book>
7. Саттон М. Fuzzing: исследование уязвимостей методом грубой силы / Майкл Саттон, Адам Грин, Педрам Амине. Пер с англ. СПб.: Символ-Плюс, 2009. 560 с.
8. Бегаев А. Н., Кашин С. В., Маркевич Н. А., Марченко А. А. Выявление уязвимостей и недеklarированных возможностей в программном обеспечении. СПб.: Университет ИТМО, 2020. 38 с.

УДК 654.739
ГРНТИ 49.33.29

ПРОБЛЕМЫ ЭТИКИ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Е. В. Копытова, В. К. Мавричев, Д. В. Петров, Ф. В. Филиппов

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

Развитие и применение искусственного интеллекта несет с собой множество этических вопросов, которые требуют внимания и обсуждения. Одной из таких проблем является использование автономных систем с принятием решений. Насколько мы можем доверять искусственному интеллекту в принятии решений? Какие из этих решений могут иметь фатальные последствия для людей или общества в целом? Как избежать участи вселенной Джеймса Кэмерона? Правила, этические принципы и ограничения, только так можно обеспечить безопасность и надежность таких систем. В статье будут рассмотрены вопросы, связанные с развитием и применением искусственного интеллекта, включая автономные системы с принятием решений, безопасность данных и приватность, а также неравенство и возможные социальные последствия.

искусственный интеллект, этические принципы, этическое регулирование искусственного интеллекта, авторские права, лицензионное соглашение

В третьем десятилетии XXI века искусственный интеллект (ИИ) – целое ответвление IT, специалисты которого разрабатывают системы анализа и обработки информации, для решения задач, подобно тому, как это сделал бы человек.

Алгоритмы, которые применяет ИИ, обрабатывают большие объемы данных и находят в них закономерности. Основываясь на этих закономерностях, ИИ может делать выводы, предсказывать события и принимать решения.

На данный момент существуют следующие принципы ИИ, такие как большой объем данных для обучения и обработки, вычислительная мощность, коммуникация на естественном языке, этические принципы и другие [4]. Без регулировки на основе принципов ИИ возможны проблемы "предвзятости" информационных систем. Например, разработчик может настроить рекомендательную систему на базе ИИ таким образом, чтобы в первую очередь предлагать товары определенного производителя. Такой подход создает неравные условия для всех участников рынка и может привести к негативной конкуренции и риску для бизнеса. Еще один пример - система распознавания лиц, которая может классифицировать людей определенной национальности как потенциальных правонарушителей.

В последние несколько лет десятки стран активно развивают искусственный интеллект. К ноябрю 2019 года было принято 34 национальные стратегии по ИИ, а до 2030 года разработана обновленная Национальная стратегия развития ИИ [1]. Будущее предполагает увеличение использования ИИ в разных сферах, поэтому важно оперативно установить этические рамки для развития искусственного интеллекта, ограничивая его неэтичное применение и обеспечивая безопасность и выгоду для общества.

Как минимум для исключения нечестной конкуренции, важно разработать лицензионные соглашения, которые учитывают специфические особенности генеративных моделей, включая их способность к созданию уникального контента. Такие соглашения должны жёстко регламентировать, какие действия допустимы при использовании результатов работы этих моделей, а какие нет, чтобы предотвратить случаи недобросовестной конкуренции, в том числе плагиат и несогласованное с автором копирование, например:

– Лицензия с Ограничением на Использование. Исследовательская организация разрабатывает генеративную модель для создания уникального контента. При публикации модели они устанавливают лицензионные условия, запрещающие использование модели для создания конкурирующего контента или коммерческого использования без предварительного согласия. Это помогает предотвратить нечестное соперничество и сохранить уникальность разработанного контента.

– Открытая Лицензия с Условиями. Исследователь создает генеративную модель для генерации изображений. Он решает опубликовать модель с открытой лицензией, позволяя другим исследователям использовать ее в своих проектах. Однако лицензионное соглашение требует указания на авторство при использовании модели и отказ от коммерческого использования без дополнительного соглашения. Это способствует распространению и использованию модели, при этом сохраняя уважение к авторским правам и исключая нечестное использование.

Для обеспечения эффективного лицензирования генеративных моделей необходимо также создание механизмов контроля за их использованием. Это может включать в себя системы мониторинга и обнаружения несанкционированного использования.

Очень важным является вопрос этичного использования данных для обучения ИИ. В развитии искусственного интеллекта большое значение имеет доступ к качественным «обучающим» данным. Вместе с тем, вопросы этики возникают при использовании данных из открытых (и условно открытых источников) и уважении авторских прав. Так в 2023 году актриса озвучки подала иск к банку «Тинькофф», когда обнаружила, что её голос, записанный несколько лет назад для обучения голосового помощника банка, был выложен в открытый доступ и стал использоваться третьими лицами для озвучки порнографических роликов [2].

По данным deermedia.ai, количество deepfake видео в 2023 году выросло по сравнению с аналогичным периодом прошлого года в три раза, аудио – в восемь. Такие артефакты часто приводят к резонансу, скандалам и судам, при том как с медийными личностями [3], так и с людьми, имеющими меньше финансовых и юридических возможностей.

Необходимо стремиться к тому, чтобы использование данных из открытых источников происходило с согласия и с уважением к их авторам. Это может включать в себя соблюдение лицензионных условий, указание на источник данных и признание труда исследователей, создавших их.

Борьба с нарушениями авторских прав и недобросовестным использованием данных требует внимания со стороны как исследователей, так и общества в целом. Организации и учреждения, занимающиеся исследованиями в области искусственного интеллекта, должны разрабатывать и соблюдать строгие этические стандарты и механизмы, которые обеспечат соблюдение авторских прав и защиту интеллектуальной собственности. Наиболее правильным представляется модель, допускающая использование только тех данных, на которые их авторы дали «прямое разрешение».

Предложенные методы лицензирования результатов и доступа к данным сделают использование и разработку ИИ корректными не только с юридической точки зрения, но и в значительной степени закроет этическую сторону вопроса. С другой стороны, очевидно, что такой подход существенно снизит темпы развития генеративных моделей и ИИ в целом, а также потребует усилий как от разработчиков и исследователей, так и от авторов и используемых ими платформ.

Список используемых источников

1. Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом».

2. DTF: актриса озвучки подала в суд на «Тинькофф» за использование её голоса в других проектах без разрешения // Хабр. URL: <https://habr.com/ru/news/758172> (дата обращения 03.02.2024)

3. Taylor Swift deepfakes spread online, sparking outrage // CBS. News. URL: <https://www.cbsnews.com/news/taylor-swift-deepfakes-online-outrage-artificial-intelligence> (дата обращения 03.02.2024).

4. Карпов В. Э., Готовцев П. М., Ройзензон Г. В. К вопросу об этике и системах искусственного интеллекта // Философия и общество. 2018. № 2(87). URL: <https://cyberleninka.ru/article/n/k-voprosu-ob-etike-i-sistemah-iskusstvennogo-intellekta> (дата обращения 03.02.2024)

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТЕЙ СУДОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е. В. Коровкина, В. Л. Литвинов

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

Приведена оценка и анализ основных специфических для кораблей технологий, на которые совершаются кибератаки. Судходство является неотъемлемой частью современной жизни, но без тонко настроенной аппаратуры движение судна может привести к трагедии, поэтому очень важно фиксировать любые угрозы информационной безопасности, научиться находить их и предотвращать. Рассмотрены основные судовые системы, которые могут быть уязвимы: Системы навигационного мостика; Грузовые системы; Системы движения и энергетического менеджмента; Системы управления доступом на судно; Системы обслуживания пассажиров; Сети общего пользования; Системы социального обеспечения экипажа; Системы радиосвязи и коммуникации.

кибербезопасность, морской транспорт, кибератаки, безопасность судов, технические средства защиты

В условиях все возрастающей цифровизации морского транспорта и роста киберугроз, обеспечение кибербезопасности становится вопросом первостепенной важности для компаний и государств, занимающихся морской деятельностью. Отрасль сталкивается с угрозами, включая кибератаки на суда, которые могут привести к серьезным последствиям, включая финансовые потери, угрозы для безопасности экипажей и загрязнение окружающей среды.

Недавний опрос в отрасли морского транспорта за 2022 год выявил тревожные тенденции в области кибербезопасности. Согласно данным исследования, 44% специалистов сообщили о кибератаках на свои организации за последние три года, а 3% из них вынуждены были заплатить выкуп, средний размер которого составил около \$3 млн [1]. Эти цифры подчеркивают нарастающую угрозу, с которой сталкиваются компании в сфере морского транспорта. Исследование также показало, что существенная часть организаций не проводит регулярное обучение по кибербезопасности (32%) и не имеет плана реагирования на кибератаки (38%) [1]. Это означает, что многие компании остаются уязвимыми перед угрозами виртуального мира.

Примеры успешных кибератак на суда подтверждают серьезность проблемы. Например, в 2017 году кибератака на компанию Maersk принесла убытки около \$250-300 млн. Вирус-шифровальщик NotPetya заразил 17 из 76 грузовых терминалов компании Maersk, приведя к значительному финансовому ущербу [2]. Недавние события также подчеркивают актуальность вопроса кибербезопасности в морском транспорте. Например, в феврале 2024 года США совершили кибератаку на иранский корабль, который, как утверждается, собирал разведданные о судах в Красном море. Это свидетельствует о том, что государства активно используют кибервооружение в геополитических целях, что увеличивает сложность управления кибербезопасностью в морской отрасли.

Существуют международные организации, такие как Международная морская организация (ИМО) и Международный морской комитет (МСС), которые играют ключевую роль в разработке стандартов и рекомендаций по кибербезопасности в морской отрасли. Например, в январе 2021 года вступили в силу обновленные глобальные требования по кибербезопасности в морском судоходстве, в соответствии с которыми киберриски должны быть учтены в системах управления безопасностью судов.

Реализация этих требований помогает снизить риск кибератак и минимизировать потенциальные убытки [1]. Тем не менее, для эффективной защиты от киберугроз требуется не только соответствие стандартам, но и постоянное обучение персонала, разработка стратегии реагирования на инциденты и инвестиции в современные технологии кибербезопасности.

В целом, обеспечение кибербезопасности в морском транспорте остается одним из наиболее важных вызовов для отрасли, требующим совместных усилий компаний, правительств и международных организаций. Только путем совместных действий можно обеспечить безопасность и надежность морской торговли в условиях все возрастающих киберугроз. Для обеспечения безопасности и предотвращения киберугроз в морской отрасли также необходимо активное внедрение и соблюдение стандартов Международного кодекса по управлению безопасной эксплуатацией судов и предотвращению загрязнения (МКУБ). Документ о соответствии, выдаваемый судну,

подтверждает соблюдение всех правил МКУБ и имеет срок действия до пяти лет. Важным аспектом обеспечения кибербезопасности является проверка судов морскими администрациями различных стран при заходе в порты на предмет выполнения рекомендаций Международной морской организации (ИМО) по кибербезопасности. Это позволяет контролировать и оценивать уровень защиты судов от потенциальных кибератак.

Следует также отметить, что в свете новых рекомендаций ИМО по кибербезопасности, киберинциденты, связанные с обменом данными между судном и портом, будут теперь рассматриваться в новом контексте. Это подчеркивает важность постоянного обновления и совершенствования подходов к кибербезопасности в морской отрасли. Реальные последствия кибератак на суда могут быть катастрофическими. Возможность изменения данных о пароходе, ложная информация о шторме, изменение параметров судна и другие атаки представляют серьезную угрозу как для безопасности судна, так и для окружающей среды и человеческой жизни [3]. Поэтому необходимость эффективной защиты от киберугроз в морском транспорте остается важной задачей для всей отрасли. В таблице 1 представлена актуальная информация о киберугрозах в области морского транспорта.

ТАБЛИЦА 1. Угрозы кибербезопасности в морском транспорте

Тип угрозы	Уязвимая судовая система	Описание
Модификация данных	Системы навигационного мостика, системы радиосвязи и коммуникации	Эта угроза заключается в изменении информации о судне, включая его местоположение и груз.
Ложные предупреждения	Системы движения и энергетического менеджмента, системы радиосвязи и коммуникации	Включает в себя отправку ложных сообщений о погодных условиях, столкновениях и других аварийных ситуациях.
Вымогательство	Любая система	Включает в себя захват и блокировку доступа к данным или системам с целью вымогательства.
Фальсификация документации и сертификатов	Система хранения и обработки информации (чаще всего портовые)	Эта угроза заключается в создании поддельных документов для обмана органов контроля и управления
Проникновение в системы управления судном	Системы управления доступом на судно	Эта угроза представляет собой несанкционированный доступ к компьютерным системам судов для их контроля и манипулирования.

Тип угрозы	Уязвимая судовая система	Описание
Внедрение вредоносного ПО	Сети общего пользования, системы управления доступом на судно, системы обеспечения экипажа и пассажиров	Включает загрузку и запуск вредоносных программ на компьютерах и сетевых устройствах, что может привести к компрометации систем безопасности и нарушению нормальной работы.
Атаки на сетевую инфраструктуру	Системы радиосвязи и коммуникации	Представляет собой попытки взлома и нарушения работы сетевых систем и коммуникаций, что может привести к утечке конфиденциальной информации.

Анализ киберугроз показал, что судовые системы подвержены различным угрозам кибербезопасности. Для безопасности судов каждый тип угрозы имеет свои характеристики и потенциальные последствия. Например, к опасным изменениям в навигационной информации может привести модификация данных, а это, в свою очередь, может привести к авариям и потере контроля над судном.

Ложные предупреждения, очевидно, могут вызвать панику среди экипажа и пассажиров и отвлечь внимание от реальных аварийных ситуаций. Взлом систем управления судном может дать злоумышленникам полный контроль над ним. Фальсификация документации и сертификатов может привести к ошибкам в процессе управления судном и взаимодействию с регулирующими органами. Внедрение вредоносного ПО и атаки на сетевую инфраструктуру могут привести к нарушению работы судовых систем и утечке конфиденциальной информации. Таким образом, эффективная защита судовых систем от киберугроз требует комплексного подхода, включающего технические, организационные и правовые меры безопасности.

С учетом международных стандартов и нормативных документов, морские компании и администрации должны активно работать над повышением уровня защиты информационных систем на судах. В настоящее время, обучение экипажа, регулярные аудиты безопасности, а также строгие политики безопасности становятся ключевыми элементами для предотвращения потенциальных киберинцидентов и обеспечения безопасности морских операций.

Список используемых источников

1. Международная морская организация. URL: [http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL/4117-Tableofcontents\(Secretariat\).pdf](http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL/4117-Tableofcontents(Secretariat).pdf) (дата обращения 15.06.2023)

2. Морская отрасль уязвима для атак хакеров // Вести Экономика. URL: <https://www.vestifinance.ru/articles/42174> (дата обращения 15.06.2023)

3. Банк данных угроз безопасности информации // ФСТЭК России. URL: <https://bdu.fstec.ru> (дата обращения 15.06.2023)

УДК 004.65
ГРНТИ 50.41.21

ИССЛЕДОВАНИЕ ВЛИЯНИЯ РАЗМЕРА СЕГМЕНТА ЖУРНАЛА ПРЕДЗАПИСИ НА ПРОИЗВОДИТЕЛЬНОСТЬ БАЗЫ ДАННЫХ В СУБД POSTGRESQL

А. А. Косенкова, С. А. Нестеров

Санкт-Петербургский политехнический университет Петра Великого

В статье рассматривается влияние размера сегмента журнала предзаписи (параметр `wal_segment_size`) на производительность базы данных в PostgreSQL. Журнал предзаписи играет важную роль в обеспечении согласованности данных при сбое сервера. На диске журнал хранится в виде последовательности файлов, также называемых сегментами. Грамотная настройка параметров журнала позволяет повысить производительность базы данных (количество транзакций, обрабатываемых за единицу времени).

базы данных, СУБД PostgreSQL, журнал предзаписи

Журнал предзаписи (англ. Write-Ahead Log, WAL) играет ключевую роль в восстановлении согласованности данных после сбоя. В PostgreSQL WAL хранит историю изменений данных в виде журнальных записей, которые должны быть сохранены на диске до того, как на него будут записаны сами измененные страницы данных [1]. Выполняемые транзакциями изменения страниц данных осуществляются в буферном кэше в общей памяти (в ОЗУ). Синхронизация кэша с основным хранилищем происходит в отложенном режиме благодаря механизму контрольных точек, который переносит данные на диск в процессе фоновой записи.

В случае сбоя сервера, такого как отказ электропитания, содержимое оперативной памяти теряется. Система управления базами данных (СУБД) при следующем запуске использует WAL для воспроизведения изменений и достижения последнего согласованного состояния.

Журнал предзаписи представляет собой набор файлов, также называемых сегментами, внутри подкаталога `pg_wal` в основном каталоге данных. Каждый сегмент журнала имеет фиксированный размер, который можно переопределить только при инициализации кластера базы данных (БД). По умолчанию размер сегмента составляет 16 Мб [2, 3].

В PostgreSQL переключение на новый сегмент журнала происходит при наступлении одного из следующих событий:

- заполнение сегмента журнала;
- выполнение функции `pg_switch_wal`;

- истечение времени, установленного в `archive_timeout`, при активном параметре `archive_mode`.

Объем WAL ограничен параметрами конфигурации и при нормальной эксплуатации количество сегментов находится в определённом диапазоне, который зависит от параметров минимального и максимального размера WAL (`min_wal_size` и `max_wal_size`, соответственно). При высоких нагрузках, особенно связанных с изменением данных, могут создаваться дополнительные сегменты, вследствие чего размер журнала может увеличиваться.

Важно отметить, что влияние на производительность БД также оказывает настройка выполнения контрольных точек. Контрольные точки подразумевают сохранение изменённых в оперативной памяти страниц данных на диск, что может привести к значительной нагрузке на подсистему ввода-вывода при их частом выполнении.

Триггером контрольной точки в PostgreSQL является выполнение одного из условий:

- истечение максимального времени между автоматическими контрольными точками, за которое отвечает настройка параметра `checkpoint_timeout`;
- превышение максимального размера WAL при выполнении автоматических контрольных точек. Конкретное значение определяется параметром `max_wal_size`.

PostgreSQL позволяет управлять включенным по умолчанию логическим параметром `full_page_writes`, который отвечает за регистрацию всего содержимого страницы данных в WAL при первом изменении страницы после каждой контрольной точки. Данный параметр гарантирует корректное восстановление согласованности БД после сбоя, так как устраняет возможность появления на диске страниц, содержащих как старые, так и новые данные. В таком случае частое выполнение контрольных точек увеличивает объем входящих в WAL записей, что приводит к увеличению количества дисковых операций ввода-вывода и возможному снижению общей производительности.

Настройка параметров WAL, а также управление процессом выполнения контрольных точек, может оказать положительное влияние на производительность БД. Предполагается, что увеличение размера сегмента WAL, который определяется параметром `wal_segment_size`, позволит повысить производительность БД за счёт снижения накладных расходов на создание нового сегмента журнала, переключение на него и удаление или переработку старых сегментов.

Для исследования влияния размера сегмента WAL на работу СУБД PostgreSQL были проведены две серии экспериментов, в которых создавалась одинаковая нагрузка на БД при разных значениях размера сегмента журнала. Сначала были инициализированы кластеры с параметрами по

умолчанию – `checkpoint_timeout = 5` мин., `max_wal_size = 1` Гб. Во второй серии экспериментов влияние контрольной точки было минимизировано за счёт увеличения значений параметров кластера: параметр `checkpoint_timeout` был переопределён до 2 часов, параметр `max_wal_size` – до 50 Гб. Перед проведением каждого эксперимента контрольная точка была записана принудительно.

При проведении экспериментов была использована виртуальная машина с операционной системой Ubuntu 22.04 с выделенными 8 Гб оперативной памяти и 8 ядрами процессора. Использовалась СУБД PostgreSQL 16.1 и утилита `pgbench`. Данная утилита позволяет создавать тестовую БД и нагрузку на нее, согласно сценарию, основанному на одном из эталонных тестов производительности БД – TPC-B. Каждая выполняемая транзакция включает в себя команды `SELECT`, `INSERT` и три команды `UPDATE`. Производительность или пропускная способность определяется как число зафиксированных транзакций в секунду (`transactions per second, tps`).

В ходе экспериментов были последовательно инициализированы кластеры с размерами сегмента WAL начиная с 1 Мб до 1024 Мб с увеличением размера в два раза на каждом шаге. Нагрузка на сервер БД составляла 1 000 000 транзакций при одном активном подключении.

В экспериментах с параметрами кластера БД по умолчанию, каждый тест был проведён 12 раз. Результаты представлены в табл. 1 и на рис. 1, в них приведено среднее значение пропускной способности БД (`tps`).

В экспериментах, где влияние контрольной точки было минимизировано, каждый тест был проведён 4 раза. Результаты представлены в табл. 2 и на рис. 2, где указано среднее значение пропускной способности БД (`tps`).

ТАБЛИЦА 1. Значения пропускной способности базы данных при различных размерах сегмента WAL, полученные в результате серии экспериментов с параметрами кластера, установленными по умолчанию

Размер сегмента WAL (<code>wal_segment_size</code>), Мб	Количество транзакций в секунду (<code>tps</code>)
1	774,30
2	777,98
4	740,00
8	805,72
16	830,07
32	830,33
64	817,73
128	799,38
256	781,91
512	837,52
1024	861,36

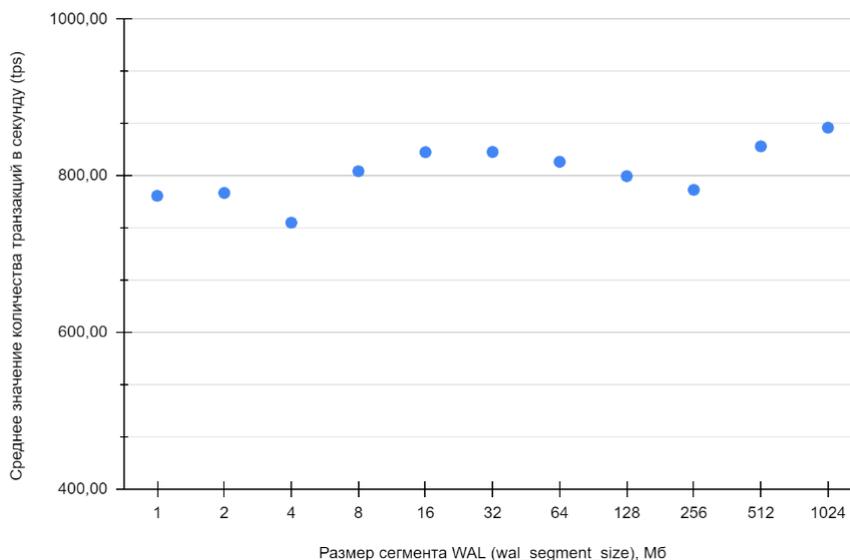


Рис. 1. Зависимость пропускной способности базы данных от размера сегмента WAL при параметрах кластера по умолчанию.

ТАБЛИЦА 2. Значения пропускной способности базы данных при различных размерах сегмента WAL, полученные в результате серии экспериментов, где влияние контрольной точки было минимизировано

Размер сегмента WAL (wal_segment_size), Мб	Количество транзакций в секунду (tps)
1	713,36
2	641,45
4	631,27
8	728,35
16	816,86
32	842,19
64	838,35
128	823,49
256	833,79
512	830,46
1024	829,44

По результатам экспериментов можно говорить о наличии зависимости пропускной способности БД от размера сегмента WAL.

В первой серии экспериментов наилучшую производительность продемонстрировал кластер с размером сегмента 1 Гб (рис. 1). При этом можно говорить о том, что выбор 16 Мб в качестве значения по умолчанию обоснован, так как в этом случае также достигается достаточно высокая производительность. Наблюдается снижение производительности для размеров сегмента 4 Мб и 256 Мб, связанное, предположительно, с возможным наличием параллельных процессов, проходящих в операционной системе виртуальной или локальной машины.

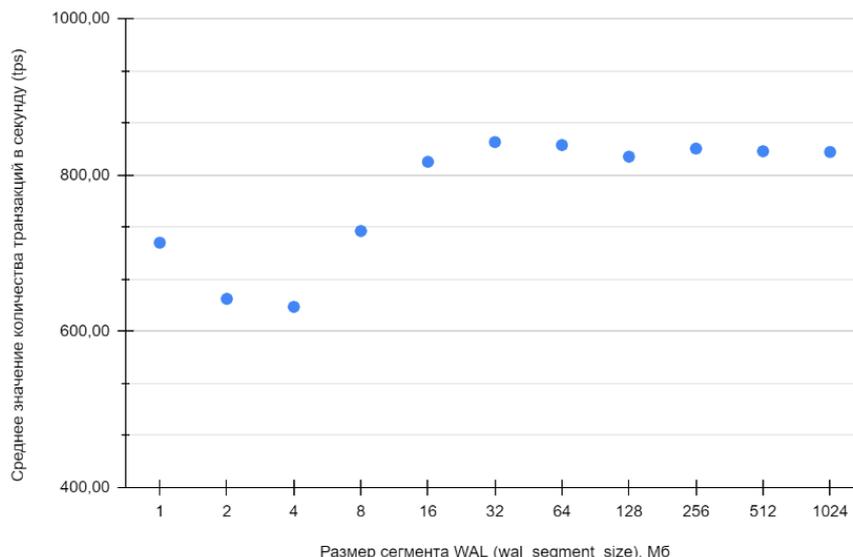


Рис. 2. Зависимость пропускной способности базы данных от размера сегмента WAL при параметрах кластера, минимизирующих вероятность записи контрольной точки

Во второй серии экспериментов, где влияние контрольной точки было минимизировано, для небольших размеров сегмента (1 и 2 Мб) показатель производительности выше, чем для 4 Мб. Предположительно, это связано с кешированием (на уровне ОС или оборудования), увеличивающим скорость работы с небольшими файлами, и не оказывающим влияния для кластеров с большими файлами. Далее, после 4 Мб, с ростом размера сегмента WAL растёт и производительность БД. Более высокую производительность, в сравнении с кластером с размером сегмента 16 Мб, продемонстрировали кластеры с размерами 32, 64, 128 Мб и далее.

В дальнейшем планируется выполнение экспериментов при нескольких одновременных подключениях к БД, в рамках которых отправляются запросы. На основе полученных результатов могут быть выработаны рекомендации по «тонкой настройке» серверов БД PostgreSQL.

Список используемых источников

1. Новиков Б. А., Горшкова Е. А., Графеева Н. Г. Основы технологий баз данных: учебное пособие / под ред. Е. В. Рогова. 2-е изд. М.: ДМК Пресс, 2020. 582 с.
2. Лесовский А. В. Мониторинг PostgreSQL. М.: Бумба, 2024. 247 с.
3. Рогов Е. В. PostgreSQL 15 изнутри. М.: ДМК Пресс, 2023. 662 с.

УДК 004.62
ГРНТИ 50.53

ВИЗУАЛИЗАЦИЯ ДАННЫХ НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ R

П. В. Косов, Р. Я. Лабковская

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

Визуализация данных – это чрезвычайно ценный навык, а также мощный инструмент для изучения закономерностей, тенденций и взаимосвязей в наборах данных. Визуализация является ключевым этапом в использовании открытых данных, поскольку она позволяет лучше понять проблемную область, извлечь и передать базовые знания из данных, а также определить направление будущего анализа с использованием более сложных методов. Для создания объективных, наглядных и понятных графиков визуализации данных необходимо учитывать определенные основные принципы, так как этот процесс может быть сложным. Данная статья посвящена рассмотрению ключевых принципов визуализации данных на языке программирования R.

визуализация данных, анализ данных, ChatGPT, открытые данные, R

Визуализация данных играет важную роль в нашей исследовательской деятельности. Чаще всего используются столбчатые и линейные диаграммы, которые применяются в презентациях и отчетах. Затем эти данные могут быть использованы в будущих исследованиях, особенно при написании статей. Поэтому умение создавать хорошие визуализации необходимо для карьеры всех ученых и исследователей. Визуализации помогут сделать данные более убедительными, а презентации – более влиятельными. Знание методов создания эффективных визуализации – полезный навык, который можно применить в самых разных областях.

R – это свободная программная среда и интерпретируемый язык программирования. Другими словами, R выполняет инструкции напрямую, без компиляции программы в инструкции машинного языка. В отличие от других программ для анализа данных, термин «среда» в R относится к полностью спланированной и согласованной системе, а не к конкретному и негибкому набору инструментов. R часто используется для статистических и графических вычислений, поскольку предоставляет широкий спектр статистических методов, включая линейные и нелинейные модели, классические статистические тесты, анализ временных рядов, классификацию, кластеризацию и т.д. [1]. Кроме того, R обладает возможностями построения графиков. R работает на различных платформах, включая UNIX-подобные системы (такие как FreeBSD и Linux), Windows и MacOS.

Основные методы визуализации данных в R

– Статические графики с помощью ggplot2 [2]. Библиотека ggplot2 является одной из наиболее популярных и мощных библиотек для создания статических графиков в R. Она предоставляет удобный и интуитивно понятный синтаксис для создания различных типов графиков, включая диаграммы рассеяния, гистограммы, ящики с усами и многое другое.

– Интерактивные визуализации с помощью plotly. Библиотека plotly позволяет создавать интерактивные визуализации прямо в R. С её помощью можно создавать диаграммы, которые позволяют пользователю взаимодействовать с данными, приближать, выбирать и фильтровать информацию.

– Тематические карты с помощью ggmap. Пакет ggmap предоставляет возможность создания тематических карт на основе данных географического положения. С его помощью можно визуализировать данные на карте, отображая распределение значений по географическим областям.

– Трёхмерные визуализации с помощью rgl. Библиотека rgl позволяет создавать трёхмерные визуализации данных. Она подходит для визуализации трёхмерных данных, таких как облака точек или поверхностные графики.

Примеры визуализаций данных на R

– Линейные графики с ggplot2 [2]. Используя ggplot2, можно построить простые линейные графики, отображающие изменение значений переменной во времени или по другому параметру (рис. 1, рис. 2).

```
1 # Установка и загрузка библиотеки ggplot2
2 install.packages("ggplot2")
3 library(ggplot2)
4
5 # Создание примеров данных
6 data <- data.frame(
7   x = c(1, 2, 3, 4, 5), # значения по оси X
8   y1 = c(2, 3, 5, 7, 11), # значения для первой линии
9   y2 = c(1, 4, 3, 6, 9) # значения для второй линии
10 )
11
12 # Построение линейного графика с использованием ggplot2
13 ggplot(data, aes(x = x)) +
14   geom_line(aes(y = y1), color = "blue") + # добавление первой линии
15   geom_line(aes(y = y2), color = "red") + # добавление второй линии
16   labs(title = "Пример линейного графика", # заголовок графика
17         x = "Значения X", # подпись оси X
18         y = "Значения Y") # подпись оси Y
```

Рис. 1 Пример программного кода для построения линейного графика

Этот код создает пример данных с двумя переменными (x и y), после чего использует библиотеку `ggplot2` для построения линейного графика с двумя линиями разных цветов.

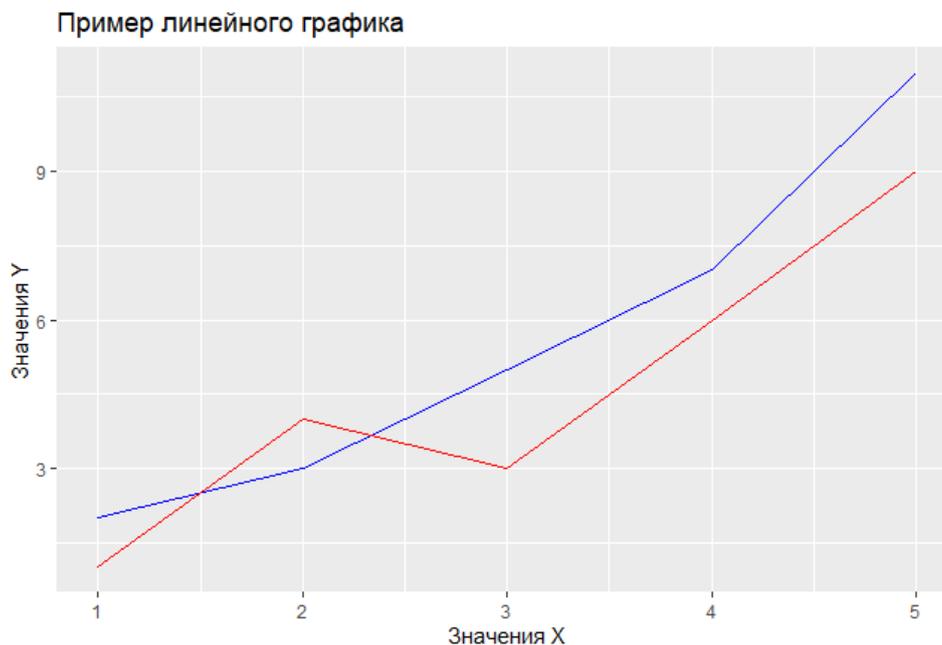


Рис 2. Пример линейного графика

– Интерактивная гистограмма с `plotly`. Создание интерактивной гистограммы с помощью `plotly` позволяет пользователю выбирать интересующие его интервалы значений и увеличивать детализацию данных (рис. 3, рис. 4).

```
1 # Установка и загрузка библиотеки plotly
2 install.packages("plotly")
3 library(plotly)
4
5 # Создание примера данных
6 data <- data.frame(
7   x = rnorm(1000) # Генерация случайных данных для гистограммы
8 )
9
10 # Построение интерактивной гистограммы с помощью plotly
11 plot_ly(data, x = ~x, type = "histogram") %>%
12   layout(title = "Интерактивная гистограмма", # Заголовок гистограммы
13          xaxis = list(title = "Значения X"), # Подпись оси X
14          yaxis = list(title = "Частота")) # Подпись оси Y
```

Рис 3. Программный код для создания интерактивной гистограммы

Этот код создает пример данных с помощью генерации случайных значений, затем использует функцию `plot_ly()` из библиотеки `plotly` для построения

ения интерактивной гистограммы. Каждый столбец на гистограмме представляет собой интервал значений переменной x , а высота столбца соответствует количеству значений в этом интервале.

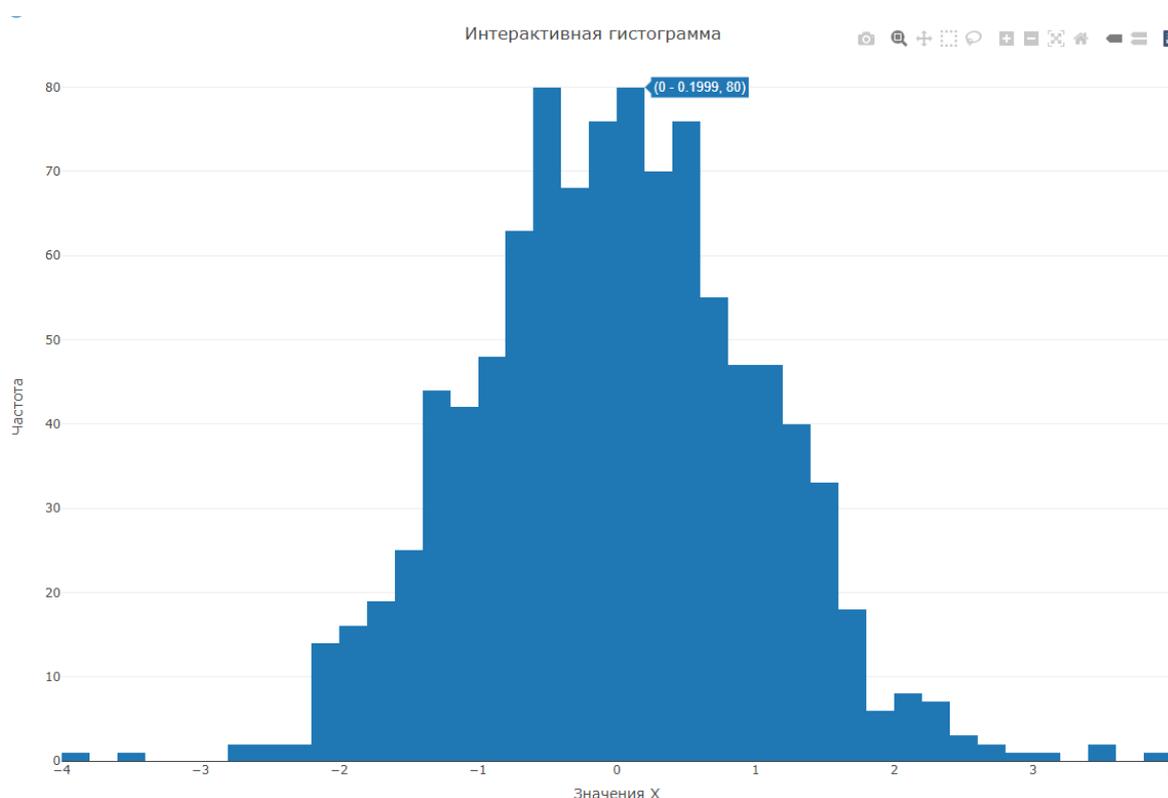


Рис. 4. Интерактивная гистограмма

– Трехмерный график с `rgl`. Создание трехмерного графика с помощью `rgl` позволяет исследовать данные в трех измерениях и лучше понять их структуру (рис. 5, рис. 6).

```
1 # Установка и загрузка пакета rgl
2 install.packages("rgl")
3 library(rgl)
4
5 # Создание трехмерного графика
6 plot3d(x = c(1, 2, 3, 4, 5), y = c(2, 3, 5, 7, 11), z = c(1, 4, 3, 6, 9),
7        type = "s", col = "blue", size = 3, # Задаем тип и параметры точек
8        xlab = "x", ylab = "y", zlab = "z", # Подписи осей
9        main = "Пример трехмерного графика с rgl") # Заголовок графика
```

Рис. 5 Программный код для создания трехмерного графика

Этот код создает трехмерный график с помощью функции `plot3d` из пакета `rgl`. В данном примере используются случайно выбранные точки для иллюстрации. Вы можете изменить координаты точек, их тип, цвет, размер, а также подписи осей и заголовок графика в соответствии с вашими потребностями.

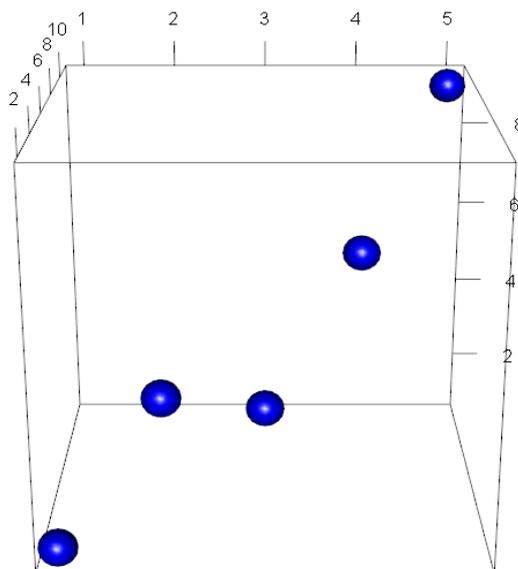


Рис. 6. Трехмерный график

Заключение

Визуализация данных на языке программирования R представляет собой мощный инструмент для исследования данных и выявления паттернов. С его помощью исследователи могут легко создавать разнообразные графики и диаграммы, которые помогают в понимании структуры данных и визуализации важной информации. Благодаря богатым возможностям и гибкости R, аналитики могут строить не только простые графики, но и сложные интерактивные визуализации. Язык программирования R предоставляет разнообразные возможности для представления данных и их визуального анализа, благодаря чему появилась возможность эффективно исследовать данные и делать обоснованные выводы на основе визуализации данных.

Список используемых источников

1. Brennan P. Data visualization with the programming language R // The Authors. Published by Portland Press Limited under the Creative Commons Attribution License 4.0 (CC BY-NC-ND). 2021. PP. 1–7. URL: https://www.researchgate.net/publication/354993237_Data_visualization_with_the_programming_language_R (дата обращения: 20.03.2024)
2. Keyes D. Using ChatGPT to Create Data Visualization with ggplot. 2022. URL: <https://rfortherestofus.com/2022/12/chatgpt-ggplot> (дата обращения: 20.03.2024)

УДК 004.62
ГРНТИ 50.53

ИСПОЛЬЗОВАНИЕ CHATGPT ДЛЯ АНАЛИЗА ДАННЫХ

П. В. Косов, Р. Я. Лабковская

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

Статья посвящена инновационному подходу к анализу данных на языке R с использованием чат-бота ChatGPT. В работе рассмотрены различные возможности ChatGPT, которые помогут оптимизировать процессы анализа данных, включая создание наборов данных, генерацию статистических сводок, построение визуализаций и написание интерактивных приложений Shiny. Особое внимание уделено взаимодействию с ChatGPT посредством запросов на языке R с целью автоматизации и улучшения процессов анализа данных.

анализ данных, чат-бот, ChatGPT, R, искусственный интеллект, визуализация данных

В современном мире, где объемы данных растут в геометрической прогрессии, эффективные методы анализа и взаимодействия с информацией становятся ключевыми для принятия обоснованных решений. В этом контексте возникает потребность в инновационных подходах, и одним из таких инструментов становится ChatGPT [1,2]. В данной статье мы рассмотрим применение ChatGPT в области анализа данных, его роль в оптимизации рабочих процессов, создании визуализаций, автоматизации кодирования на языке R и взаимодействии с различными аспектами аналитических задач [3].

Для начала, хотим обратить внимание на ряд преимуществ, которые представляет ChatGPT для анализа данных:

– обработка естественного языка (Natural Language Processing, NLP): ChatGPT может анализировать текстовые данные на естественном языке, что позволяет эффективно работать с различными источниками информации, включая текстовые документы, отчеты, новостные статьи и даже социальные медиа;

– автоматизация процессов [1, 2]: ChatGPT способен автоматически обрабатывать и анализировать большие объемы данных, что ускоряет процесс принятия решений и снижает нагрузку на аналитиков данных;

– понимание контекста [3]: благодаря своей способности понимать контекст и связи между различными элементами текста, ChatGPT может выявлять скрытые паттерны и тренды в данных, которые могут остаться незамеченными при традиционном анализе;

– генерация выводов: на основе анализа данных ChatGPT может генерировать выводы и рекомендации, помогая принимать обоснованные решения на основе данных.

В данной части статьи мы на практике продемонстрируем использование ChatGPT для анализа данных. Первое, с чего мы начнем – это напишем запрос в ChatGPT: «Напиши код на R, который создаст выборку данных, содержащую данные клиента». Всего создадим 3 запроса: через ChatGPT в мессенджере Telegram (рис. 1) и 2 запроса на официальном сайте ChatGPT <https://chat.openai.com/> (рис. 2, рис. 3).

На рис. 1–3 видно, что помимо сгенерированного кода ChatGPT предоставляет нам комментарии к каждой строчке кода. Чтобы проверить работоспособность полученных кодов, скопируем их в интегрированную среду разработки RStudio и убедимся, что он выполняется. Результаты проверки будут представлены на рис. 4–6.

```
R
# Создаем выборку данных
ID <- c(1, 2, 3, 4, 5) # ID клиента
Имя <- c("Анна", "Иван", "Мария", "Петр", "Елена") #
Имена клиента
Возраст <- c(25, 35, 30, 45, 28) # Возраст клиента
Город <- c("Москва", "Санкт-Петербург", "Киев",
"Нью-Йорк", "Лондон") # Город клиента

# Создаем dataframe (таблицу) с данными клиента
данные_клиента <- data.frame(ID, Имя, Возраст,
Город)

# Выводим выборку данных на экран
print(данные_клиента)
```

Рис. 1. Сгенерированный через ChatGPT датасет

Этот код создает датафрейм (таблицу) с данными клиента, включая ID клиента, имя, возраст и город проживания. Для создания выборки по конкретным клиентам можно изменить значения переменных ID, Имя, Возраст и Город.

Давайте по порядку запустим три кода и разберем результаты. Результаты проверки показали работоспособность сгенерированного кода.

Новое задание, которое получил ChatGPT выглядело так: с помощью пакета *shiny*, используя набор данных *gapminder* пакета *gapminder*, необходимо построить интерактивное веб-приложение, позволяющее строить график формата *ggplot*, по заданным настройкам. Приложение должно содержать минимум 3 конструкции типа *input*. Также необходимо оформить приложение соответствующим образом, т.е. необходимо, чтобы каждая из форм ввода входных данных имела соответствующую подпись, также, как и итоговый график, формируемый приложением.

Мы можем видеть, что код создает веб-приложение с тремя видами входных данных: выбор переменных для осей X и Y, и ползунок для выбора года. График будет обновляться в соответствии с выбранными настройками. Давайте запустим этот код в RStudio и посмотрим результат (рис. 8).

```
R Copy code  
  
# Создание выборки данных о клиентах  
set.seed(123) # Задаем seed для воспроизводимости результатов  
  
# Генерация данных  
customer_data <- data.frame(  
  customer_id = 1:100,  
  name = sample(c("John", "Jane", "Alex", "Emily", "Michael"), 100, rep  
age = sample(18:65, 100, replace = TRUE),  
  email = paste0("customer", 1:100, "@example.com"),  
  city = sample(c("New York", "Los Angeles", "Chicago", "San Francisco"  
)  
  
# Вывод первых нескольких строк данных  
head(customer_data)
```

Рис. 2. Сгенерированный через ChatGPT датасет

```
R Copy code  
  
# Установка и загрузка необходимых пакетов  
install.packages("dplyr")  
library(dplyr)  
  
# Создание исходных данных (предположим, у вас уже есть некоторые данные)  
set.seed(123) # для воспроизводимости случайных чисел  
n <- 100 # количество клиентов  
clients <- data.frame(  
  ID = 1:n,  
  Name = sample(c("Иван", "Мария", "Александр", "Екатерина", "Дмитрий"), n  
Country = sample(c("Россия", "США", "Германия", "Франция"), n, replace  
Age = sample(18:60, n, replace = TRUE)  
)  
  
# Создание выборки данных для клиентов в России  
clients_russia <- clients %>% filter(Country == "Россия")  
  
# Вывод результата  
print(clients_russia)
```

Рис. 3. Сгенерированный через ChatGPT датасет с уточнением «клиенты в России»

	ID	Имя	Возраст	Город
1	1	Анна	25	Москва
2	2	Иван	35	Санкт-Петербург
3	3	Мария	30	Киев
4	4	Петр	45	Нью-Йорк
5	5	Елена	28	Лондон

Рис. 4. Интерпретация кода, представленного на рис. 1

	customer_id	name	age	email	city
1	1	Alex	36	customer1@example.com	Los Angeles
2	2	Alex	42	customer2@example.com	Boston
3	3	Jane	56	customer3@example.com	New York
4	4	Jane	43	customer4@example.com	Boston
5	5	Alex	26	customer5@example.com	New York
6	6	Michael	24	customer6@example.com	San Francisco

...

97	97	Alex	43	customer97@example.com	Boston
98	98	Emily	58	customer98@example.com	San Francisco
99	99	Emily	37	customer99@example.com	New York
100	100	Emily	23	customer100@example.com	Los Angeles

Рис. 5. Интерпретация кода, представленного на рис. 2

	ID	Name	Country	Age
1	1	Александр	Россия	43
2	3	Мария	Россия	42
3	7	Екатерина	Россия	37
4	11	Дмитрий	Россия	54
5	18	Дмитрий	Россия	59
6	23	Александр	Россия	38
7	32	Иван	Россия	34
8	37	Дмитрий	Россия	50
9	42	Дмитрий	Россия	22

...

28	94	Мария	Россия	26
29	96	Дмитрий	Россия	51
30	99	Екатерина	Россия	45

Рис. 6. Интерпретация кода, представленного на рис. 3

```
R Copy code  
  
# Установка и загрузка необходимых пакетов  
install.packages("shiny")  
install.packages("gapminder")  
library(shiny)  
library(gapminder)  
library(ggplot2)  
  
# Определение UI  
ui <- fluidPage(  
  titlePanel("Gapminder Data Visualization"),  
  
  sidebarLayout(  
    sidebarPanel(  
      selectInput("x", "Choose X-axis variable:", choices = c("gdpPercap", "lifeExp",  
        selectInput("y", "Choose Y-axis variable:", choices = c("gdpPercap", "lifeExp",  
        sliderInput("year", "Choose Year:", min = 1952, max = 2007, value = 1952)  
      ),  
    ),  
  
    mainPanel(  
      plotOutput("plot")  
    )  
  )  
)  
  
# Определение серверной части  
server <- function(input, output) {  
  output$plot <- renderPlot({  
    filtered_data <- gapminder %>%  
      filter(year == input$year)  
  
    ggplot(filtered_data, aes_string(x = input$x, y = input$y, color = "continent"))  
      geom_point() +  
      scale_x_log10() +  
      scale_y_log10() +  
      labs(x = input$x, y = input$y, color = "Continent", title = "Gapminder Data Vis  
  })  
}
```

Рис. 7. Сгенерированный ChatGPT код, который строит интерактивное веб-приложение с использованием пакета Shiny

В целом, видно, что сгенерированный код довольно полезен, его можно использовать даже без внесения изменений. Данное исследование показало, что использование искусственного интеллекта в аналитических рабочих процессах может быть не только интересным, но и полезным.

Использование ChatGPT для анализа данных представляет собой мощный инструмент, который может значительно улучшить процесс принятия

решений и помочь выявить скрытые паттерны и тренды в данных. Однако важно помнить, что для достижения оптимальных результатов необходимо правильно настроить и обучить модель, а также внимательно оценивать полученные выводы.

Gapminder Data Visualization

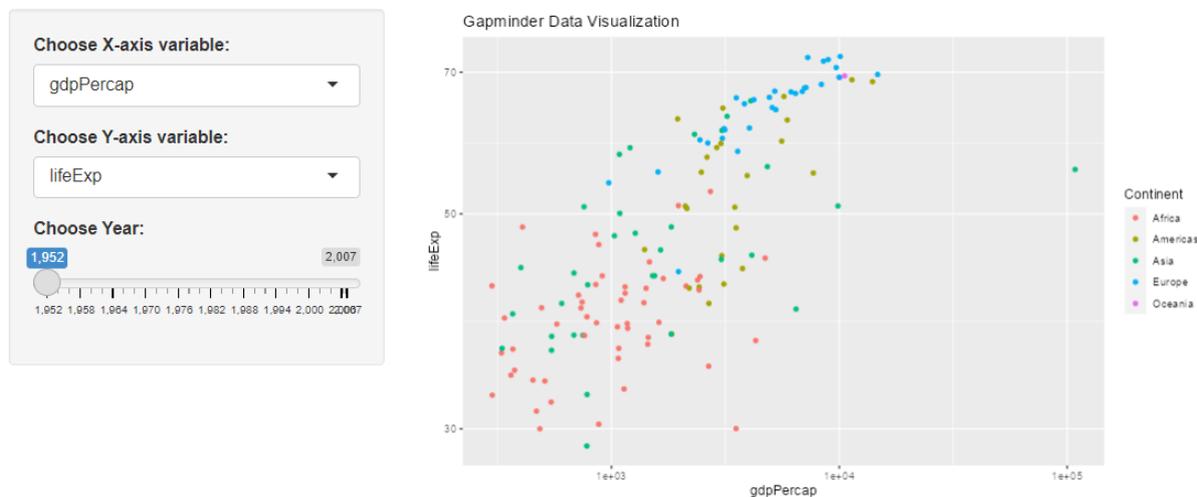


Рис. 8. Построенное при помощи ChatGPT интерактивное веб-приложение с использованием пакета Shiny

Список используемых источников

1. Aljanabi M. ChatGPT: Future Directions and Open possibilities // Mesopotamian Journal of Cyber Security. 2023. PP. 16–17. DOI: 10.58496/MJCS/2023/003
2. Christenson A., Goldstein W. Impact of data analytics in transforming the decision-making process // Business & IT. XII. PP. 74–82. DOI: 10.14311/bit.2022.01.09
3. Ashok Kumar M., Nandhini N., Kavitha G., Nuhu Ezra, Pushpavalli R. ChatGPT in Future Data Analytics // European Chemical Bulletin. 2023. Vol. 12. Iss. 8. PP. 3423–3433.

УДК 004.896
ГРНТИ 50.41.25

ИССЛЕДОВАНИЕ И АНАЛИЗ ПОТЕНЦИАЛА АВТОМАТИЗАЦИИ МОНИТОРИНГА МИКРОКЛИМАТА

К. А. Красавцева, О. В. Раковский

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

Рассмотрены и проанализированы основные аспекты развития средств мониторинга микроклимата. Определены сферы применения инструментов мониторинга микроклимата. Выполнен анализ технических средств, применяемых для мониторинга микроклимата. Определены особенности микроклимата как объекта автоматизации.

микроклимат, мониторинг, мониторинг микроклимата, анализ, инструмент, датчик

С древних времён люди использовали различные инструменты для мониторинга микроклимата. Солнечные камни помогали мореплавателям определять положение солнца и время суток, облегчая навигацию и настройку парусов для оптимальных условий ветра. Ранние термометры, такие как термоскоп Галилея, изобретённый в 16 веке, позволяли измерять изменения температуры. Эти инструменты играли важную роль в понимании и использовании условий окружающей среды.

В эпоху Средневековья и Ренессанса были изобретены новые инструменты. Гигрометры измеряли уровень влажности, что было важно для сельского хозяйства и текстильного производства. Анемометры измеряли скорость ветра и активно применялись в навигации и прогнозировании погоды. Осадкомеры применялись в сельском хозяйстве и управления водными ресурсами. Эти инструменты позволили людям более точно отслеживать и предсказывать изменения микроклимата, что привело к улучшению сельскохозяйственных методов, навигации и управления водными ресурсами.

Промышленная революция 19-го века привела к стремительному всех отраслей. Барометры, например, ртутный, стали широко использоваться для измерения атмосферного давления. С их помощью можно было получить расширенное представление о погодных условиях и высоте над уровнем моря. Психрометры измеряли как температуру, так и влажность, обеспечивая более точные измерения микроклимата. Кроме того, были разработаны первые датчики влажности почвы, что оказалось особенно полезно для сельского хозяйства. Эти инструменты внесли значительный вклад в понимание и управление микроклиматом.

В 20 веке также были разработаны новые инструменты для мониторинга микроклимата. Электронные датчики, например, такие как термисторы, обеспечили более точные измерения микроклиматических параметров в режиме реального времени.

Современные интеллектуальные инструменты позволяют осуществлять мониторинг микроклимата ещё более эффективно. Беспроводные датчики с поддержкой Bluetooth и Wi-Fi обеспечивают простое развёртывание и удалённый мониторинг. Устройства интернета вещей, такие как интеллектуальные метеостанции, объединяют множество датчиков предоставляя возможности дистанционного управления.

Понимание микроклимата имеет большое значение по разным причинам. В сельском хозяйстве оно помогает оптимизировать растениеводство и управление животноводством. В городском планировании – определяет дизайн городов с точки зрения комфорта жителей и устойчивости среды. В архитектуре понимание микроклимата улучшает эксплуатационные характеристики зданий.

В Центральной долине Калифорнии фермеры используют инструменты мониторинга микроклимата для отслеживания температуры и влажности на своих виноградниках. Эти данные помогают определить оптимальное время для применения средств орошения и других методов поддержания оптимальных условий, что приводит к увеличению урожайности винограда и улучшению качества вина [1].

Рыбоводы в Мурманской области используют датчики микроклимата для мониторинга температуры и уровня кислорода в воде лососёвых ферм. Эти данные помогают выявлять ранние признаки заболеваний и принимать своевременные меры по их предотвращению, что приводит к снижению потерь рыбы и повышению прибыльности [2].

Московский государственный университет имени М.В. Ломоносова использует инструменты мониторинга микроклимата для оценки воздействия городских "островков тепла" и выявления районов с плохим качеством воздуха. Эти данные используются для разработки стратегий улучшения городского микроклимата [3].

В Барселоне институт глобального здравоохранения использует инструменты мониторинга микроклимата для изучения взаимосвязи между городским микроклиматом и здоровьем человека. Это исследование привело к разработке руководящих принципов городского планирования и дизайна, которые повышают комфорт пешеходов и снижают количество заболеваний, связанных загрязнением воздуха [4].

В Дубае Burj Khalifa использует инструменты мониторинга микроклимата для управления температурой здания и системами вентиляции. Это гарантирует, что в здании будет комфортно даже при экстремальной жаре и влажности [5].

Национальный медицинский исследовательский центр имени В. А. Алмазова (Санкт-Петербург) использует систему мониторинга микроклимата в операционных и палатах интенсивной терапии. Это позволяет поддерживать оптимальные условия для пациентов и медицинского персонала, снижая риск инфекций и осложнений [6].

Таким образом, в современном мире средства мониторинга микроклимата имеют важное значение. Они применяются в жилых и коммерческих помещениях, производственных предприятиях, а также в сельском хозяйстве и медицине. Мониторинг микроклимата позволяет отслеживать и контролировать параметры окружающей среды, с целью обеспечения комфортных условий для пребывания людей, эффективности производственных процессов и заботы о здоровье растений и животных. При такой востребованности особое внимание следует обратить на перспективные тенденции в области мониторинга микроклимата.

Технологический процесс мониторинга микроклимата включает в себя сбор данных с датчиков, их анализ и отображение результатов. Для проведения мониторинга необходимо установить датчики температуры, влажности и других параметров в помещении или на территории, которую необходимо контролировать. Эти датчики должны быть связаны с системой сбора данных, которая будет регистрировать информацию и передавать ее на центральный дисплей или компьютер для анализа [7, 8].

Таким образом, технологический процесс мониторинга микроклимата включает следующие этапы:

1. Сбор данных. Данные передаются в центральную систему мониторинга через проводные или беспроводные соединения.
2. Обработка данных. Данные очищаются и анализируются для выявления тенденций, обнаружения аномалий и расчёта отчётных показателей, например, таких как средняя температура и влажность.
3. Визуализация и отчётность. Визуализация данных в режиме реального времени и за исторические периоды с помощью информационных панелей и отчётов.

На условия микроклимата влияет множество факторов, включая температуру, влажность, качество воздуха и освещение. Эти переменные взаимодействуют и влияют друг на друга, что затрудняет мониторинг, контроль и оптимизацию микроклимата.

Условия микроклимата могут значительно изменяться в пределах помещения и с течением времени. Такие факторы, как использование оборудования и внешние погодные условия, могут вызывать значительные колебания параметров, поэтому необходимо учитывать различные факторы, которые могут варьироваться в зависимости от задач и видов деятельности в исследуемой области.

К особенностям мониторинга микроклимата можно отнести следующие факторы:

1. Мониторинг в режиме реального времени. Очень часто данные об условиях окружающей среды необходимо фиксировать и анализировать в режиме реального времени, чтобы оперативно реагировать на возможные последствия.

2. Удалённый доступ. Зачастую, необходимо прибегать к средствам дистанционного мониторинга, которые обеспечивают удалённый доступ к данным.

3. Объёмная аналитика данных. Системы мониторинга могут анализировать значительные объёмы данных для выявления тенденций, обнаружения аномалий и предоставления информации о характеристиках микроклимата.

4. Интеграция с другими системами. Системы мониторинга микроклимата могут быть интегрированы с различными системами, для автоматизированного управления и иных целей. Интеграция может быть сложной и требовать дополнительных пользовательских интерфейсов или промежуточного программного обеспечения.

5. Точность и калибровка датчиков. Обеспечение точности и надёжности датчиков имеет большое значение для эффективного мониторинга микроклимата. Для поддержания работоспособности датчиков необходимы регулярная калибровка и техническое обслуживание. Помимо этого, датчики должны поставлять данные в едином формате или на систему обработки данных должна быть возложена задача по оптимизации разрозненных данных [9–11].

Внедрение современных технологий и методов автоматизации может значительно повысить эффективность и надёжность системы мониторинга микроклимата, но процесс этого внедрения связан с определёнными трудностями ввиду специфичности сферы применения. Микроклимат, как объект автоматизации, характеризуется изменчивостью параметров и зависит от различных факторов. Это необходимо учитывать при определении требования к системе мониторинга.

На основе проведённого анализа можно сделать вывод, что сфера мониторинга микроклимата представляет собой перспективное направление, в котором есть большой потенциал для развития и совершенствования. С появлением новых методов анализа данных, мониторинг микроклимата может стать ещё более точным, эффективным и доступным для широкого круга пользователей. Способность автоматизированных систем собирать, анализировать и представлять данные в режиме реального времени уже даёт многочисленные преимущества. Поскольку технологии продолжают развиваться, вполне вероятно, что автоматизация мониторинга микроклимата получит более широкое распространение в различных отраслях промышленности и условиях эксплуатации.

Список используемых источников:

1. Калифорнийский университет в Дэвисе. URL: <https://ucanr.edu/blogs/blogcore/post-detail.cfm?postnum=27912>
2. Федеральное агентство по рыболовству. URL: <https://www.fish.gov.ru>
3. Московский государственный университет имени М.В. Ломоносова. URL: <https://www.msu.ru/science/research-areas/earth-science/ecology>
4. Барселонский институт глобального здравоохранения. URL: <https://www.is-global.org>
5. Центр проектирования и строительства небоскребов. URL: <https://www.skyscraper-center.com/building/burj-khalifa/124>
6. НМИЦ им. В. А. Алмазова. URL: <https://www.almazovcentre.ru/press-tsentr/novosti/v-ntsmc-im-v-a-almazova-zapushchena-sistema-monitoringa-mikroklimata-v-operatsionnykh-ipalatakh-reanimatsii>
7. Руководство ASHRAE. Приложения для ОБКВ. URL: <https://www.ashrae.org/technical-resources/ashrae-handbook>
8. Техническое примечание NIST 1471. Системы автоматизации зданий. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/TN/nbstechnicalnote1471.pdf>
9. Проблемы и решения для мониторинга и управления микроклиматом в зданиях. URL: <https://www.mdpi.com/2073-4395/9/10/213>
10. Техническое примечание NIST 1864. Системы автоматизации и управления зданиями. URL: <https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1864.pdf>
11. Руководство ASHRAE 13. Системы кондиционирования и охлаждения Commissioning. URL: <https://www.ashrae.org/technical-resources/bookstore/ashrae-bookstore/product-details?ProductID=596401>

УДК 004.056
ГРНТИ 78.21.13

АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С УЧЕТОМ РЕЗУЛЬТАТОВ РАНЖИРОВАНИЯ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ

Д. В. Кривко, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье приводятся результаты разработки средства автоматизации тестирования на проникновение с учетом результатов ранжирования сведений об уязвимостях. Представлено описание взаимодействия структурных элементов средства автоматизации со средствами сканирования, реестрами уязвимостей и сведениями о наличии эксплойтов.

тестирование на проникновение, уязвимости, эксплойт, сканирование

В настоящее время, с увеличением количества программного обеспечения и его значимости для современного общества, вопросы безопасности программного обеспечения становятся все более важными. Особенно актуальными становятся вопросы, связанные с возможными угрозами для безопасности информации, которые могут возникнуть в результате несанкционированного доступа к программному обеспечению. Для обеспечения безопасности программного обеспечения необходимо использовать различные методы и средства тестирования на проникновение.

Автоматизация тестирования на проникновение – процесс использования автоматизирующих инструментов для проверки безопасности приложений и систем, повышающий оперативность исследования и включающий в себя применение техник тестирования на проникновение, которые используют злоумышленники для поиска уязвимостей в программном обеспечении, операционных системах, и позволяет команде сотрудников быстро обнаруживать проблемы безопасности [1].

Nmap и Metasploit являются одними из наиболее известных инструментов тестирования на проникновение, которые широко используются как при ручном, так и автоматизированном тестировании.

Использование Python-скриптов для взаимодействия с Nmap и Metasploit через API позволяет автоматизировать процесс тестирования на проникновение и улучшить его эффективность и гибкость [1]. Это также позволяет создавать интеграции с другими инструментами и системами, такими как системы управления уязвимостями и информационные панели, для получения более полной картины о состоянии безопасности организа-

ции. Модули `Rymetasploit` и `nmap3`, имеют поддержку API Python, что позволяет автоматизировать процесс тестирования на проникновение и интегрировать его в существующие системы автоматизации.

Модуль `Rymetasploit` обеспечивает программный интерфейс для работы с `Metasploit Framework`, который позволяет управлять эксплойтами и пейлоадами, создавать сессии и выполнять другие задачи, необходимые для проведения тестирования на проникновение. `Rymetasploit` также предоставляет удобный интерфейс для работы с `Metasploit RPC API`, который позволяет запускать сканеры уязвимостей и выполнять другие задачи с помощью Python-скриптов.

Структура модуля `Rymetasploit` представлена на рисунке 1.

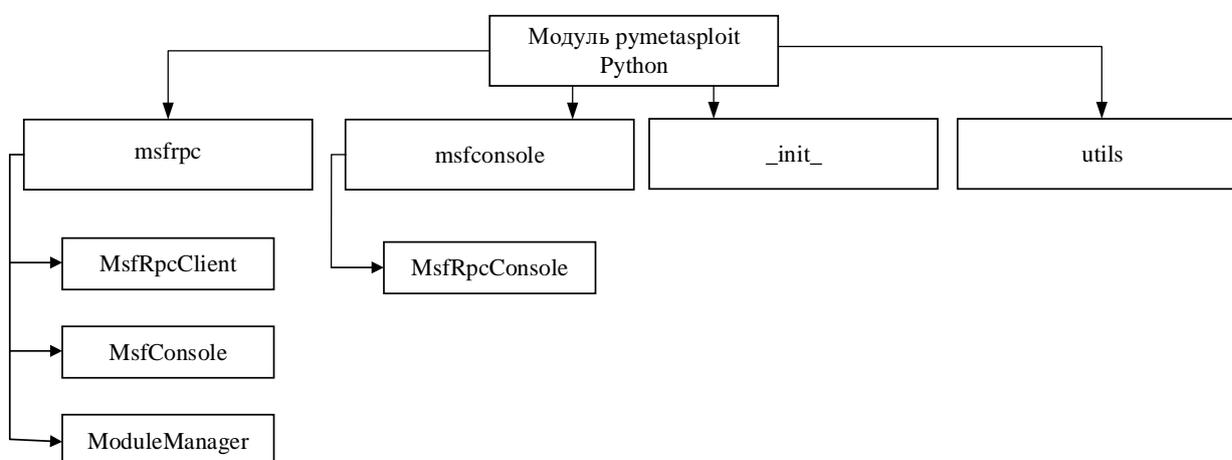


Рис. 1. Структура модуля `Rymetasploit Python`

С помощью `Rymetasploit` можно запускать модули `Metasploit Framework`, которые могут выполнять такие действия, как сканирование уязвимостей, сбор информации, эксплуатация уязвимостей и многое другое. `Rymetasploit` также позволяет управлять сеансами в `Metasploit Framework`, например, создавать новые сеансы и удалять старые.

Функциональная схема работы средства автоматизированного тестирования на проникновение представлена на рисунке 2 и достигается путем создания комплексного средства, в котором интегрируются несколько инструментов, выполняющих разные задачи по тестированию на проникновение [2]. Для повышения автоматизации выходные данные одной утилиты должны быть интерпретированы под входные данные другого программного средства.

Схема взаимодействия модуля интерфейса и утилиты `Nmap` представлена на рисунке 3. Схема взаимодействия модуля интерфейса `Nmap` и модуля анализа представлена на рисунке 4.

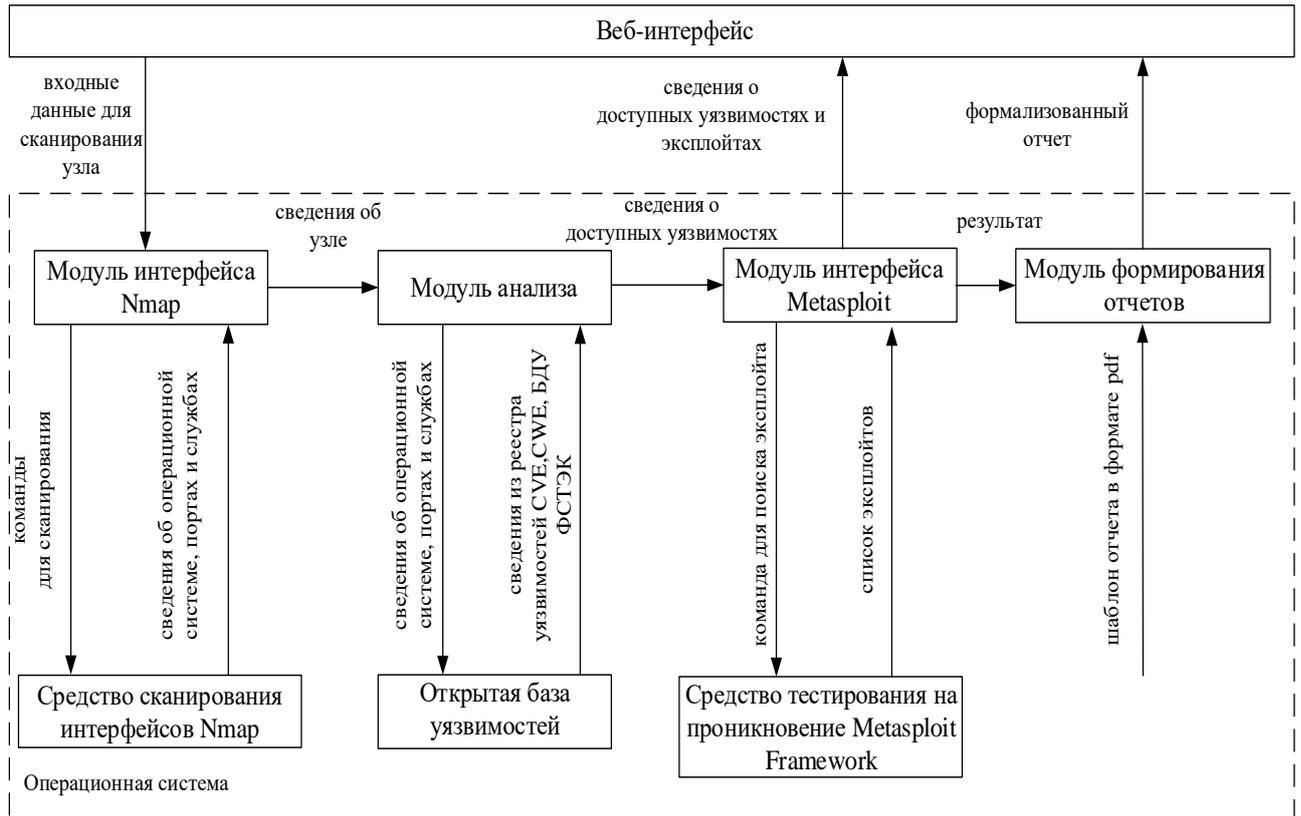


Рис. 2. Схема работы средства автоматизированного тестирования на проникновение

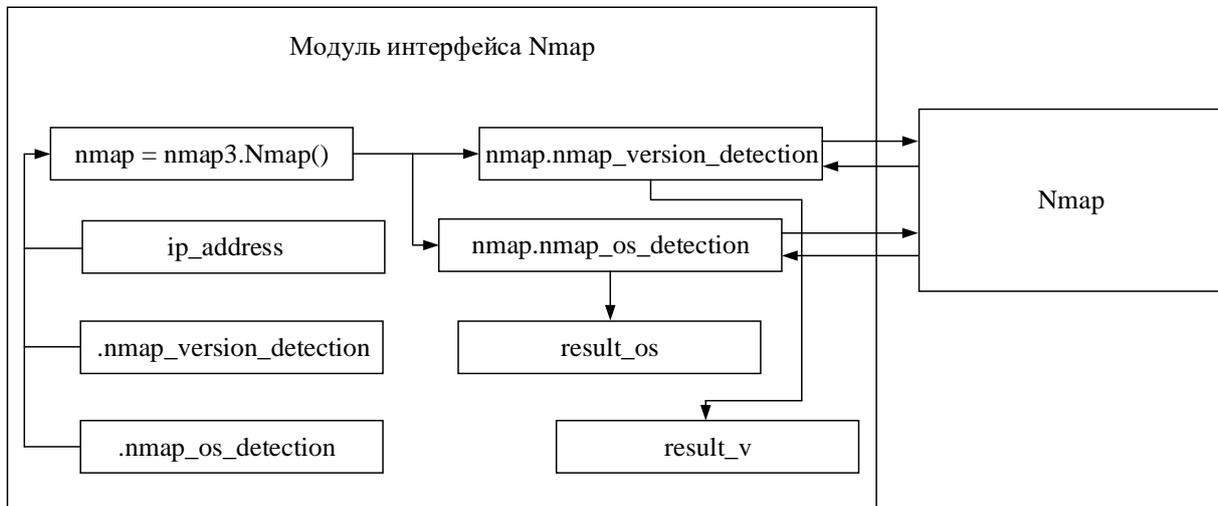


Рис. 3. Схема взаимодействия модуля интерфейса и утилиты Nmap

Далее модуль анализа формирует запрос на основе данных со сканирования, включающий порт, службу, программный продукт и операционную систему. Запрос отправляется в открытую базу уязвимостей NVD NIST через API 2.0 данного реестра. С помощью метода `KeywordSearch` производится поиск уязвимостей по данному запросу. В модуль анализа возвращаются идентификаторы уязвимостей CVE в список `cve_n`.

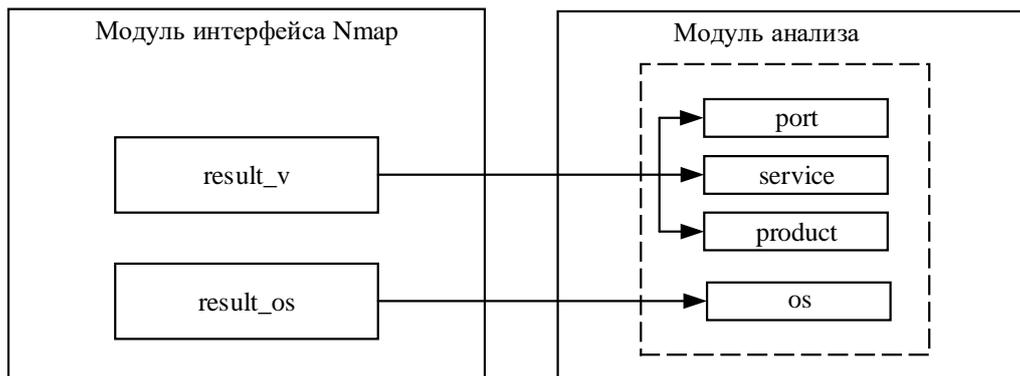


Рис. 4. Схема взаимодействия модуля интерфейса Nmap и модуля анализа

Далее модуль анализа производит поиск каждого элемента списка `cve_n` в Базе данных уязвимостей ФСТЭК. Поиск производится по первичному ключу – идентификатор CVE. В модуль анализа возвращаются данные в список `exploit_data`. Каждый элемент списка содержит следующую информацию: идентификатор БДУ; идентификатор CVE; вендор ПО; наименование ОС; класс уязвимости; уровень критичности; ссылки на источники; описание ошибки CWE; тип ошибки CWE.

Схема анализа уязвимостей в открытых реестрах для представлена на рисунке 5.

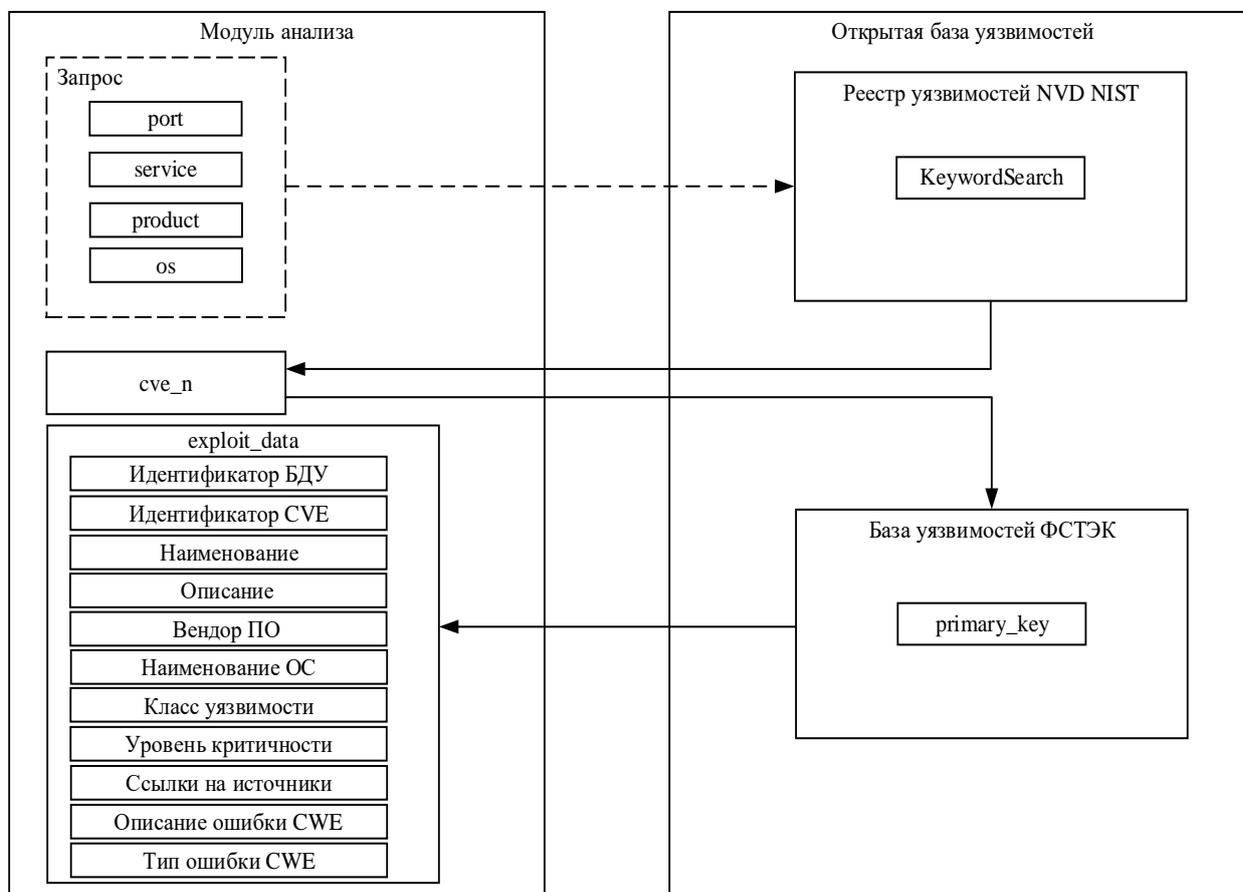


Рис. 5. Схема взаимодействия модуля анализа и открытой базы уязвимостей

Схема взаимодействия модуля анализа, модуля интерфейса и утилиты Metasploit Framework представлена на рисунке 6.

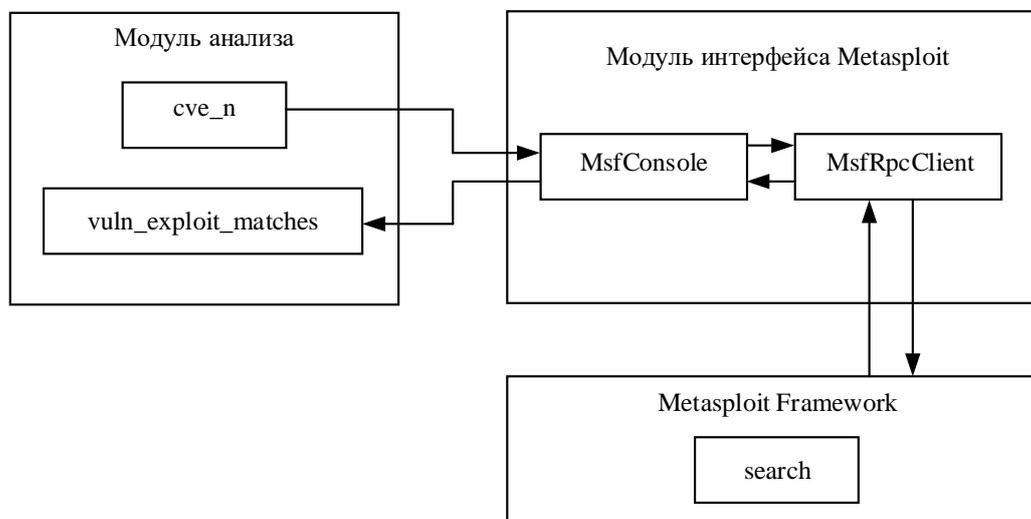


Рис. 6. Схема взаимодействия модуля анализа, модуля интерфейса и утилиты Metasploit Framework

Заключительным этапом работы программного средства автоматизированного тестирования на проникновение является вывод результатов тестирования на веб-интерфейс. Данные, обработанные в процессе тестирования, возвращаются в шаблон веб-страницы ответа. Схема взаимодействия представлена на рисунке 7.



Рис. 7. Схема взаимодействия модуля анализа и веб-интерфейса

Таким образом, обеспечив взаимодействие между отдельными модулями программного средства автоматизированного тестирования на проникновение разработан алгоритм работы данного средства.

Список используемых источников

1. Тестирование методом серого ящика: основные понятия и особенности, 2023 // Хабр [сайт]. URL: <https://habr.com/ru/company/solarsecurity/blog/590673> (дата обращения: 10.02.2024)
2. Автоматизация пентеста, 2022 // ib-bank. URL: <https://ib-bank.ru/bisjournal/post/1530> (дата обращения: 21.02.2023)

УДК 004.946
ГРНТИ 28.17.33

ВЫБОР ТЕХНОЛОГИИ И ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ПРОЦЕССОВ ВИЗУАЛЬНОГО КОНТРОЛЯ КАЧЕСТВА ВЫПОЛНЕНИЯ СБОРОЧНЫХ ОПЕРАЦИЙ

Д. А. Криволапов, А. А. Павлович

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

Рассматриваются пути снижения трудоёмкости и обеспечения оперативности и простоты процесса обучения выполнению сборочных операций для инженеров в сфере телекоммуникаций за счёт современных технологий виртуальной/дополненной и смешанной реальности на основе средств общего применения. Исследуются процедуры анализа и выбора программных средств для моделирования информативных моделей, а также процедуры выбора и анализа технологии для их подробного отображения. Представлены результаты применения варианта комплексирования выбранных программных средств.

телекоммуникации, дополненная реальность, виртуальная реальность, автоматизация

Для выполнения конструкторских и сборочно-разборочных работ, или эксплуатации техники связи человеку для минимизации рисков поломки оборудования или причинения себе вреда требуется практика работы с ним [1].

Под визуальным контролем подразумевается метод управления процессом сборки с помощью визуальных сигналов. Обучение в данном контексте приобретает смысл деятельности, направленной на приобретение практических навыков сборочных операций посредством применения современных технологий.

Оборудование не всегда есть в доступности. Бывают ситуации, когда обучение требуется до того, как придёт оборудование или его не хватает, чтобы выдать всем.

Готовые решения существуют на рынке, по этой причине говорить о полном отсутствии таковых нельзя. Но предложенные продукты или услуги недоступны для многих пользователей или компаний в силу различных причин. Например, дороговизны использования предлагаемых решений или создания собственных. Поэтому первая причина поиска новой возможности реализации технологии – дороговизна. Вторая – растущий рынок, показывающий наличие спроса. Прогноз динамики роста российского рынка промышленных VR (Virtual Reality – виртуальная реальность) /AR (Augmented Reality – дополненная реальность) решений представлена на рисунке 1 [2].



Рис. 1. Прогноз динамики роста российского рынка промышленных VR/AR решений

С целью снижения сложности разработки результата были проанализированы три технологии (рисунок 2, 3), применимые для реализации системы визуального контроля. В данном случае рационально использование дополненной реальности.

Параметр	Наименование технологии		
	Виртуальная реальность	Дополненная реальность	Смешанная реальность
1. Сложность программной реализации	0	1	0,5
2. Стоимость дополнительного оборудования	0	1	0,5
3. Наглядность	0,5	0	1

Рис. 2. Оценка применимости технологии

Анализ технологий показал, что наибольшую дешевизну обеспечивает визуальное представление в виде дополненной реальности с реализацией сборки на экране смартфона или планшета.

С целью снижения сложности разработки были проанализированы несколько типовых программных средств и возможность их свободного распространения (рисунок 4).

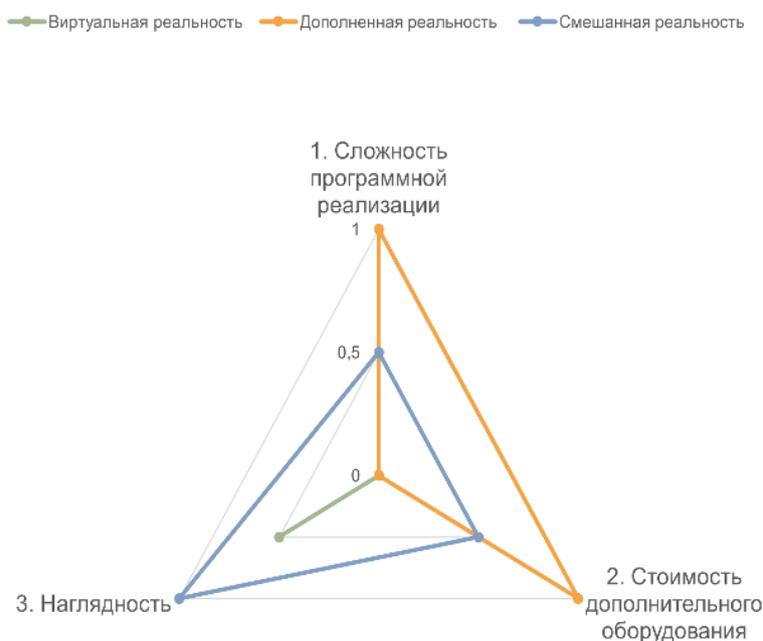


Рис. 3. Оценка применимости технологии

Параметр	Наименование программного обеспечения					
	AR Foundation Unity	Vuforia	Onirix	Google ARCore	Apple ARKit	Maxst
1. Возможность работы на целевых операционных системах	1	1	1	0,7	0,3	0,7
2. Применяемые средства разработки	0,9	1	0,7	0,9	0,8	0,6
3. Распространение	1	0,2	0,6	1	1	0,8

Рис. 4. Оценка применимости программных средств разработки

Составлена схема процессов визуального контроля качества выполнения сборочных операций (рисунок 6). Для реализации требуется объект, модель которого будет использована для обучения и устройство с экраном и камерой, на котором будет установлено разрабатываемое программное обеспечение. Рядом представлены варианты применения технологий – ДР, ВР и СМР.



Рис. 6. Схема процессов визуального контроля качества выполнения сборочных операций

Проведенный анализ функциональных возможностей, существующих программных и технологических средств реализации визуального контроля качества выполнения сборочных операций выявил необходимость реализации модуля идентификации объекта для определения модели и интерфейса для работы пользователей студентов и рабочих производства.

Предложена функциональная структура комплекса программно-технических средств (рисунок 7), который реализует интегрированное использование данных в управлении процессом сборки, а также принятые ограничения, накладываемые на него.



Рис. 7. Функциональная структура комплекса программно-технических средств

Таким образом, рассмотрены и отобраны рациональные для использования при реализации метода контроля качества выполнения сборочных операций технологии и программные средства. На основе оценки предложена функциональная структура комплекса программно-технических средств. Эффект от применения данного комплекса ожидается следующий:

1. Формируются обоснованные решения с применением автоматизированных комплексов.
2. Комплекс программных средств обеспечивает ограниченные риски по применяемым санкциям и минимум затрат на применение.
3. Обеспечивается доступность и простота пользовательского интерфейса за счёт апробированных решений.

Список используемых источников

1. Российский рынок промышленных VR/AR-решений – прогноз роста на 4 года. <https://chemtech.ru/rossijskij-rynok-promyshlennyh-vr-ar-reshenij-prognoz-rosta-na-4-goda/?ysclid=lufwwe4je6114069356>

2. Кузьминых Е.С., Маслова М.А. Анализ возможностей виртуальной и дополненной реальности: учебное пособие // Научный результат. 2022. № 7. С. 50–58.

УДК 004.42
ГРНТИ 50.41.25

ОРГАНИЗАЦИЯ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ВРЕМЕННЫМИ ТРУДОВЫМИ КОЛЛЕКТИВАМИ В РАМКАХ ВИРТУАЛЬНОГО ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ РЕЙТИНГОВОЙ СИСТЕМЫ

Э. Р. Крылова

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

В статье рассматривается проблема оптимизированного формирования временных трудовых коллективов на базе виртуальных предприятий, а также затрагивается вопрос развития рейтинговой системы или системы электронной репутации внутри компаний, предложен вариант использования интерфейса веб-приложения по автоматическому вычислению рейтинга участника киберсреды со стороны юридического лица.

киберсреда, виртуальные предприятия, электронная репутация, умное производство, временные трудовые коллективы, рейтинговая система

Виртуальное предприятие представляет собой временный союз предприятий, которые объединяются для обмена навыками или основными компетенциями и ресурсами, чье сотрудничество поддерживается компьютерными сетями в режиме реального времени. Предприятия отбираются по специальным организационно-техническим аспектам. Интеграция предприятий в единое киберфизическое пространство приводит к гибкой, эффективной и динамичной организационной системе, способной быстро кооперироваться для выполнения конкретных задач, исследований или выпуска продукции. Это проявление распределенных коллаборативных сетей.

Постепенно виртуальные предприятия образуют новые структуры под названием «Умное производство» (*Smart Factory*). Умное производство представляет собой полностью интегрированную корпоративную производственную систему, которая реагирует в режиме реального времени на все меняющиеся требования и условия на предприятии через компьютерную сеть. В процессе жизнедеятельности любого предприятия возникает необходимость создания временных трудовых коллективов (ВТК) для организации единого рабочего процесса и достижения конкретных целей, поставленных задач. Самой распространенной формой создания ВТК является формирование штатной группы в рамках одной компании (внутреннее формирование ВТК), с целью выполнения краткосрочных договоров и проектов для выполнения конкретной задачи.

На основе необходимости создания инициативных трудовых групп возникает потребность модернизации и оптимизации данного процесса, а также

процесса ведения рейтинговой системы. Возникает вопрос о правильном подборе кадровых ресурсов по фиксированным компетенциям и рейтинговым отборам для качественного формирования групп специалистов. В настоящее время данная проблема остается открытой для новых идей и разработок, в связи с чем предлагается создать систему по автоматическому ведению электронной репутации физических и юридических лиц. Такая система будет не только управлять электронной репутацией, но и иметь такие функции, как создание ВТК, автоматическая генерация документов и отчетов, поиск информации по физическим лицам и достижениям, составление отзывов и рецензий, интеграция со сторонними информационными ресурсами.

На рис. 1 представлена схема использования интерфейса веб-приложения по автоматическому вычислению рейтинга участника киберсреды (юридического лица).

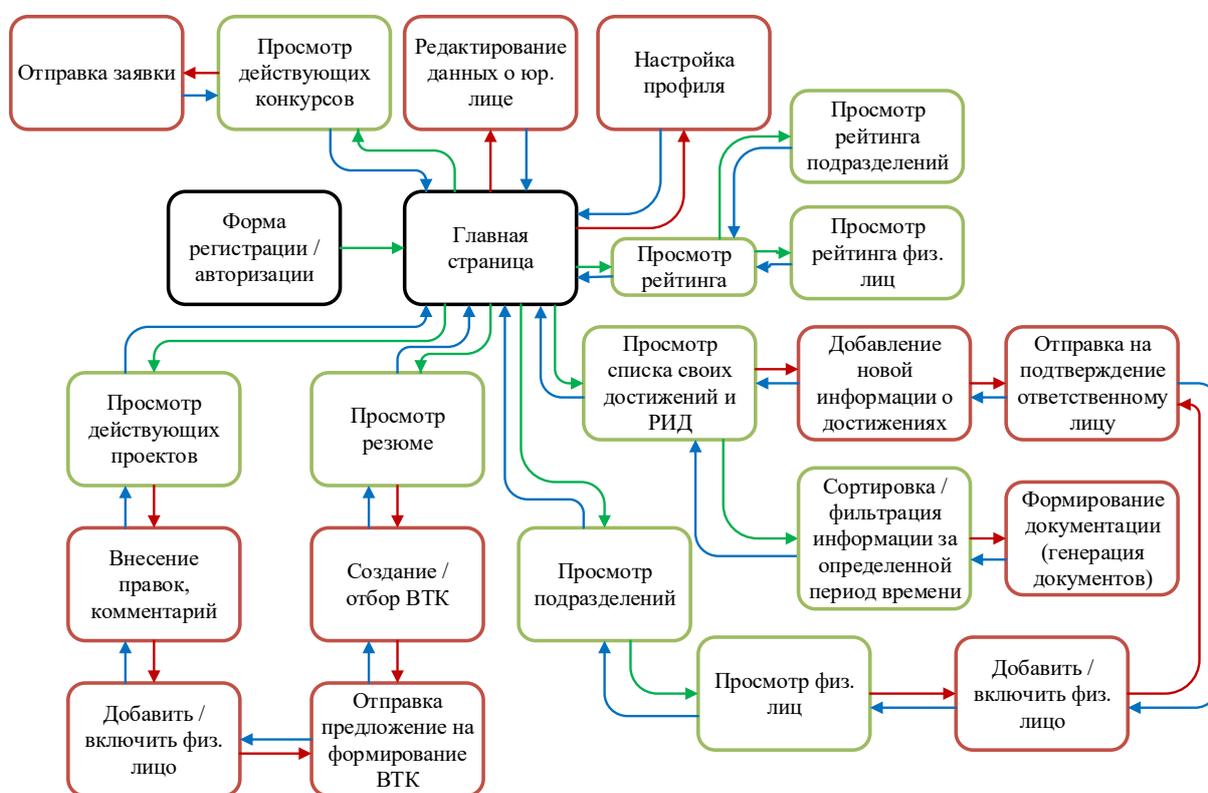


Рис. 1. Схема смены экранов интерфейса юридического лица

На рисунке 1 отражена схема смены экранов интерфейса профиля юридического лица при использовании приложения. Зелеными стрелками обозначены переходы на экраны режима просмотра, красные – на экраны редактирования, добавления, отправки, а синие – возврат на предыдущую страницу. Пример смены экранов использования приложения для юридических лиц, продемонстрированный в виде вайрфрейма (*WireFrame*), показан на рис. 2. На рисунке представлен сценарий создания ВТК с использованием веб-приложения.

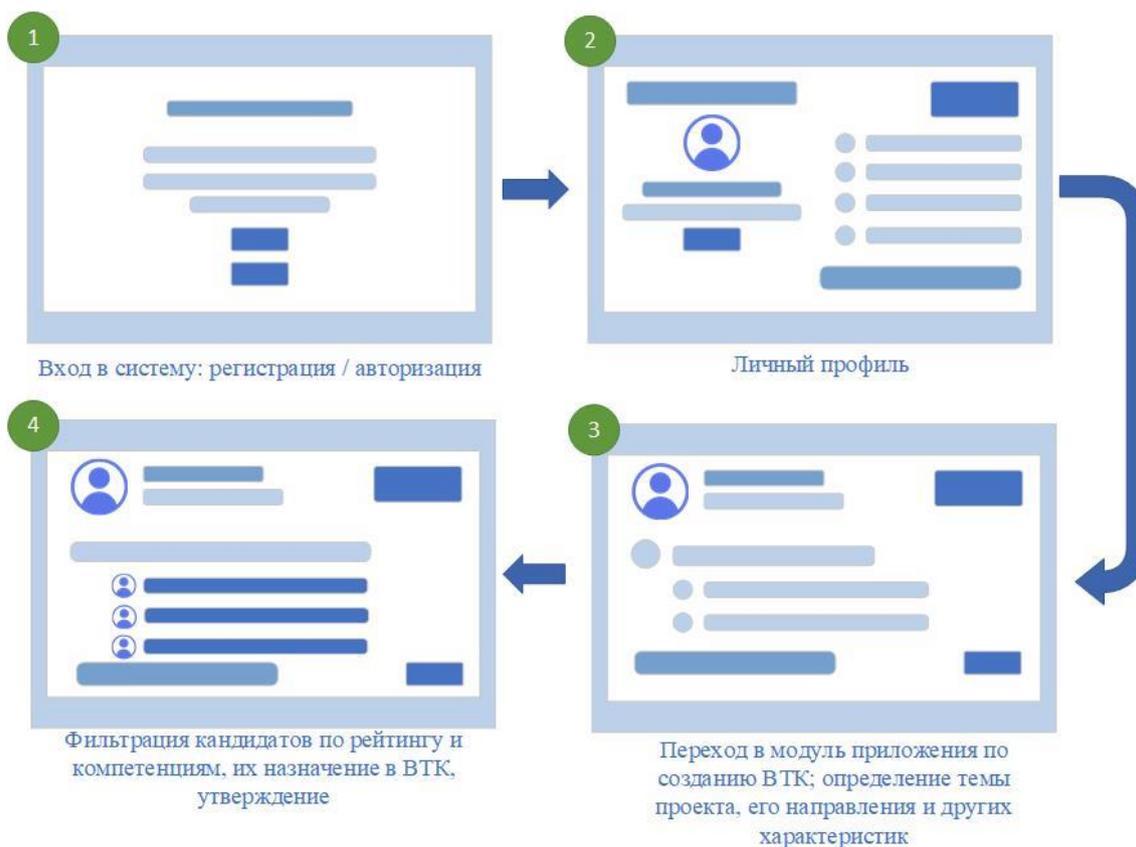


Рис. 2. Демонстрация схемы смены экранов приложения методом *WireFrame*

При создании ВТК для работы над каким-либо проектом через веб-приложение можно использовать такие функции, как сортировка, фильтрация, чтобы отобрать кандидатов по их рейтингам и компетенциям. Рейтинг каждого кандидата будет зависеть от его опыта и достижений в научно-профессиональной деятельности. Рейтинг юридического лица зависит от среднего арифметического достижений физических лиц, входящих в его состав [1]. Результат совместной работы в команде над единым проектом также будет влиять на рейтинг участников этого проекта и организации, в которой создавался этот проект.

Специфика системы электронной репутации заключается в методологии оценки интеллектуального уровня и компетенции пользователя или групп пользователей, которая реализована на основе полученных результатов интеллектуально-профессиональной деятельности на протяжении определенного периода времени. А электронная репутация является нематериальным активом виртуальных предприятий в условиях их развития [2].

Система управления репутацией является сложной структурой, направленной на формирование статуса как участника системы, так и организации, на основе которой обе стороны имеют определенное положение на рынке труда. С помощью такой системы с легкостью обеспечивается взаимосвязь компаний-партнеров, специалистов и организаций, вовлеченных в общее дело [3].

Список используемых источников

1. Верховая Г. В., Крылова Э. Р. Модели автоматического формирования электронной репутации юридических лиц в рамках, распределенных интероперабельных киберфизических сред // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 2. С. 451–455.

2. Абрамкина О. М. Институт репутации в современной России. Перспективы развития // Скиф. Вопросы студенческой науки. 2020. Выпуск № 5(45). С. 123–126.

3. Акимов С. В., Давлетшина Э. Р. Модели управления кадровыми ресурсами в киберсреде виртуальных предприятий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 23–27.

Статья представлена научным руководителем, профессором кафедры ИСАУ СПбГУТ, доктором технических наук, профессором Г. В. Верховой.

УДК 004.9
ГРНТИ 50.41.25

ГИС-СЕРВИС ПО ДОСТАВКЕ МИКРОЗЕЛЕНИ В МУРМАНСКОЙ ОБЛАСТИ

О. Б. Кузнецова, Д. В. Куликов, К. А. Трубчанинов

Мурманский арктический университет

В последнее время микрозелень получила большую популярность и теперь все легче становится приобретение свежей зелени. Несмотря на рост интереса, вопрос по доставке микрозелени все еще остается не решенным. Выходом из сложившейся ситуации может быть использование геоинформационных систем.

геоинформационное обеспечение, ГИС-сервис, микрозелень, доставка микрозелени

Микрозелень – это крайне интересный и относительно новый продукт на российском рынке. С недавних пор такая ветвь в развитии фермерского дела стала популярной. Многие люди заинтересованы в здоровом питании ради того, чтобы быть здоровее, спортивнее и т.д. Эта группа людей представляет точку роста аграрной отрасли.

Микрозелень – это молодые побеги растений, которые принимаются в пищу или служат для украшения блюд. Ее особенностью является наличие большого количества витаминов и питательных веществ. Также, она очень быстро созревает (чуть меньше недели). Для того чтобы получить всю пользу, необходимо есть микрозелень только в свежем виде [1, 2, 3].

Отсюда, вытекают особенности в процессе производства и продажи: товар имеет малый жизненный цикл, его можно продать только в течение нескольких дней (иначе она перерастает) и доставлять его нужно только в свежем виде (иначе польза теряется).

Таким образом, чтобы грамотно спланировать производство и доставку микрозелени, необходимо применение современных информационных технологий. Геоинформационные системы как нельзя лучше подходят для решения подобных задач.

Целью работы является разработка и реализация ГИС-сервиса по доставке микрозелени в Мурманской области (на примере компании «МикроЗеленьЕм»).

ГИС-сервис состоит из двух подсистем:

- обработки и хранения данных;
- отображения и визуализации данных.

Результатом является веб-приложение, позволяющее работать с клиентами, товарами, заказами, а также анализировать статистику по продажам.

Рассмотрим работу ГИС-сервиса с точки зрения конечного пользователя. При открытии ГИС-сервиса пользователь увидит главную страницу. На этой странице пользователь может прочесть информацию о компании, перейти в другие разделы, а также оставить заявку на дегустацию (рис. 1).



Рис. 1. Главная страница ГИС-сервиса

После нажатия на кнопку «Посмотреть весь ассортимент» мы попадаем на страницу с товарами. На данной странице отображаются все товары, ко-

торые можно сейчас приобрести. Карточка товара состоит из названия, количества оставшегося товара, цены, кнопки «Положить в корзину» и непосредственно изображения товара (рис. 2).



Рис. 2. Страница «Ассортимент»

После нажатия на кнопку «корзина» пользователю откроется страница корзины, в которой будут находиться все товары, которые были выбраны. На данной странице можно оформить заказ, а также изменить количество товара в корзине.

Пользователь не сможет оформить заказ, если он не авторизирован.

В случае, если у пользователя нет аккаунта он может зарегистрироваться, нажав на кнопку «Регистрация».

После входа пользователь может зайти в свой профиль и изменить информацию о себе, а также может посмотреть список заказов.

Первая вкладка «Работа с клиентами» включает себя информацию о всех клиентах и заявках на дегустацию. На этой странице можно удалить или добавить пользователя (рис. 3).

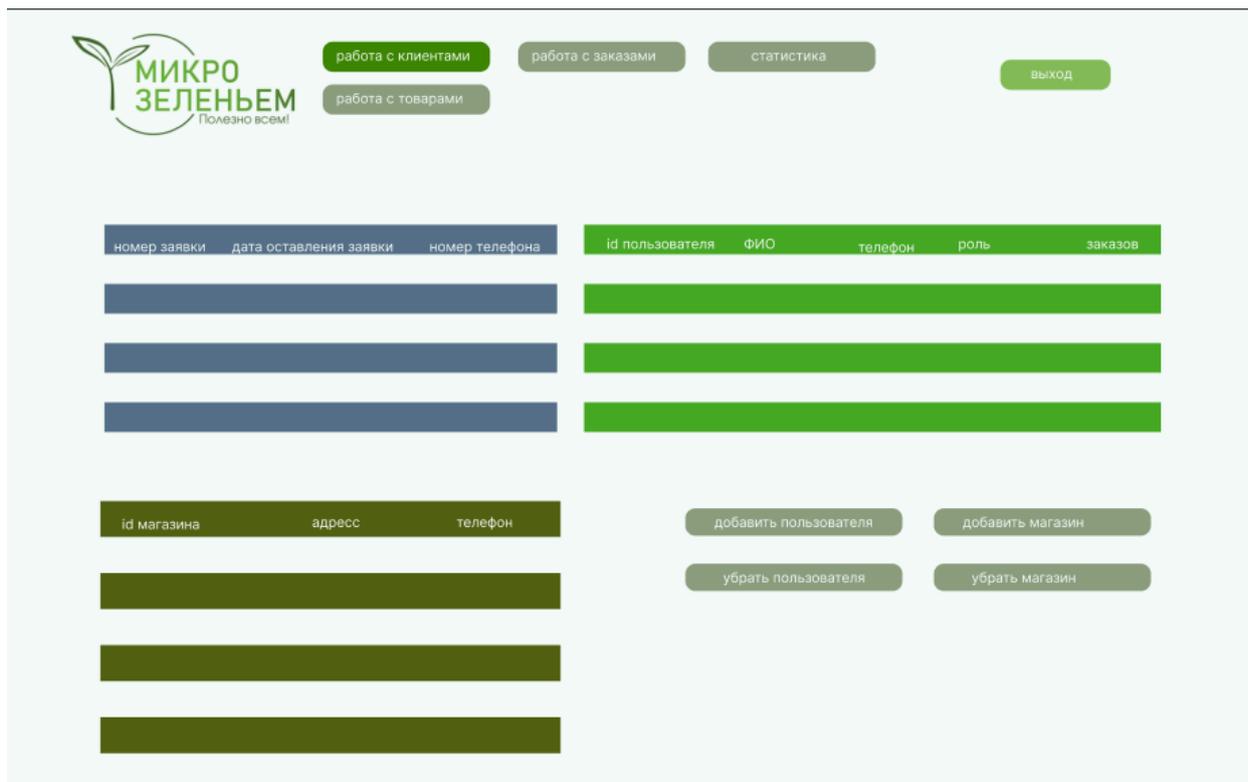


Рис. 3. Страница «Работа с клиентами»

Следующая страница – это страница работы с заказами. На данной странице можно посмотреть места заказов, посмотреть все заказы, а также можно обновить статус заказа (рис. 4).

Далее идет страница с товарами. На этой странице администратор может добавить новый товар, возобновить продажу товара или же приостановить продажу, а также редактировать карточку товара и изменять количество товара.

В завершении на вкладке «Статистика» можно просмотреть аналитическую информацию по продажам микрозелени.

Таким образом, можно констатировать, что цель работы достигнута.

Предложенное решение позволит ускорить процесс доставки микрозелени компании «МикроЗеленьЕм», а также оптимально планировать процесс производства.

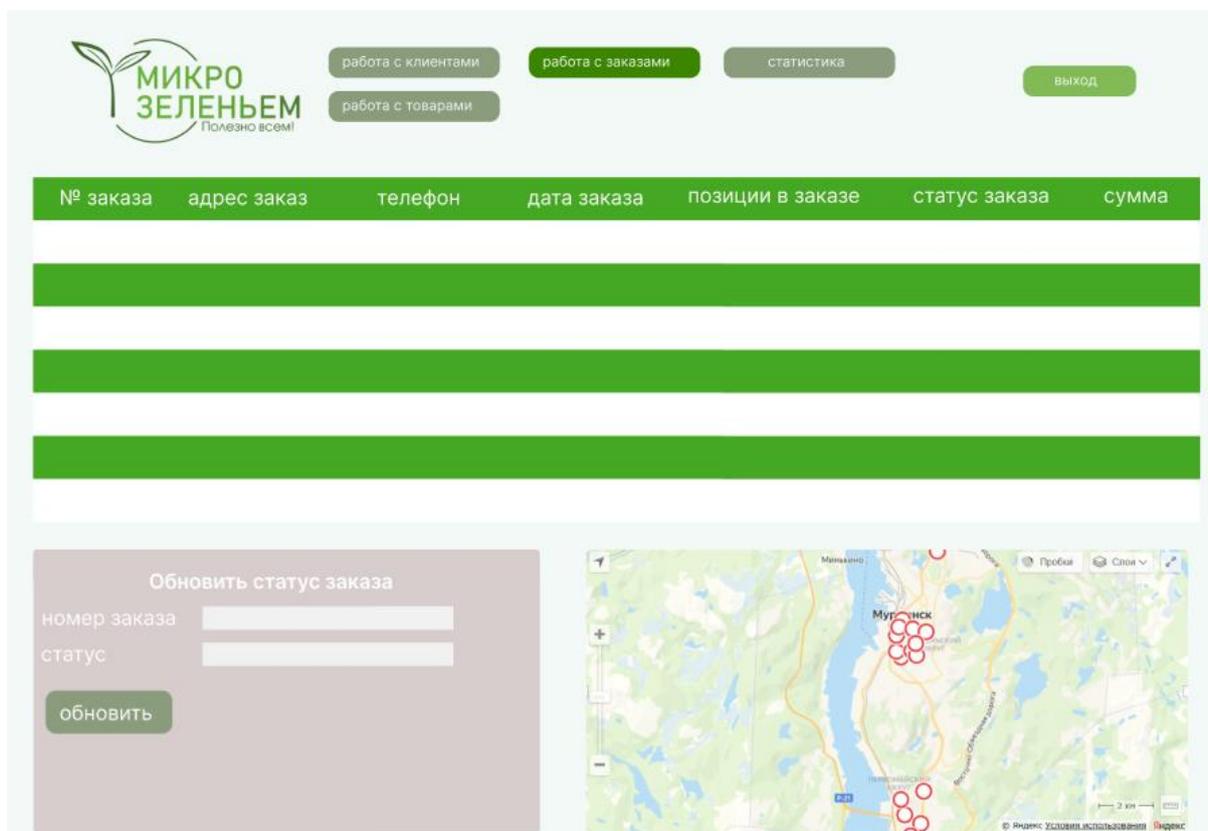


Рис. 4. Страница «Работа с заказами»

Список используемых источников

1. Сайт компании МИКРОЗЕЛЕНЬЕМ. URL: <https://microzelen51.ru/mikrozelen>—1 (дата обращения 13.01.2024)

2. Покупка микрозелени через Авито. URL: <https://www.avito.ru/murmansk?q=%D0%BC%D0%B8%D0%BA%D1%80%D0%BE%D0%B7%D0%B5%D0%BB%D0%B5%D0%BD%D1%8C&ysclid=lrjvhkxby7800914318> (дата обращения 13.01.2024)

3. Покупка зелени через Микрогрин. URL: <https://microgreen51.vsite.pro> (дата обращения 13.01.2024)

УДК 004.9
ГРНТИ 50.41.25

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ВИЗУАЛИЗАЦИИ ЗНАКОВЫХ ЛИЧНЫХ ПЛОЩАДОК

О. Б. Кузнецова, В. Ю. Попова

Мурманский арктический университет

Геоинформационные системы и мобильные технологии прочно вошли в жизнь большинства людей – не стала исключением и их личная сфера. Визуализация знаковых для человека мест на карте с помощью мобильного приложения дает широчайшие возможности по конструированию и сохранению личной истории.

геоинформационное обеспечение, мобильное приложение, визуализация, личные знаковые площадки, конструирование личной истории

В настоящее время личные знаковые площадки приобретают все большую ценность для людей, т. к. это то физическое пространство, которое принадлежит непосредственно человеку и дает ему ощущение безопасности, сокровенности и индивидуальности. Другими словами – это любые места, где люди чувствуют себя комфортно и свободно, могут погрузиться в собственные мысли, отдохнуть или перезагрузиться [1, 2].

Сохранить память о подобных знаковых для человека местах и свою индивидуальную историю в целом невозможно без применения современных технологий – в первую очередь геоинформационных и мобильных, которые позволяют визуализировать всю необходимую информацию на карте, причем сделать это непосредственно в собственном смартфоне с возможностью увидеть описание, фото, видео о знаковом месте [2].

Целью работы является разработка и реализация мобильного приложения визуализации личных знаковых площадок.

Основной функцией приложения является размещение на карте точек – маркеров мест, которые имеют особое значение для людей, а также возможность добавить к ним описательную информацию; фото, видео, название места; название самого маркера; категорию для времяпрепровождения. Вся информация вводится непосредственно самим пользователем.

Результатом является визуализированная карта города Мурманска, отображающая информацию о маркерах пользователей приложения, а именно метки, которые делятся на категории «дружба», «любовь», «семья», а также «свои» и «общие», при долгом нажатии на которые можно увидеть описание, фото, видео о месте, который пользователь хотел выделить.

Рассмотрим работу мобильного приложения с точки зрения конечного пользователя.

При входе в приложение открывается экран с полями «Логин» и «Пароль» и кнопками «Войти» и «Зарегистрироваться». При нажатии на кнопку «Зарегистрироваться» будет осуществлен переход к экрану регистрации. Экран регистрации приведен на рисунке 1.

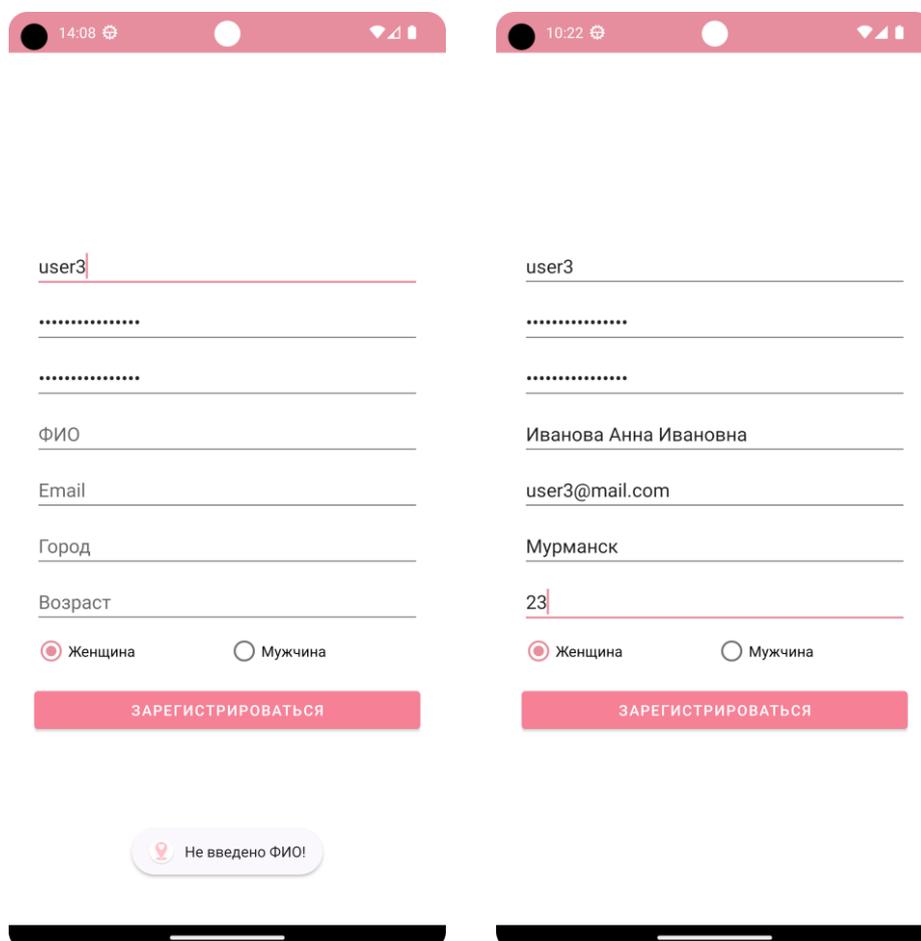


Рис. 1. Экран регистрации

В случае, если одно из полей не введено или ввод осуществлен некорректно будет выведено сообщение об ошибке с указанием поля. При корректном вводе значений всех полей на экране регистрации будет осуществлен переход на экран авторизации и выведено сообщение об успешной регистрации.

При нажатии на кнопку «Войти» в случае, если были введены верные данные зарегистрированного пользователя будет осуществлен вход и осуществлен переход к экрану «Просмотр мест», в случае если данные не были введены или были введены неверно будет выведено сообщение об ошибке. Экран «Просмотр мест» приведен на рисунке 2.

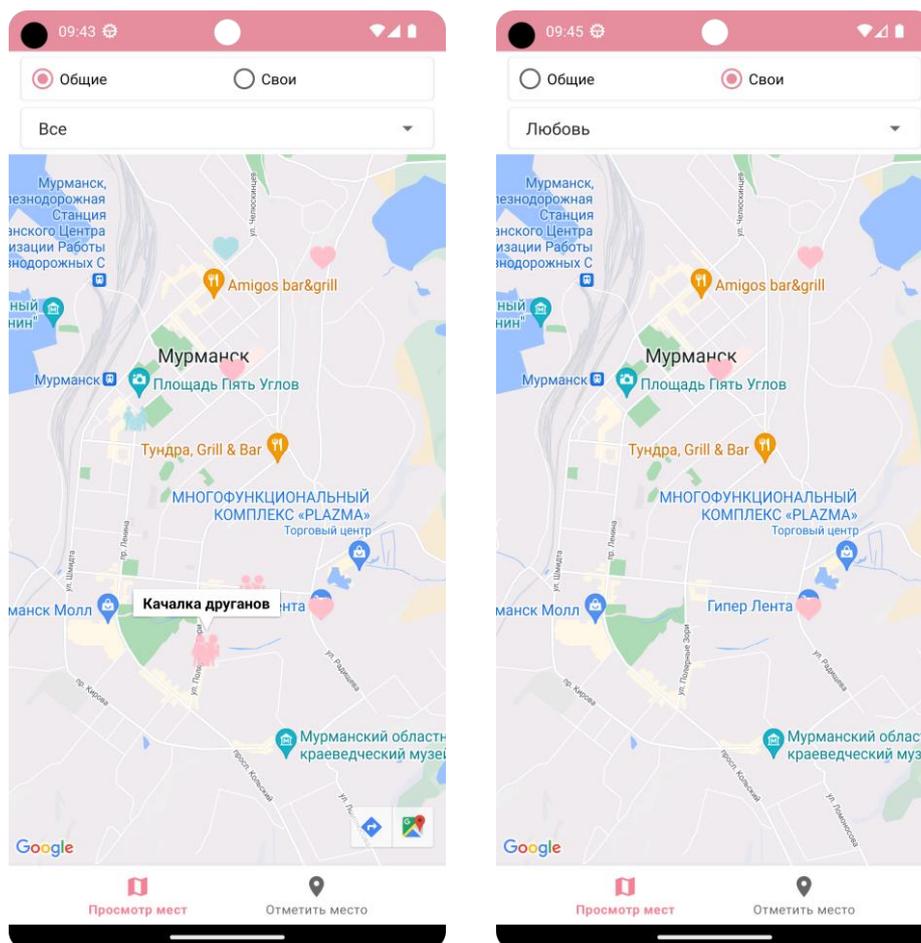


Рис. 2. Экран «Просмотр мест»

На экране просмотр мест доступна карта с отметками. Собственные отметки пользователя отображаются розовым цветом, чужие отметки голубым. При нажатии на отметку коротким нажатием отображается заголовок для отмеченного места. При нажатии на отметку длинным нажатием осуществляется переход на экран с подробной информацией о месте.

Для добавления нового маркера необходимо переключить режим на «Отметить место» в нижнем меню приложения, выбрать категорию и нажать долгим нажатием в нужном месте на карте. Откроется экран добавления нового маркера (рис. 3).

Если все поля были заполнены верно после нажатия на «Сохранить маркер» маркер будет сохранен, если же одно из полей не было заполнено или было заполнено неверно будет выведено сообщение об ошибке.

В сохраненный маркер можно добавлять фото. По нажатию на кнопку «Добавить фото» будет открыт файловый менеджер телефона и можно будет выбрать любое нужное изображение (рис. 4). После выбора фото будет выведено сообщение «Фото маркера добавлена» или сообщение об ошибке

в случае, если фото не удалось загрузить на сервер. Добавленные фото добавляются в прокручиваемый список под данными маркера, количество добавляемых фото неограниченно.

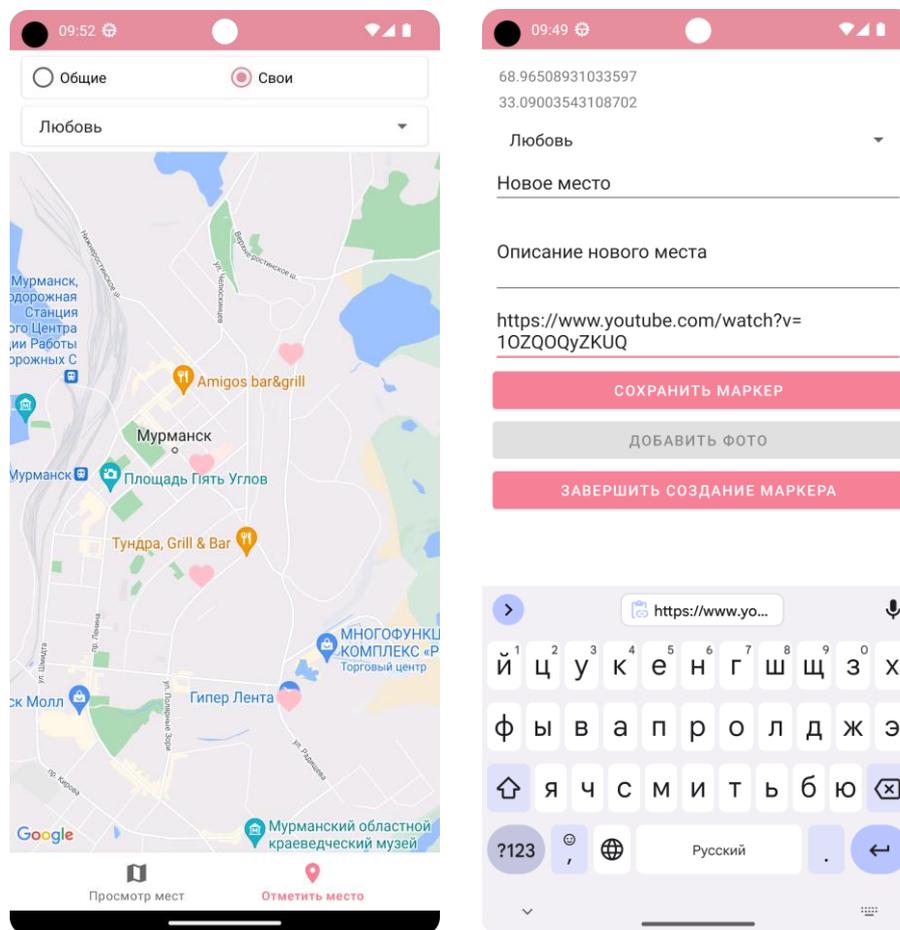


Рис. 3. Режим «Отметить место» и экран добавления нового маркера

При долгом нажатии на маркер в режиме «Просмотр мест» открывается детальная информация о маркере. А при нажатии на изображение на экране с детальной информацией о маркере изображение будет раскрыто на весь экран. В случае если к маркеру прикреплено более одного изображения переключаться между ними в полноэкранном режиме можно при помощи свайпов.

При нажатии на ссылку на видео откроется видео в приложении, без запуска браузера.

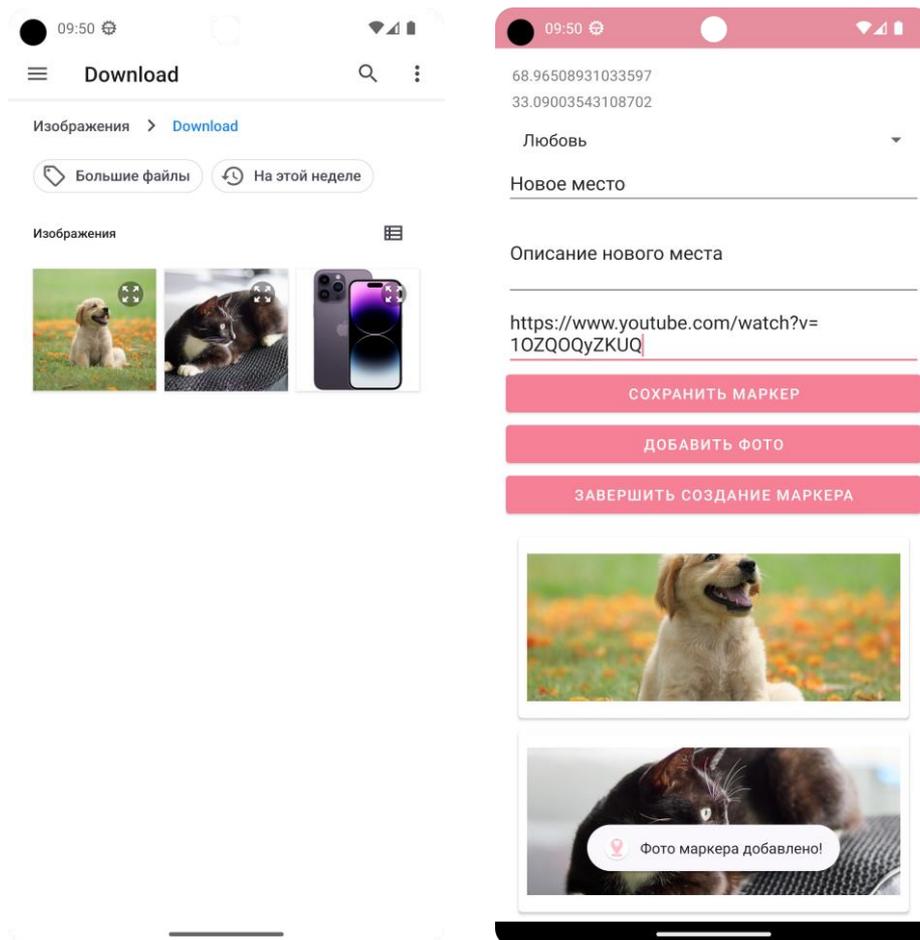


Рис. 4. Экран с выбором фото и экран создания маркера с добавленными фото

Таким образом, можно констатировать, что цель работы достигнута.

Предложенное решение позволит сохранить личную (родовую) историю, сэкономить время при поиске информации о нужном месте, улучшить психологическое и эмоциональное благополучие.

Список используемых источников

1. Корнющенко-Ермолаева Н. С. Коллективная историческая память: основания выделения понятия и роль в современной культуре / Н. С. Корнющенко-Ермолаева URL: <https://cyberleninka.ru/article/n/kollektivnaya-istoricheskaya-pamyat-osnovaniya-vydeleniya-ronyatiya-i-rol-v-sovremennoy-kulture/viewer> (дата обращения 03.02.2024)

2. Кузнецова О. Б. Геоинформационная поддержка визуализации личных знаковых площадок / О. Б. Кузнецова, В. Ю. Попова // Актуальные аспекты научных исследований: сборник статей XII Международной научно-практической конференции. Мск: Международный научно-издательский центр «Твоя наука», 2024. С. 143–147.

УДК 004.9
ГРНТИ 50.41.25

ГЕОИНФОРМАЦИОННОЕ ПРИЛОЖЕНИЕ ДЛЯ ПРОДВИЖЕНИЯ ИТ-НАПРАВЛЕНИЙ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

О. Б. Кузнецова, В. В. Явдощук

Мурманский арктический университет

Цель любого университета – обеспечить 100% набор студентов, удовлетворяющих требованиям ВУЗа в части знаний и желания получить соответствующие специальности. Чтобы этого добиться, необходимо вступать в контакт с абитуриентом заблаговременно, а не в момент подачи документов, и/или лишь предоставляя информацию об изучаемых специальностях. Геоинформационные технологии помогут существенно облегчить взаимодействие с потенциальными абитуриентами.

геоинформационное обеспечение, геоинформационное приложение, ИТ-направления, продвижение ИТ-направлений

Поступление в высшее учебное заведение (ВУЗ) – процесс достаточно сложный и многоступенчатый. Безусловно, он сопровождается постоянным поиском информации. Важнейшим элементом привлечения в ситуации конкуренции между университетами за наиболее талантливых и заинтересованных абитуриентов является эффективная информационно-коммуникационная система, когда абитуриент быстро получает достоверную, полную и полезную информацию об университете из воспринимаемого надежным источником. Высоким потенциалом для привлечения абитуриентов обладают мероприятия, нацеленные на профессиональную ориентацию школьников. Результатом должно стать повышение информированности как самих абитуриентов, так и их родителей об особенностях предлагаемых направлений обучения, актуальности выбранных профессий, их престижу в современных экономических условиях, востребованности на рынке и способности к адаптации в стремительно меняющихся условиях [1, 2].

Решение данного вопроса может быть достигнуто посредством разработки геоинформационного приложения для продвижения ИТ-направлений высшего учебного заведения.

Геоинформационное приложение включает следующие задачи (рис. 1):

- картографическая визуализация образовательных программ ИТ-направлений;
- блок основной информации по образовательным программам ИТ-направлений;
- блок интерактивных заданий по образовательным программам ИТ-направлений.

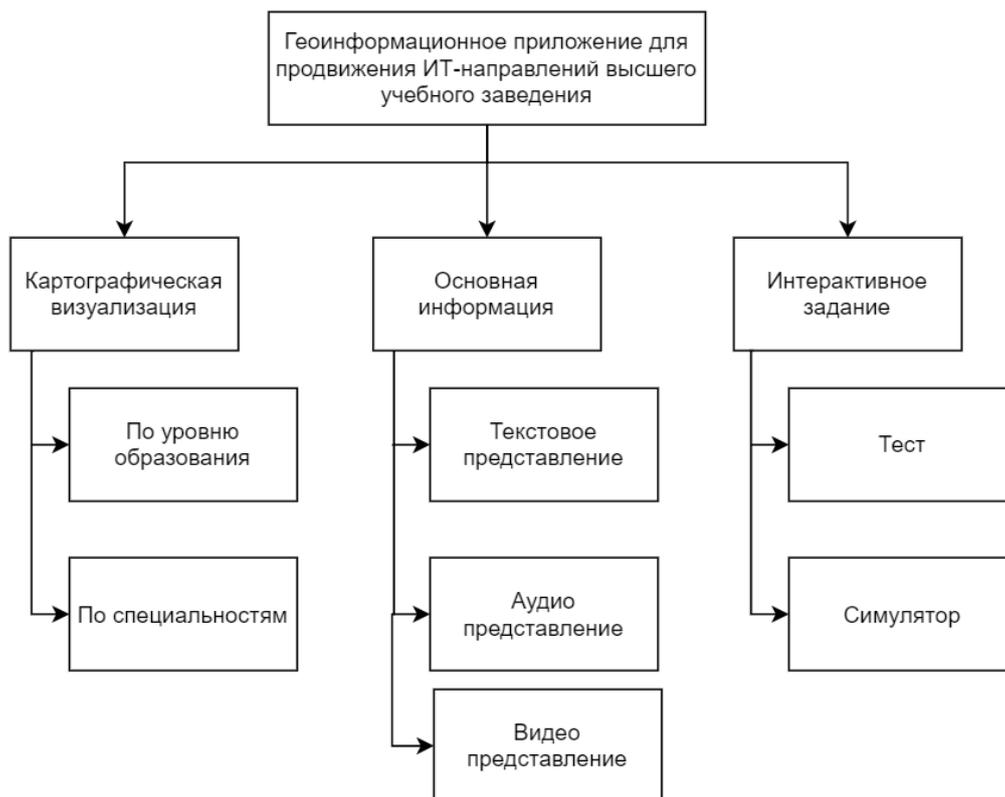


Рис. 1. Задачи геоинформационного приложения

Итогом решения задач будет визуализированная карта образовательных программ ИТ-направлений Мурманского арктического университета, отображающая информацию об образовательных программах, с интерактивными заданиями.

Такое решение повысит наглядность, сократит время сбора информации по предлагаемым образовательным программам.

Приложение носит тестовый характер, поэтому его работа показана на примере двух направлений бакалавриата.

При первом запуске приложения открывается экран приветствия с краткой информацией о приложении и его функционале, а также с окном для ввода имени пользователя (рис. 2).

Далее в случае первого запуска приложения запрашивается разрешение на отправку уведомлений.

При последующих запусках приложения сразу открывается карта ИТ-направлений (рис. 3). На нижней панели представлены кнопка «Прогресс» для перехода к списку текущих незавершенных контрольных точек карты, и кнопка «Закладки» для перехода к списку избранных точек. Чтобы добавить точку в избранное, нужно нажать на сердечко в правом верхнем углу соответствующего направления. При нажатии на одну из контрольных точек, представленных на карте, откроется информация о выбранном направлении (рис. 4).



Рис. 2. Экран приветствия при первом запуске



Рис. 3. Карта ИТ-направлений

Переход к следующей части информации по образовательной программе происходит при нажатии кнопки «Продолжить». Для возврата к карте необходимо нажать на крестик в левом верхнем углу. Для отключения аудиосопровождения на динамик в верхнем правом углу.

Когда блок информации по образовательной программе завершается, происходит переход к блоку заданий (рис. 5). После завершения блока информации и блока заданий по выбранному направлению, открывается поздравление с завершением.

Результатом проделанной работы явилось геоинформационное приложение, которое позволяет на интерактивной карте ИТ-направлений ФГАОУ ВО «МАУ» в игровой форме рассказать абитуриенту об особенностях каждого направления, дисциплинах, которые будут изучены за период обучения, этапах практической подготовки, возможностях дальнейшего трудоустройства, правилах приема и т. п.



Рис. 4. Информация о выбранном направлении

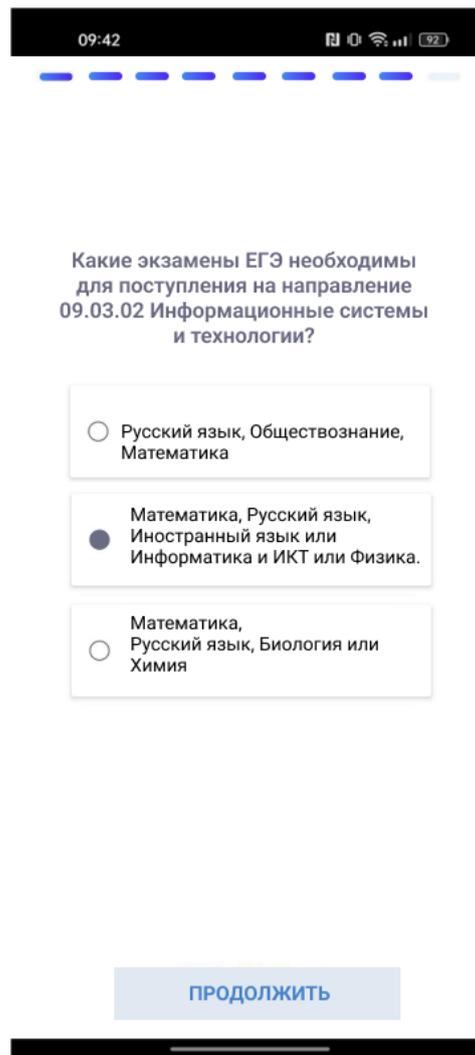


Рис. 5. Внешний вид формы «Задание»

Список используемых источников

1. Рябоконт М. В. Информационно-коммуникационная стратегия университета как средство привлечения абитуриентов / Рябоконт М. В., Черномор М. С. URL: <https://cyberleninka.ru/article/n/informatsionno-kommunikatsionnaya-strategiya-universiteta-kak-sredstvo-privlecheniya-abiturientov?ysclid=ln2oxaszm108291363> (дата обращения: 27.01.2024)

2. Авралева Н. В. Оптимизация стратегии вуза в области реализации новых программ рекрутинга студентов / Авралева Н. В., Ефимова И. Н., Маковойчук А. В. URL: <https://cyberleninka.ru/article/n/optimizatsiya-strategii-vuza-v-oblasti-realizatsii-novyh-programm-rekrutinga-studentov?ysclid=ln2qk0bxa677635387> (дата обращения: 20.01.2024)

УДК 004.725.5
ГРНТИ 20.51.19

ИССЛЕДОВАНИЕ ПОДХОДА К ИНТЕЛЛЕКТУАЛИЗАЦИИ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ

Р. Я. Лабковская, В. А. Тарасов

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

Современную организацию, даже небольшую, невозможно представить без развитой и разнообразной информационной инфраструктуры, которая требует оперативного управления, обслуживания и модернизации. От скорости и точности принятия решений при управлении компонентами корпоративной информационной системы зависит эффективность работы организации и, в конечном счёте, её прибыль, репутация и т. д. Необходимо сформировать подход к организации такого управления – выбор критериев оптимизации, средств и механизмов её реализации.

корпоративная информационная инфраструктура, программно-конфигурируемая сеть, классификация трафика, машинное обучение, нейронные сети

На современную корпоративную информационную систему, в отличие от компьютерных сетей прошлого, обеспечивавших преимущественно электронный документооборот и коллективный доступ к приложениям, возлагается широкий спектр задач, в том числе: аутентификация и авторизация пользователей, выделение им ресурсов хранения, вычислительных мощностей, предоставление доступа во внешние системы и к внутренним узлам, удалённая печать, обеспечение доступа на территорию и в помещения организации, осуществление визуального и иного контроля состояния объекта, обеспечение сигнализации и оповещения, разделение общей среды на виртуальные сегменты, реализация антивирусной защиты и препятствование несанкционированному доступу посредством среды передачи, шифрование трафика, проходящего через операторов связи и иные внешние системы, организация телефонии и видеоконференцсвязи, управление организационными и технологическими процессами, организация ассоциаций с фирмами-партнёрами и т. д.

Такой значительный объём разнородных задач, особенно в рамках крупной корпорации, налагает повышенные требования к инфраструктуре – аппаратным и программным средствам, технологиям реализации.

Особое внимание в данной связи следует уделить механизмам управления инфраструктурой корпоративной системы [1].

В процессе эксплуатации информационной системы могут возникнуть ситуации, требующие гибкой модификации инфраструктуры: увеличение

нагрузки на сегменты сети, необходимость подключения нового оборудования вследствие расширения системы, потребность в реконфигурации из-за изменения организационной инфраструктуры, задействование резервных маршрутов, обусловленное выходом из строя системных компонентов, приоритезация прикладных процессов и др. Всё это требует оперативного принятия управленческих решений – либо исключительно административным персоналом, либо персоналом с использованием систем автоматизации, либо автоматической системой. Последний вариант представляется более целесообразным ввиду следующих причин: отсутствия необходимости загрузки персонала (можно ограничиться мониторингом), повышенная скорость принятия решений и их реализации, потенциально меньшая вероятность ошибки при принятии решений и более высокая точность.

Важнейшей характеристикой, требующей мониторинга и управления, является нагрузка на передающий тракт. Поэтому для программно-конфигурируемой сети (SDN) встаёт задача классификации, идентификации трафика с последующей балансировкой нагрузки [2].

Существует ряд методов идентификации трафика. В том числе, сигнатурный анализ, классификация на основе блоков данных, машинное обучение.

Сущность первого заключается в определении типа трафика по характерным чертам структуры информационного блока. Недостатком метода является невозможность идентификации новых типов трафика.

Второй метод основан на анализе открытых полей пакета – портов, физических и логических адресов отправителя и получателя и т. д. Однако зашифрованный и тунелированный трафик с его помощью обработать не представляется возможным. Кроме того, использование некоторыми приложениями динамического порта лишает возможности идентифицировать трафик и его приложение.

Третий базируется на принципах машинного обучения, позволяющих как идентифицировать новый трафик, так и обходить устройства его меняющие, а также метод более точен, чем анализ поведения. Вместе с тем, требования к вычислительным мощностям при использовании данного метода выше. Тем не менее, более приемлемым представляется последний.

Задачу классификации трафика можно представить тремя этапами.

На первом осуществляется обучение системы на основе анализа признаков трафика, позволяющих отнести его к определённому классу.

Второй этап предусматривает проверку возможностей системы на основе анализа тестового набора данных, который не был включён в обучающую выборку.

Особенностью третьего этапа является поступление в систему трафика, обладающего своими характеристиками; система должна классифицировать его.

Для классификации сетевого трафика используются следующие виды машинного обучения: логистическая регрессия, деревья решений, случайный лес, метод опорных векторов, нейронные сети, k-ближайших соседей, градиентный бустинг, статистический подход.

В настоящее время классификация осуществляется применительно к потокам, а не отдельным пакетам – из потока выбирается определённое количество пакетов, на основе анализа которых по некоторому количеству характеристик идентифицируется поток как порождающее его приложение.

В качестве таких характеристик (параметров для машинного обучения) выступают следующие: тип протокола прикладного уровня, порт отправителя и получателя, IP-адрес отправителя и получателя, протокол шифрования, размер пакета в байтах, количество пакетов, переданных в секунду, задержка передачи, длительность потока, количество потоков, количество пакетов в потоке, длина заголовка, сигнатуры, время поступления данных, незашифрованные пакеты подтверждения, идентификатор протокола, пакеты для обслуживания сети, временные интервалы между пакетами.

Расширение масштабов сетей и обработка больших данных вызвали значительный рост трафика. Традиционные нейронные сети оказываются неспособными выявлять необходимые дополнительные классифицирующие показатели. Для более детальной оценки трафика рекомендуется использовать нейронные сети с глубоким обучением [3].

На основе SDN и механизмов глубокого обучения можно сформировать метод классификации, включающий следующие модули: модель классификации сетевых приложений на основе глубокого обучения; комбинация многоуровневого автокодировщика для извлечения параметров и свойств потока и регрессионной модели для классификации сетевых приложений.

И хотя в рамках данного подхода остаётся ряд нерешённых вопросов, комбинация архитектуры SDN с технологиями искусственного интеллекта способна выработать механизмы управления корпоративной информационной инфраструктурой, позволяющие обеспечить надлежащее качества обслуживания, балансировку нагрузки и прогнозирование состояния сети.

Список используемых источников

1. Литвинов, В. Л., Тарасов В. А. Технологии управления корпоративными инфокоммуникационными инфраструктурами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международной научно-технической и научно-методической конференция: сб. науч. ст. в 4-х т. СПб.: СПб ГУТ, 2023. Т. 2. С. 787–790.

2. Дмитриева Ю. С., Окунева Д. В., Елагин В. С. Анализ методов идентификации трафика для управления ресурсами в SDN // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 42–57.

3. Елагин В. С. Модель классификации трафика в программно-конфигурируемых сетях с элементами искусственного интеллекта // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 66–78.

УДК 004.657
ГРНТИ 20.23.17

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ПОВЕДЕНИЯ ТРАНЗАКЦИЙ НА РАЗЛИЧНЫХ УРОВНЯХ ИЗОЛЯЦИИ В СУБД POSTGRESQL

А. Н. Лапко

Академия Федеральной службы охраны Российской Федерации

Статья посвящена исследованию поведения транзакций на различных уровнях изоляции в СУБД PostgreSQL. Приведены аномалии, возможные в базе данных при параллельном выполнении транзакций. Детально описаны снимки данных, поведение SQL-операторов и причины возникновения аномалий на различных уровнях изоляции транзакций в СУБД PostgreSQL. Представлены результаты исследования в виде наборов SQL-операторов, которые при параллельном выполнении могут привести к ошибке доступа с откатом последней фиксируемой транзакции на различных уровнях изоляции.

база данных, параллельное выполнение транзакций, СУБД PostgreSQL, уровень изоляции транзакций, снимок данных, SQL-оператор, фиксация и откат транзакции

Одним из основных свойств, которым должны обладать транзакции при организации параллельного доступа в реляционных базах данных (БД), является изоляция транзакций. Свойство изоляции требует, чтобы все транзакции выполнялись независимо друг от друга [1].

В системе управления БД (СУБД) PostgreSQL изоляция транзакций обеспечивается на основе модели многоверсионного управления конкурентным доступом (Multiversion Concurrency Control, MVCC), в соответствии с которой каждый SQL-оператор видит свой снимок данных [2].

Обеспечение изоляции транзакций при их параллельном выполнении позволяет предотвратить негативные последствия (аномалии) в БД [1–3]:

1. Потерянное обновление – запись результата изменения данных, перекрывающая результат изменения этих же данных другой транзакции.

2. «Грязное» чтение (чтение «мусора») – чтение данных, измененных другой транзакцией, которая впоследствии отменяется.

3. Неповторяемое чтение – повторное чтение одних и тех же данных с получением различных значений.

4. Фантомное чтение – повторное выполнение запроса с получением различного количества строк в результирующем наборе.

5. Аномалия сериализации (несогласованности) – результат параллельного выполнения транзакций отличается от одного из возможных вариантов их последовательного выполнения.

Допустимость тех или иных аномалий в БД при организации параллельного доступа к данным определяется принятым в СУБД уровнем изоляции транзакций. В СУБД PostgreSQL поддерживаются три уровня изоляции транзакций [2–4]:

1. Уровень чтения зафиксированных данных обеспечивает частичную изоляцию транзакций и не допускает в БД возникновения аномалий потемного обновления и «грязного» чтения.

2. Уровень повторяемого чтения обеспечивает более строгую изоляцию транзакций и не допускает в БД возникновения никаких аномалий, за исключением аномалии сериализации.

3. Уровень сериализации обеспечивает самую строгую изоляцию транзакций и не допускает в БД возникновения никаких аномалий.

Следует отметить, что СУБД PostgreSQL формально поддерживает уровень чтения незафиксированных данных, но он аналогичен уровню чтения зафиксированных данных.

Рассмотрим поведение транзакций на различных уровнях изоляции в СУБД PostgreSQL.

На уровне чтения зафиксированных данных каждому SQL-оператору в транзакции предоставляется снимок (версия) данных, в котором отображаются результаты всех успешно зафиксированных транзакций на момент начала выполнения SQL-оператора, а также результаты изменения данных, выполненные ранее в текущей транзакции [2]. Отсутствие в снимке SQL-операторов выборки данных результатов незафиксированных транзакций исключает аномалию «грязного» чтения. Наличие же разных снимков у двух одинаковых SQL-операторов выборки данных, последовательно идущих друг за другом в одной транзакции, потенциально допускает аномалии неповторяемого и фантомного чтения. Аномалия неповторяемого чтения возможна, если в интервале времени между выполнением SQL-запросов выборки данных была успешно зафиксирована другая транзакция, изменившая эти данные, а аномалия фантомного чтения, – если в этом интервале была успешно зафиксирована транзакция, вставившая или удалившая строки из результирующего набора данных.

SQL-операторы изменения (удаления) данных при отборе целевых строк найдут только те, которые будут зафиксированы на момент начала выполнения этих операторов. Все отобранные строки, которые не будут заблокированы, подвергнутся требуемому изменению (удалению). Отобранные строки, которые окажутся заблокированными другими транзакциями, переведут текущую транзакцию в режим ожидания до тех пор, пока транзакции, выполнившие блокировки целевых строк, не завершатся фиксацией или откатом. После чего в текущей транзакции повторно проверится условие отбора для строк, которые были заблокированы, и выполнится требуе-

мое изменение (удаление) тех строк, для которых условие окажется выполненным. Операция изменения (удаления) строки выполнена не будет, если при повторной проверке условие для нее окажется невыполненным или эта строка будет удалена другой успешно завершившейся транзакцией.

На уровне повторяемого чтения каждому SQL-оператору в транзакции предоставляется снимок (версия) данных, в котором отображаются результаты всех успешно зафиксированных транзакций на момент начала выполнения текущей транзакции, а также результаты изменения данных, выполненные ранее в текущей транзакции [2]. Таким образом, на этом уровне исключается аномалия «грязного» чтения, поскольку в снимках SQL-операторов выборки данных отсутствуют результаты незафиксированных транзакций, а также исключаются аномалии неповторяемого и фантомного чтения, поскольку у двух одинаковых SQL-операторов выборки данных, последовательно идущих друг за другом в текущей транзакции, будут одинаковые снимки данных, даже если между их выполнением были успешно зафиксированы другие транзакции.

SQL-операторы изменения (удаления) данных при отборе целевых строк найдут только те, которые будут зафиксированы на момент начала текущей транзакции. Если среди отобранных строк некоторые из них окажутся заблокированными другой транзакцией для выполнения над ними операций изменения (удаления), то текущая транзакция перейдет в режим ожидания до тех пор, пока транзакция, выполнившая блокировку целевых строк, не завершится фиксацией или откатом. Если она завершится откатом, то текущая транзакция сможет выполнить требуемую операцию изменения (удаления) отобранных строк. Если же она завершится фиксацией результатов с изменением или удалением целевых строк, то произойдет откат текущей транзакции.

Уровень сериализации функционирует по правилам уровня повторяемого чтения, дополнительно отслеживая согласованность результатов параллельно выполняемых транзакций с результатами этих же транзакций при их последовательном выполнении [2].

Описанное поведение SQL-операторов на различных уровнях изоляции транзакций в СУБД PostgreSQL позволяет объяснить причину недопустимости «грязного» чтения на всех уровнях и потенциальной возможности неповторяемого и фантомного чтения на уровне чтения зафиксированных данных. Однако, не совсем понятно, как решается проблема потерянного обновления на различных уровнях изоляции, и какие именно SQL-операторы могут привести к аномалии сериализации.

Для ответа на эти вопросы проведена экспериментальная проверка поведения SQL-операторов на различных уровнях изоляции транзакций. В этой проверке исследованы SQL-операторы выборки, вставки (без предложения `On Conflict Do Update`), изменения и удаления данных, а также их

различные комбинации. Эти операции выполнялись применительно к таблице employ (табл. 1) в параллельных транзакциях, запущенных в двух сеансах. При этом предполагается, что SQL-операторы первого сеанса должны выполняться раньше SQL-операторов второго сеанса.

ТАБЛИЦА 1. Структура и данные таблицы employ

id (integer)	fio (text)	depart (integer)	salary (float)
1	Иванов	1	121.1
2	Петров	1	122.2
3	Сидоров	2	123.3
4	Попов	2	124.4
5	Титов	3	125.5

Результаты исследования показали, что на уровне чтения зафиксированных данных наличие любых комбинаций SQL-операторов в транзакциях позволяет зафиксировать в БД результаты обеих транзакций, тем самым исключая возможность аномалии потерянного обновления. Однако при этом параллельное выполнение SQL-операторов изменения или удаления пересекающегося набора строк (табл. 2), переводит транзакцию второго сеанса в состояние ожидания фиксации или отмены результатов транзакции первого сеанса.

ТАБЛИЦА 2. Примеры SQL-операторов, которые приводят к ошибке доступа на уровне повторяемого чтения

SQL-операторы одной транзакции	SQL-операторы другой транзакции
UPDATE employ SET salary = 100 WHERE fio = 'Иванов';	UPDATE employ SET salary = 150 WHERE depart = 1;
UPDATE employ SET salary = 100 WHERE fio = 'Иванов';	DELETE FROM employ WHERE depart = 1;
DELETE FROM employ WHERE fio = 'Иванов';	DELETE FROM employ WHERE depart = 1;

На уровне повторяемого чтения наличие любых комбинаций SQL-операторов в транзакциях, за исключением SQL-операторов изменения и удаления пересекающегося набора строк, позволяет зафиксировать в БД результаты обеих транзакций. Параллельное выполнение SQL-операторов изменения или удаления пересекающегося набора строк (табл. 2), переводит транзакцию второго сеанса в состояние ожидания. Только при отмене результатов транзакции первого сеанса могут быть зафиксированы результаты транзакции второго сеанса. В противном случае в БД произойдет ошибка

доступа из-за параллельного изменения с откатом результатов транзакции второго сеанса.

На уровне сериализации дополнительно к транзакциям, которые завершаются с ошибкой на уровне повторяемого чтения, невозможно зафиксировать результаты обеих транзакций, которые (табл. 3):

- – изменяют или удаляют даже непересекающийся набор строк;
- – вставляют и выбирают данные из одной таблицы, или одна, – вставляет и выбирает данные, а другая – изменяет или удаляет;
- – вставляют данные в таблицу с использованием подзапросов, или одна, – вставляет данные с подзапросом, а другая – изменяет или удаляет.

Параллельное выполнение транзакций с SQL-операторами (табл. 3) на уровне сериализации приводит к ошибке доступа из-за зависимостей чтения/записи с откатом результатов транзакции, фиксируемой последней.

ТАБЛИЦА 3. Примеры SQL-операторов, которые приводят к ошибке доступа на уровне сериализации

SQL-операторы одной транзакции	SQL-операторы другой транзакции
UPDATE employ SET salary = 100 WHERE depart = 1;	UPDATE employ SET salary = 150 WHERE depart = 2;
UPDATE employ SET salary = 100 WHERE fio = 'Иванов';	DELETE FROM employ WHERE fio = 'Петров';
DELETE FROM employ WHERE fio = 'Иванов';	DELETE FROM employ WHERE depart = 2;
SELECT * FROM employ; INSERT INTO employ VALUES (6, 'Орлов', 3, 126.6);	SELECT * FROM employ; INSERT INTO employ VALUES (7, 'Жуков', 1, 127.7);
	UPDATE employ SET salary = 100 WHERE fio = 'Петров';
	DELETE FROM employ WHERE id = 1;
INSERT INTO employ VALUES (6, 'Орлов', 3, (SELECT MIN(salary) FROM employ WHERE depart = 3));	INSERT INTO employ VALUES (7, 'Жуков', 1, (SELECT MIN(salary) FROM employ WHERE depart = 1));
	UPDATE employ SET salary = 100 WHERE fio = 'Петров';
	DELETE FROM employ WHERE id = 1;

Таким образом, на уровне сериализации параллельно без возникновения ошибок доступа можно выполнять лишь транзакции:

- одна, из которых только вставляет данные в таблицу без использования подзапросов или только выбирает данные из таблицы, а другая – изменяет, удаляет или выбирает данных из той же таблицы;
- с операциями выборки, вставки, изменения и удаления данных из разных таблиц.

На уровнях повторяемого чтения и сериализации аномалия потерянного обновления исключается за счет отката результатов некоторых транзакций. В этом случае следует предусмотреть повторное выполнение таких транзакций при возникновении ошибок доступа.

В заключении отметим, чем строже в БД изоляция транзакций, тем меньше аномалий в ней возможно, но тем больше транзакций требуют повторного выполнения из-за возникновения ошибок доступа.

Список используемых источников

1. Коннолли Т., Бегг К. Базы данных. проектирование, реализация и сопровождение. Теория и практика. 3-е изд.: пер. с англ. М. Вильямс, 2003. 1440 с.
2. Документация к PostgreSQL 15.1 // Постгрес Профессиональный, 2022. 2770 с. URL: <http://repo.postgrespro.ru/doc/pgsql/15/ru/postgres-A4.pdf> (дата обращения 12.12.2023)
3. Моргунов, Е.П. PostgreSQL. Основы языка SQL: учеб. пособие / Е.П. Моргунов; под ред. Е.В. Рогова, П.В. Лузанова. СПб.: БХВ-Петербург, 2018. 336 с.
4. Lapko A. On the issue of transactions isolation levels in the PostgreSQL DBMS // Modern informatization problems in the technological and telecommunication systems analysis and synthesis. Yelm, WA, USA: Science Book Publishing House, 2023. PP. 143–148.

УДК 004.422
ГРНТИ 50.41.25

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕДАКТОРОВ УРОВНЕЙ В РЕАЛИСТИЧНЫХ СИМУЛЯТОРАХ БПЛА

Д. В. Лебедев, А. А. Шиян

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

В данной статье приведен сравнительный анализ редакторов уровней в симуляторах БПЛА. В ходе сравнения учитывался функционал по созданию декораций, возможность настройки сценария, изменения погоды, системы физики. Были рассмотрены редакторы уровней симуляторов Liftoff, AI Drone Simulator, Velocidrone и The Drone Racing League Simulator.

БПЛА, симулятор, редактор уровней, редактор сценариев

В современной эпохе технологических достижений и инноваций, беспилотные летательные аппараты (БПЛА) выступают в качестве критически важных технических средств, находя применение в широком спектре областей, например, георазведке, мониторинге, поисково-спасательных операциях, военных задачах [1]. С ростом функциональности и значимости данного вида техники возникает необходимость в обучении операторов БПЛА. Однако, в силу ограничений полётных зон, получение практических навыков пилотирования затруднено. Данную проблему частично решают виртуальные симуляторы БПЛА [2].

Симуляторы БПЛА позволяют получить базовые навыки управления данными устройствами за счёт воплощения максимально приближенной к реальной физики полёта. Для получения профильных навыков использования БПЛА в той или иной сфере необходимо дополнительное обучение с использованием соответствующих виртуальных локаций и сценариев. Критически важным элементом в современных симуляторах БПЛА является редактор уровней. Этот инструмент используется для создания сценариев обучения, тестирования программного обеспечения и моделирования различных миссий. Целью данной статьи является сравнительный анализ наиболее популярных симуляторов БПЛА, в которых есть встроенный редактор сценариев. Среди таких симуляторов можно выделить следующие: Liftoff; AI Drone Simulator; Velocidrone; The Drone Racing League Simulator.

При сравнении редакторов уровней в данных симуляторах учитывались следующие критерии по функционалу: наличие инструмента по размещению декоративных объектов; возможность изменения ландшафта; отображение иерархии объектов в сцене уровня; возможность изменения погодных условий; поддержка разработки сценария уровня; наличие настроек физики окружения.

Liftoff

Симулятор Liftoff имеет встроенный конструктор уровней, который позволяет пользователю составить собственную трассу для дрон-рейсинга. Трассу можно создать только на основе подготовленной локации без возможности её изменения. Также пользователю доступен функционал по размещению декоративных и сценарных объектов, однако все они привязаны к единственному режиму симулятора – дрон-рейсингу. Настройки погодных условий и времени суток не предусмотрены. В симуляторе представлен только режим дрон-рейсинга, вследствие чего поддержка разработки собственного сценария отсутствует. Также в редакторе не представлена иерархия объектов и настройка физики окружения.

AI Drone Simulator

AI Drone Simulator, аналогично симулятору Liftoff, имеет встроенный редактор, основанный на создании уровней с применением подготовленных неизменяемых ландшафтов. Настройка декораций представлена с аналогичным Liftoff функционалом, однако количество декораций и их тематики разнообразнее. Также в редакторе имеется отображение иерархии объектов, которая позволяет быстро переключаться между объектами, а также настраивать гонку. Система погоды отсутствует. Основной режим в AI Drone Simulator – дрон-рейсинг, и, как следствие, это единственный тип сценария, который можно создать в редакторе уровней. Несмотря на то, что в симуляторе представлен ещё один режим – фристайл, он не имеет функциональных настроек и для него не могут быть созданы сценарии.

Velocidrone

Редактор уровней в Velocidrone использует подготовленные ландшафты и объекты окружения без возможности их редактирования, однако предоставляет пользователю расширенный функционал по работе с добавляемыми объектами, а также большой набор декораций, разбитых по категориям. В редакторе не отображается иерархия добавляемых объектов. Настройка погоды присутствует. Система физики окружения не представлена. В симуляторе Velocidrone единственный функциональный режим – дрон-рейсинг, вследствие чего настройка сценария ограничивается порядком ворот трассы.

The Drone Racing League Simulator

Данный симулятор позволяет создавать уровни с использованием только подготовленных локаций без возможности их изменения. Функционал добавления декораций и сценарных объектов аналогичен рассмотренным ранее AI Drone Simulator и Liftoff. The Drone Racing League

Simulator является наиболее технологичным из рассматриваемых сценариев в силу того, что здесь есть настройка системы физики декораций. Иерархия объектов и настройка освещения не представлены. В симуляторе представлены режимы дрон-рейсинга и свободного полёта, в силу чего настройка сценария уровня ограничивается только изменением порядка прохождения гоночной трассы. Результаты сравнения симуляторов представлены в таблице 1.

ТАБЛИЦА 1. Сравнение функционала редакторов уровней

Название	Изменение ландшафта	Система погоды	Трансформация декораций	Разработка сценария	Система физики	Иерархия объектов
Liftoff	–	–	+	–	–	–
AI Drone Simulator	–	–	+	–	–	+
Velocidrone	–	+	+	–	–	–
The DRL Simulator	–	+	+	–	+	–

На основе полученных результатов можно сделать следующие выводы:

- все рассмотренные редакторы уровней не имеют возможности создавать собственные ландшафты или изменять встроенные;
- в большинстве редакторов уровней представлен только режим дрон-рейсинга, создание собственного режима с помощью редакторов не предусмотрено;
- система погоды представлена только в половине редакторов уровней;
- настройка системы физики окружения есть только в одном редакторе уровней;
- иерархия объектов также представлена только в одном редакторе уровней.

Список используемых источников:

1. Будкин Е. Г., Постников А. А., Лагутина Е. И. Роль симулятора в подготовке оператора БПЛА вызов современности процессу обучения в военном вузе // Вестник военного образования. 2023. № 3(42). С. 27–30.

2. Миронов А. Б. Проблемы и перспективы использования беспилотных летательных аппаратов в сфере ландшафтной архитектуры / А. Б. Миронов, А. В. Терешкин // Материалы IV Национальной конференции по итогам научной и производственной работы преподавателей и студентов в области лесного дела, мелиорации и ландшафтной архитектуры, посвященной 100-летию подготовки специалистов в области лесного дела в Саратовском ГАУ (1922–2022 г.г.): Материалы конференции, Саратов, 16–20 мая 2022 г. Саратов: Амирит, 2022. С. 150–155.

УДК 007.3
ГРНТИ 28.23.37

МЕТОД ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ УПРАВЛЕНИИ СЕТЬЮ СВЯЗИ НА ОСНОВЕ ТЕХНОЛОГИИ НЕЙРОННЫХ СЕТЕЙ

В. А. Липатников, В. А. Парфиров

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

Предложен метод, в котором нейронная сеть в зависимости от доступности ресурсов определяет наборы действий, которые оцениваются на предмет соответствия результата их применения заданным критериям с максимальной эффективностью. Разработанный метод может быть использован в системах поддержки принятия решений в интересах обеспечения устойчивого функционирования сетей связи, а также других сложных организационно-технических систем, функционирующих в условиях деструктивных воздействий.

сеть связи, нейронная сеть, критерий, эффективность управления, действия по управлению, система поддержки принятия решений, управляющее решение

Сети связи (СС) в зависимости от назначения могут функционировать в условиях изменяющейся сигнально-помеховой обстановки (СПО) и возможных деструктивных воздействий (программных, радиоэлектронных, физических и т. д.) [1–4]. Для поддержания функционирования СС при заданных требованиях необходимо реализовывать управляющие воздействия на их элементы. Каждое управляющее воздействие выполняется при соответствующей обоснованности и эффективности.

Качество функционирования СС в общем виде характеризуется совокупностью показателей, зачастую находящимся во взаимно антагонистических соотношениях, зависящих от внешних и внутренних факторов, при этом, учет их является сложной задачей, в общем виде являющейся многокритериальной [5]. Поэтому, известные решения по управлению СС [3, 6–8], как правило, связаны с некоторыми ограничениями условия задачи. В частных случаях они могут приводить к некорректному результату, сказывающемуся на качестве функционирования СС.

В интересах устойчивого функционирования СС в [9] предлагается метод управления, который реализуется в виде алгоритма определения оптимального набора действий по поддержанию СС в заданных условиях. Однако, в алгоритме фактически осуществляется полный перебор возможных вариантов наборов управляющих действий [9, 10], из-за чего обладает относительно низкой оперативностью, так как при оценке каждого допустимого

набора требуется последовательно моделировать значение интересующего параметра при условии применения данного набора. Таким образом, требуется разработать технологию, позволяющую обеспечить поддержку принятия решения при управлении СС и обеспечить оперативное определение эффективного набора действий по управлению, исключая недостаток, связанный с последовательным анализом доступных наборов действий.

Целью статьи является повышение оперативности принятия решений по управлению СС при сохранении обоснованности и эффективности принятых решений.

Задача статьи состоит в разработке метода поддержки принятия решений при управлении СС на основе технологии нейронных сетей (НС), направленного на достижение поставленной цели.

Решение. В общем виде показатели, характеризующие каждое требование, предъявляемое к СС, заданы в руководящих документах и описаны в литературе [3, 11, 12]. Данные требования в общем виде можно представить, как соответствие значения вероятности соответствия показателя качества процесса функционирования соответствующему вероятностному критерию в течение заданного промежутка времени:

$$P_j(\xi_i(t) \left\{ \begin{array}{l} \geq \\ \leq \end{array} \right\} \xi_{i \text{ зад.}}) \left\{ \begin{array}{l} \geq \\ \leq \end{array} \right\} P_{j \text{ зад.}} \mid \forall i, i = \overline{1, N_j}; t \leq t_{\text{зад.}}, \quad (1)$$

где $\xi_i(t)$ – зависимость i -го параметра, влияющего на значение j -го показателя качества процесса функционирования СС от времени; $\xi_{i \text{ зад.}}$ – заданное значение i -го параметра (критерий), влияющего на значение j -го показателя;

$\left\{ \begin{array}{l} \geq \\ \leq \end{array} \right\}$ – знак, в общем виде характеризующий соотношение двух сравниваемых скалярных величин; P_j – вероятность выполнения процесса функционирования СС с требуемым качеством по j -му показателю; $P_{j \text{ зад.}}$ – заданное значение вероятности (критерий) выполнения процесса функционирования СС с требуемым качеством по j -му показателю; N_j – количество параметров, влияющих на значение j -го показателя качества процесса функционирования СС; i – номер параметра, влияющего на значение j -го показателя качества выполнения процесса функционирования СС; j – номер показателя качества выполнения процесса функционирования СС, $j = \overline{1, J}$, J – количество параметров, характеризующих качество процесса функционирования СС; t – время; $t_{\text{зад.}}$ – время в течение, которого требуется обеспечить выполнение условия (1).

Из выражения (1) следует, что, контролируя значения параметров и предпринимая действия по их корректировке на предмет поддержания ве-

роятности P_j в заданных пределах, можно обеспечить выполнение требований, предъявляемых к СС. Тогда, целевую функцию управления можно представить следующим выражением:

$$M_j : \langle S_j, R_j, D_j, W_j, t \rangle \rightarrow P_j(t) \left\{ \begin{array}{l} \geq \\ \leq \end{array} \right\} P_j \text{ зад.}; \quad (2)$$

$$\forall j, j = \overline{1, J};$$

$$t \leq t_{\text{зад.}},$$

где M_j – искомое преобразование, позволяющее определить значение вероятности выполнения процесса функционирования СС с требуемым качеством по j -му показателю; S_j – множество, характеризующее значения параметров СС, влияющее на значение вероятности процесса функционирования с требуемым качеством по j -му показателю; R_j – множество, характеризующее значения параметров внешнего воздействия, влияющее на значение вероятности процесса функционирования СС с требуемым качеством по j -му показателю; D_j – множество, характеризующее набор действий по приведению значения параметров СС к заданным значениям по j -му показателю; W_j – множество, характеризующее наличие ресурсов для обеспечения выполнения действий по приведению значения параметров СС к заданным значениям по j -му показателю.

Оценить адекватность управления СС можно путем оценки применения управляющих воздействий D_j и оценки выполнения условия (1). Эффективность набора действий D_j (управленческого решения) можно осуществить путем вычисления и оценки стоимости и времени его реализации:

$$F: \langle D_j, W_j \rangle \rightarrow \langle c_{\text{реал.}}, t_{\text{реал.}} \rangle \mid c_{\text{реал.}} \leq c_{\text{доп.}}; t_{\text{реал.}} \leq t_{\text{доп.}}, \quad (3)$$

где $c_{\text{реал.}}$ – стоимость реализации набора действий D_j ; $t_{\text{реал.}}$ – время реализации набора действий; F – искомое преобразование по вычислению $c_{\text{реал.}}$ и $t_{\text{реал.}}$; $c_{\text{доп.}}$ – допустимая стоимость реализации набора действий; $t_{\text{доп.}}$ – допустимое время реализации набора действий.

После оценки адекватности и эффективности наборов действий требуется выбрать оптимальное решение в соответствии с предпочтениями вышестоящей системы [13]:

$$A: \langle D_j \text{ адекв.}, \Pi \rangle \rightarrow D_j \text{ опт.}, \quad (4)$$

где A – искомое преобразование по определению оптимального набора действий; $D_j \text{ адекв.}$ – множество адекватных решений по управлению СС,

$D_j \text{ адекв.} = \bigcup_{k=1}^N D_{j,k}$, N – количество наборов действий, для которых выполняются

условия (2) и (3); $D_j opt$ – оптимальный набор действий по управлению СС; Π – функция предпочтений вышестоящей системы по отношению к СС.

В работе [9, 10] предложен метод и реализующий его алгоритм выработки управляющих воздействий на элементы СС в интересах обеспечения заданного качества функционирования, которые фактически реализуют решение задачи комбинаторики, направленной на перебор всех возможных вариантов управленческих решений из числа доступных. Известно [14], что эффективным решением комбинаторных задач является использование подходов основанных на механизмах искусственного интеллекта на базе технологии НС.

Структурная схема варианта реализации блока системы выработки управляющих воздействий с использованием технологии НС представлена на рис. 1.

Для простоты представления в качестве управляющих отдельных действий используются только четыре действия, доступность которых проверяется в первом слое СС в соответствии с доступными ресурсами. Из данных четырех действий формируется набор действий по управлению СС. Оценка адекватности (результативности) набора действий, выражение (2), проводится во втором слое НС. В третьем и четвертом слоях проводится оценка выполнения критериев стоимости реализации, выражение (3). В пятом слое из множества адекватных наборов действий (решений) определяется адекватный в соответствии с функцией предпочтения, выражение (4).

Соединив НС, представленные на рис. 1 и вычисляющие наборы действий по одному j -му показателю качества функционирования, параллельно, можно определить оптимальные наборы действий по приведению всех J показателей качества функционирования СС к заданному критерию. За рамками данной публикации осталось рассмотрение шестого и последующего слоев НС, которые должны обеспечивать сопоставление решений по приведению отдельных показателей качества функционирования СС к общему решению в зависимости от важности каждого отдельного показателя для решения общей задачи функционирования СС.

Разработанный метод может быть использован при создании систем поддержки принятия решений для управления СС, функционирующими в условиях изменяющейся СПО и возможных деструктивных воздействий. Применение технологий НС при выработке управленческих решений позволяет повысить оперативность принятия решений за счет выполнения параллельной обработки множества вариантов доступных действий, которое значительно увеличивается при увеличении количества доступных действий.

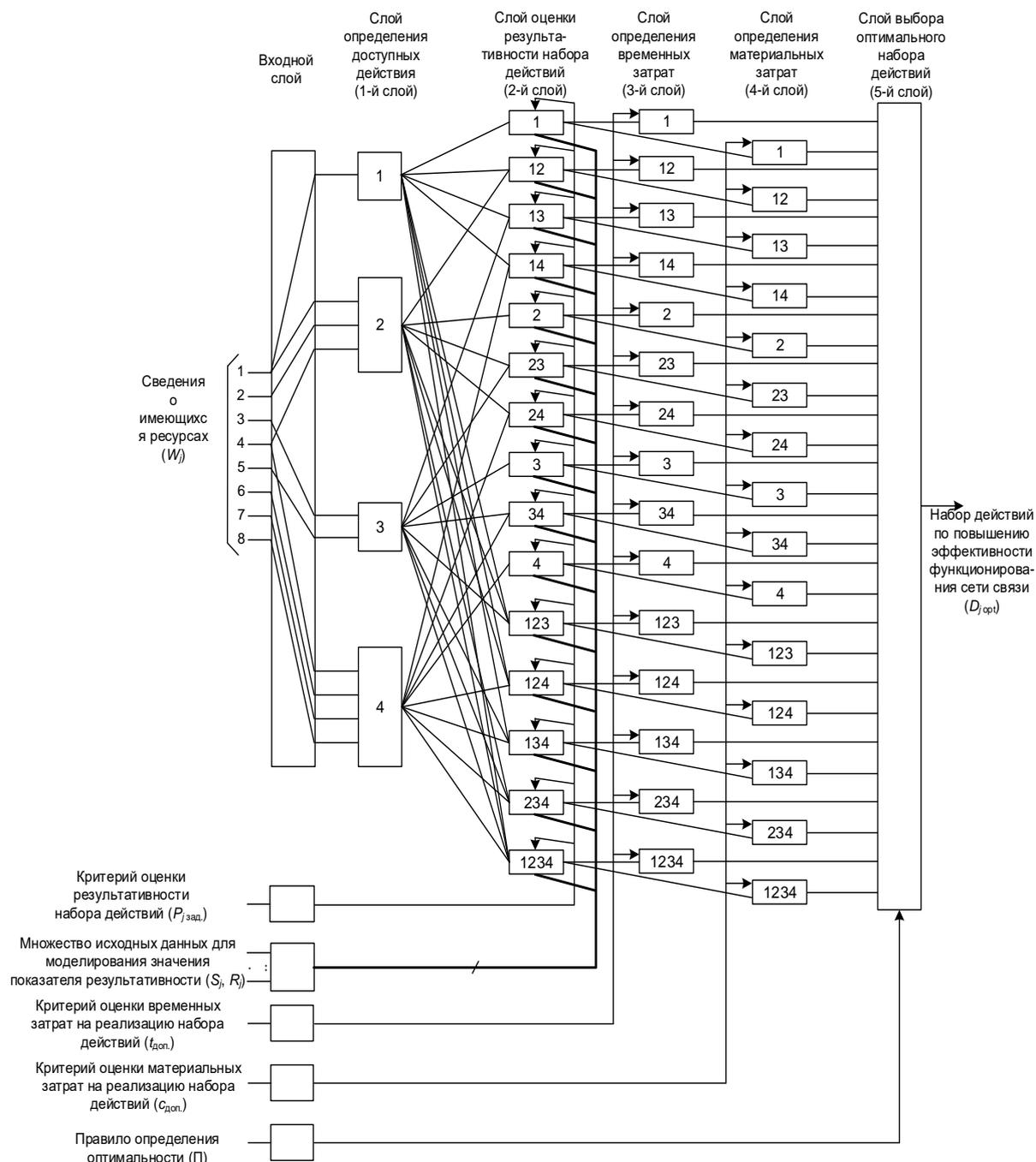


Рис. 1. Структурная схема НС вырабатывающая решение по управлению СС по одному из параметров

Список используемых источников

1. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства / Под ред. В. А. Липатникова. СПб.: ВАС, 2020. 716 с.
2. Липатников В. А., Парфиров В. А., Шевченко А. А., Мелехов К. В. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства // Актуальные проблемы защиты и безопасности: труды XXVI всерос.

науч.-практич. конф., Санкт-Петербург, 03–06 апр. 2023 г. СПб.: Типография Любавич, 2023. Т. 1. С. 569–572.

3. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. СПб.: Научно-технологические, 2020. 337 с.

4. Стародубцев Ю. И., Липатников В. А., Парфиров В. А. Проблема повышения разведывательной защищенности элементов военной системы связи // Военная мысль. 2023. № 7. С. 88–99.

5. Липатников В. А., Парфиров В. А., Петренко М. И. Общий алгоритм динамического управления устойчивым функционированием сети связи специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 3. С. 814–819.

6. Гречишников Е. В., Стародубцев Ю. И., Белов А. С. и др. Способ (варианты) управления демаскирующими признаками системы связи. Пат. 2450337 Российская Федерация; заявитель и патентообладатель Академия ФСО России. № 2011117814/08; заявл. 03.05.11; опубл. 10.05.12.

7. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем: материалы всерос. науч.-практич. конф. с междунар. участием, Санкт-Петербург, 28–29 мая 2019 г. СПб.: Институт проблем транспорта им. Н. С. Соломенко РАН, 2019. С. 207–214.

8. Липатников В. А., Парфиров В. А., Петренко М. И. Общая модель самоорганизующейся сети радиосвязи с мультиплексированием потоков // Транспорт России: проблемы и перспективы – 2022: материалы междунар. научно-практич. конф., Санкт-Петербург, 09–10 нояб. 2022 г. СПб.: Институт проблем транспорта им. Н. С. Соломенко РАН, 2022. Т. 1. С. 293–297.

9. Липатников В. А., Парфиров В. А. Структурно-параметрический метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта // Системы управления, связи и безопасности. 2023. № 4. С. 105–156.

10. Липатников В. А., Парфиров В. А., Петренко М. И. Метод и алгоритм управления ресурсами телекоммуникационной сети в интересах обеспечения требований вышестоящей системы // Региональная информатика и информационная безопасность: сб. тр. междунар. конф., Санкт-Петербург, 25–27 октября 2023 г. СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 385–389.

11. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Ч. 1. Методологические основы построения организационно-технических систем военной связи. СПб.: ВАС, 2005. 740 с.

12. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения. Учеб. СПб.: ВАС, 2008. 460 с.

13. Микони С. В. Теория принятия управленческих решений: учебное пособие для вузов. 2-е изд., испр. и доп. СПб.: Лань, 2022. 384 с.

14. Брюхомицкий Ю. А. Нейросетевые модели для систем информационной безопасности: учеб. пособие. Таганрог: Изд-во ТРТУ, 2005. 160 с.

УДК 004.7:004.422.8
ГРНТИ 28.29.01

АЛГОРИТМ ПРИВЕДЕНИЯ НЕОДНОРОДНЫХ ЗНАЧЕНИЙ ДИСКРЕТНОГО ВРЕМЕНИ КОНЕЧНЫХ ЦЕПЕЙ МАРКОВА К ОДНОРОДНОМУ ВИДУ

В. Л. Литвинов, Н. Эль Сабаяр Шевченко

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

Актуализирована задача приведения неоднородных значений дискретного времени в конечных цепях Маркова к их однородному виду. Описаны ситуации, при которых необходимо применять данный алгоритм. Раскрыты основные этапы формирования алгоритма. Разработано программное обеспечение для имитационного моделирования алгоритма. Проведены экспериментальные исследования и сравнительный анализ результатов конечной цепи Маркова с применением разработанного алгоритма для подтверждения его вычислительной правильности. Раскрыта практическая значимость применения разработанного алгоритма при моделировании вероятностных процессов на основе конечных цепей Маркова.

конечные цепи Маркова, дискретное время, временной профиль, показатели качества, неоднородность

При анализе временного профиля марковских моделей с поглощающим состоянием зачастую временная длительность перехода между состояниями не является однородным. Такая особенность может затруднять анализ априорного качества работы моделируемого вероятностного процесса.

Аналитические формализации из теории конечных цепей Маркова [1] позволяют получать развернутый временной профиль, но только при условии, что значения дискретного времени на всех переходах между состояниями равны одной единице дискретного времени.

Существуют аналитические методы, предназначенные для анализа вероятностных марковских процессов с неоднородными значениями дискретного времени, однако невозможно получать, кроме математического ожидания, расширенный статистический временной профиль моделируемого процесса.

Для решения данного вопроса разработан алгоритм, позволяющий преобразовать неоднородные значения дискретного времени Марковского процесса к их однородному виду. Благодаря данному решению обеспечивается формирование плотности распределения вероятностей дискретного времени выполнения деятельности [2], на основе которой вычисляются необходимые показатели качества, такие как дисперсия и риск срыва временного

регламента. Основные этапы получения плотности распределения вероятностей представлены в работах [3, 4].

Для обеспечения перехода к этапу формирования плотности распределения вероятностей необходимо преобразовать неоднородный Марковский граф в его однородный вид. В данном контексте временная однородность графа означает, что на всех дугах графа длительность перехода между состояниями равняется единице дискретного времени.

Для выполнения данной задачи разработан специальный алгоритм для приведения к однородному виду статистических временных характеристик и доведения их до атомарного уровня путём увеличения количества дуг до $d = t_{i,j} - 1$ при условии, что $t_{i,j} > 1$, где $t_{i,j}$ – длительность перехода между состояниями i и j , d – количество дуг.

В качестве примера преобразуем граф, представленный на рисунке 1, в его однородный вид, с вероятностным матричным описанием (1) и (2), соответственно.

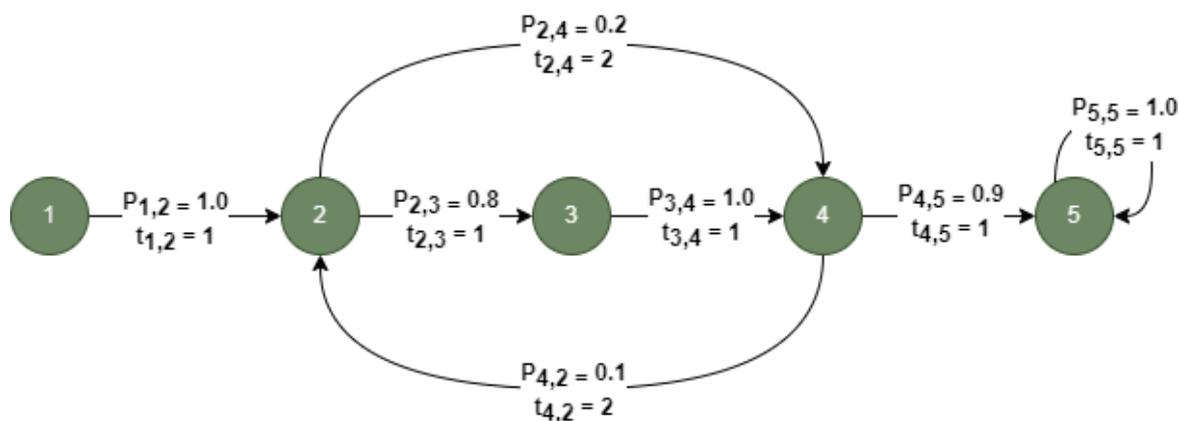


Рис. 1. Граф с неоднородными значениями дискретного времени

$$P_{i,j} = \begin{bmatrix} 0.0 & 1.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.8 & 0.2 & 0.0 \\ 0.0 & 0.0 & 0.0 & 1.0 & 0.0 \\ 0.0 & 0.1 & 0.0 & 0.0 & 0.9 \\ 0.0 & 0.0 & 0.0 & 0.0 & 1.0 \end{bmatrix}, \quad (1)$$

$$t_{i,j} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}; \quad (2)$$

где $P_{i,j}$ – вероятностное матричное описание цепи Маркова с поглощающим состоянием, $t_{i,j}$ – временное матричное описание дискретного времени к вероятностной матрице $P_{i,j}$.

Преобразование предполагает добавление новых вершин на дугах графа где $t_{i,j} > 1$. При добавлении новых вершин необходимо соблюдать следующий алгоритм действий (рис. 2):

1. Первая исходная вершина графа всегда является первой по счету в новой $P'_{i,j}$ вероятностной матрице (3).
2. Нумерация промежуточных состояний остаётся прежней согласно нумерации исходного матричного описания. Новые вершины нумеруются от $num_states+1$ до num_added_states , где num_states – количество вершин исходного графа, num_added_states количество добавленных вершин, за исключением последней вершины исходной матрицы.
3. Вероятность перехода из состояния, исходящая дуга которого содержит значение дискретного времени $t_{i,j} > 1$, сохраняет исходную вероятность. Исходящие из добавленных вершин дуги осуществляют переход в следующее состояние с вероятностью, равной $P'_{i,j} = 1.0$.
4. Последняя (поглощающая) вершина нумеруется числом N , равному количеству всех вершин $((num_states+num_added_states) + 1)$. Таким образом остаётся последней по счету вершиной.

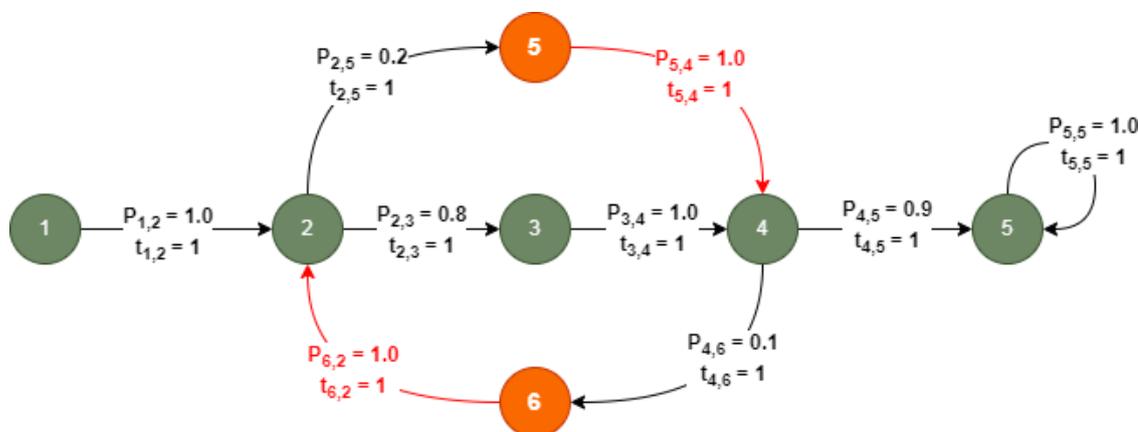


Рис. 2. Итоговый граф с однородными значениями дискретного времени. Добавлены состояния 5 и 6 с новыми переходами

Матричное описание обновленного графа имеет следующий вид:

$$P'_{i,j} = \begin{pmatrix} 0.0 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.8 & 0.0 & 0.2 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.1 & 0.9 & 0.0 \\ 0.0 & 0.0 & 0.0 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 1.0 \end{pmatrix} \quad (3)$$

Для подтверждения вычислительной правильности разработан аналитический программный инструмент на языке программирования Python, вычисляющий показатели качества исследуемого процесса. В данном случае будем ориентироваться на математическое ожидание. Вычислим точное значение среднего времени выполнения исходного Марковского графа (рис. 1) на основе матричных операций, представленных в [1]. Программное обеспечение выдает результат, представленный на рисунке 3.

```
In [13]: mean_time = solve_matrix(prob_matrix_, temp_matrix_)
         mean_time
```

```
Out [13]: 4.4444444444444445
```

Рис. 3. Результат в переменной mean_time, соответствующий среднему времени, выполнения Марковского процесса

Метод solve_matrix() предназначен для разрешения графов с неоднородными временными длительностями. Метод основан на аналитических формализациях из теории конечных цепей Маркова для последовательного исключения вершин, что позволяет находить математического ожидания среднего времени выполнения укрупнённых сегментов графа после сокращения отдельных его сегментов.

Также вычисляются приближенные значения математического ожидания среднего времени выполнения Марковского процесса нового преобразованного графа (рис. 2) с уже однородными значениями дискретного времени, на основе формализаций, представленных в работах [2–4]. На рисунке 4 изображен вывод экрана с результатом проведения имитационного моделирования.

```
get_pdd_indicators(prob_matrix_)
```

```
Длительность выполнения процесса:
- Кол-во допустимых шагов: 32
- Сумма плотностей распр. вероятностей: 0.99999999~1
- Матожидание: 4.44444408
```

Рис. 4. Математическое ожидание на основе плотности распределения вероятностей при однородных значения дискретного времени графа Марковского процесса

Метод `get_pdd_indicators()` предназначен для получения значения математического ожидания среднего времени деятельности на основе плотности распределения вероятностей [4].

Проведенное имитационное моделирование подтверждает вычислительную правильность разработанного алгоритма и аналитического инструментального средства. Представленные решения позволяют формировать и анализировать развернутые временные профили с расширенным набором показателей качества Марковских процессов на основе конечных цепей Маркова с поглощающим состоянием.

Список используемых источников

1. Кемени Д. Д., Снелл Д. Л. Конечные цепи Маркова. М.: Наука, 1970. 272 с.
2. Птицына Л. К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка ВРЕЛ: учеб. пособие / Л. К. Птицына, Н. Г. Смирнов. СПб.: Изд-во Политехн. ун-та, 2011. 105 с.
3. Птицына Л. К., Эль Сабаяр Шевченко Н. Динамический профиль сервис-ориентированных систем с адаптивным управлением их качеством // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст., под ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич. СПб.: СПбГУТ, 2019. Т.2. С. 523–528.
4. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П. Моделирование сервис-ориентированных систем в условиях неопределённости // Международная конференция по мягким вычислениям и измерениям. 2018. Секция 2. С. 291–294.

УДК 004.023
ГРНТИ 27.45.15

К ВОПРОСУ РЕШЕНИЯ ЗАДАЧИ КОММИВОЯЖЕРА В СИСТЕМАХ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ

А. Г. Любимов¹, С. А. Любимов²¹ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича² Научно-инженерный центр Санкт-Петербургского электротехнического университета

В работе показаны особенности решения прикладных задач коммивояжера эвристическими методами и алгоритмами в путевой форме. Предлагается метод послойной декомпозиции неориентированного взвешенного графа для поиска гамильтонова цикла минимального веса с применением инвариантных структур и процедуры стягивания ребер.

задача коммивояжера, гамильтонов цикл минимального веса, эвристические методы комбинаторной оптимизации, инвариантные структуры, послойная декомпозиция графа

Существует достаточно много прикладных задач, которые в формализованном виде удобно представить в постановке задачи коммивояжера (*Traveling Salesman Problem, TSP*). Принято считать [1], что в общем виде задача коммивояжера является *NP*-полной (*NP*-трудной), т. е. в настоящее время не известен точный метод ее решения с полиномиальным временем работы. В общем виде задача коммивояжера заключается в нахождении на взвешенном графе $G = (V, E, c)$ гамильтонова цикла $V_0(G) = (v_1, v_2, \dots, v_n, v_1)$ минимального веса. Вес гамильтонова цикла рассматривается как сумма весов ребер графа, входящих в гамильтонов цикл. В качестве веса ребра $c_{ij}(E)$ может рассматриваться в принципе любой показатель (расстояние, время, стоимость и т. п.).

Известные к настоящему времени методы и алгоритмы решения задачи коммивояжера можно разделить на две основные группы: точные и приближенные (эвристические), отличающиеся алгоритмической сложностью и точностью вычислений. Точные методы основаны на полном или частичном (например, метод ветвей и границ) переборе вариантов решения. В общем случае метод полного перебора дает точное решение задачи за время, пропорциональное $n!$. Очевидно, что для графов с количеством вершин $n \geq 20$ точные методы и алгоритмы полного перебора и их модификации, как правило, не находят практического применения. В связи с этим для решения целого ряда задач в постановке задачи коммивояжера используются эвристические методы и алгоритмы, позволяющие получить пусть не оптимальный, но с практической точки зрения вполне приемлемый результат. Среди известных эвристик наибольшее практическое применение находят следу-

ющие методы и алгоритмы: метод ближайшего соседа, метод минимального остовного дерева, генетические, поведенческие (роевые) алгоритмы и т.п. Разработка и применение эвристических методов и алгоритмов позволяет получать результаты решения для большинства прикладных задач коммивояжера за полиномиальное время работы.

Практически все известные эвристические методы и алгоритмы решения задачи коммивояжера основаны на поиске в полном взвешенном графе маршрута минимального веса (*разомкнутая задача коммивояжера*) от некоторой начальной вершины, выбранной произвольным образом. Считается [2], что если научиться находить на взвешенном графе гамильтонов маршрут минимального веса, то задача коммивояжера будет решена. Гамильтонов цикл при этом получается замыканием исходной вершины с последней вершиной маршрута минимального веса. Можно показать, что выбор начальной вершины произвольным образом существенно сказывается на результате решения. На рисунке 1 приведен полный неориентированный взвешенный граф, для которого выполнен поиск гамильтонова цикла минимального веса с использованием эвристического алгоритма ближайшего соседа при двух вариантах задания исходной вершины. Стрелками отмечен маршрут минимального веса. Аналогичный результат следует ожидать и при использовании алгоритма на основе минимального остовного дерева.

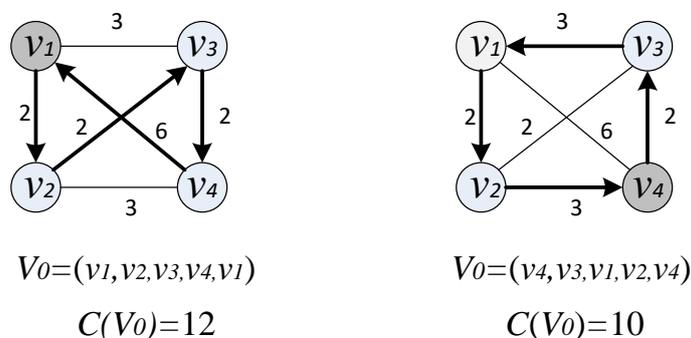


Рис.1. Расчет гамильтонова цикла минимального веса в путевой форме

Для целого ряда практических задач, решаемых в системах автоматизации и управления, точность и сложность вычислений играет весьма принципиальное значение. Поэтому разработка новых эффективных методов и алгоритмов решения задачи коммивояжера остается актуальной как с теоретической, так и с практической точки зрения.

В настоящей работе предлагается отказаться от решения задачи коммивояжера в путевой форме. В основу рассматриваемого эвристического метода положена «послойная» декомпозиция исходного графа путем выделения в каждом «слое» некоторой *инвариантной структуры*. В качестве инвариантной структуры выступает полный подграф $G_0(V, E, c)$ исходного графа с равными весами всех его ребер (рис. 2).

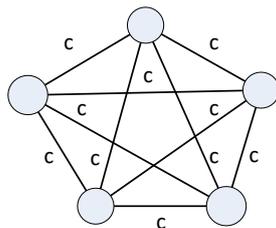


Рис. 2. Инвариантная структура полного взвешенного графа

Для представленной на рисунке 2 варианта структуры инвариантность означает, что независимо от выбора начальной вершины на симметричном графе всегда существует возможность нахождения одного из $(n-1)!/2$ гамильтонова цикла минимального веса $\min C(V_0(G))$. Каждое ребро такого графа входит в гамильтонов цикл минимального веса. Очевидно, что в результате применения любого из известных эвристических алгоритмов справедливо следующее равенство:

$$\min C(V_0(G)) = \text{opt}C(V_0(G)),$$

где $\text{opt}C(V_0(G))$ – оптимальное (точное) решение задачи коммивояжера (гамильтонов цикл минимального веса).

Утверждение 1. В любом взвешенном неориентированном полном графе можно выделить полный подграф инвариантной структуры.

Утверждение 2. Если во взвешенном неориентированном графе существует гамильтонов цикл минимального веса, то увеличение или уменьшение весов ребер на некоторое целое число не меняет структуру гамильтонова цикла минимального веса.

В общем виде задача коммивояжера формулируется для полного графа. В практических задачах связный граф, как правило, не является полным. Известно [1], что для существования гамильтонова цикла граф должен быть как минимум 2-связным (граф без шарниров). Не нарушая общности задачи достаточно дополнить неполный связный граф до полного графа ребрами с максимально большими значениями весов. Для 2-связного графа дополнение ребрами с максимальными весами не скажется на результате поиска гамильтонова цикла минимального веса.

Метод послойной декомпозиции взвешенного графа представляет собой итерационный процесс. На каждой итерации выделяется *инвариантная структура*. При удалении ее из взвешенного графа, после коррекции весов ребер, обязательно появится хотя бы одно или несколько ребер с нулевым значением веса. Такие ребра на текущей итерации (в текущем «слое») следует рассматривать как элементы гамильтонова цикла. Для перехода к следующему «слою» необходимо выполнить процедуру *стягивания* ребер с нулевыми весами. Процедура *стягивания* ребра в методах комбинаторной

оптимизации [3] заключается в замене смежных вершин на вновь организуемую вершину («мультиузел») и удалении из графа стянутого ребра. При этом появляющиеся в результате слияния вершин параллельные ребра заменяются одним ребром с суммарным весом. В результате процедуры *стягивания* получается граф меньшей размерности, а ряд ребер отсекаются на данной итерации от вхождения в гамильтонов цикл минимального веса.

Следует отметить, что процедура *стягивания* ребер в предлагаемом методе имеет принципиальное значение. Такая процедура, по сути, аналогична процедуре ветвления в методе ветвей и границ, обеспечивающей целенаправленное сокращение полного перебора маршрутов при поиске гамильтонова цикла минимального веса. Здесь выбор стягиваемых ребер направлен на преобразование взвешенного графа для определения и удаления *инвариантной структуры* и перехода к следующему «слою» выбора элементов гамильтонова цикла. В результате многократного применения процедуры *стягивания* ребер и послойного удаления *инвариантных структур* все вершины окажутся стянутыми в один мультиузел, что означает окончание поиска гамильтонова цикла минимального веса.

Приведем вербальное описание предлагаемого метода решения задачи коммивояжера.

Пусть задан полный неориентированный взвешенный граф $G_p=(V, E, c)$.

Требуется определить гамильтонов цикл $V_0(G_p)$ минимального веса $\min C(V_0(G_p))$.

1. Определяется в исходном графе $G_p=(V, E, c)$ полный подграф $G_0(V, E, c)$ с весами ребер, равными минимальному значению веса ребер исходного графа (инвариантная структура).

2. Подграф $G_0(V, E, c)$ удаляется из исходного графа и объявляется основной (базовым «слоем») поиска гамильтонова цикла минимального веса.

3. Выполняется коррекция весов ребер исходного графа $G_p=(V, E, c)$. Ребра с нулевыми весами помечаются на базовом «слое» в качестве ребер гамильтонова цикла.

4. Если на помеченных ребрах базового «слоя» получен гамильтонов цикл, следует определить суммарный вес цикла $C(V_0(G))$ и завершить расчет.

5. Выполняется процедура выбора и стягивания ребер из множества ребер с нулевыми весами графа $G_p=(V, E, c)$. Далее возврат к шагу 1.

В качестве иллюстрации на рисунке 3 показана методология послойной декомпозиции взвешенного неориентированного графа при определении гамильтонова цикла минимального веса. В приведенном примере для понимания работы предлагаемого метода послойной декомпозиции при поиске гамильтонова цикла минимального веса граф не является полным. Как уже отмечалось, дополнение графа ребрами с максимально возможными весами не влияет на конечный результат.

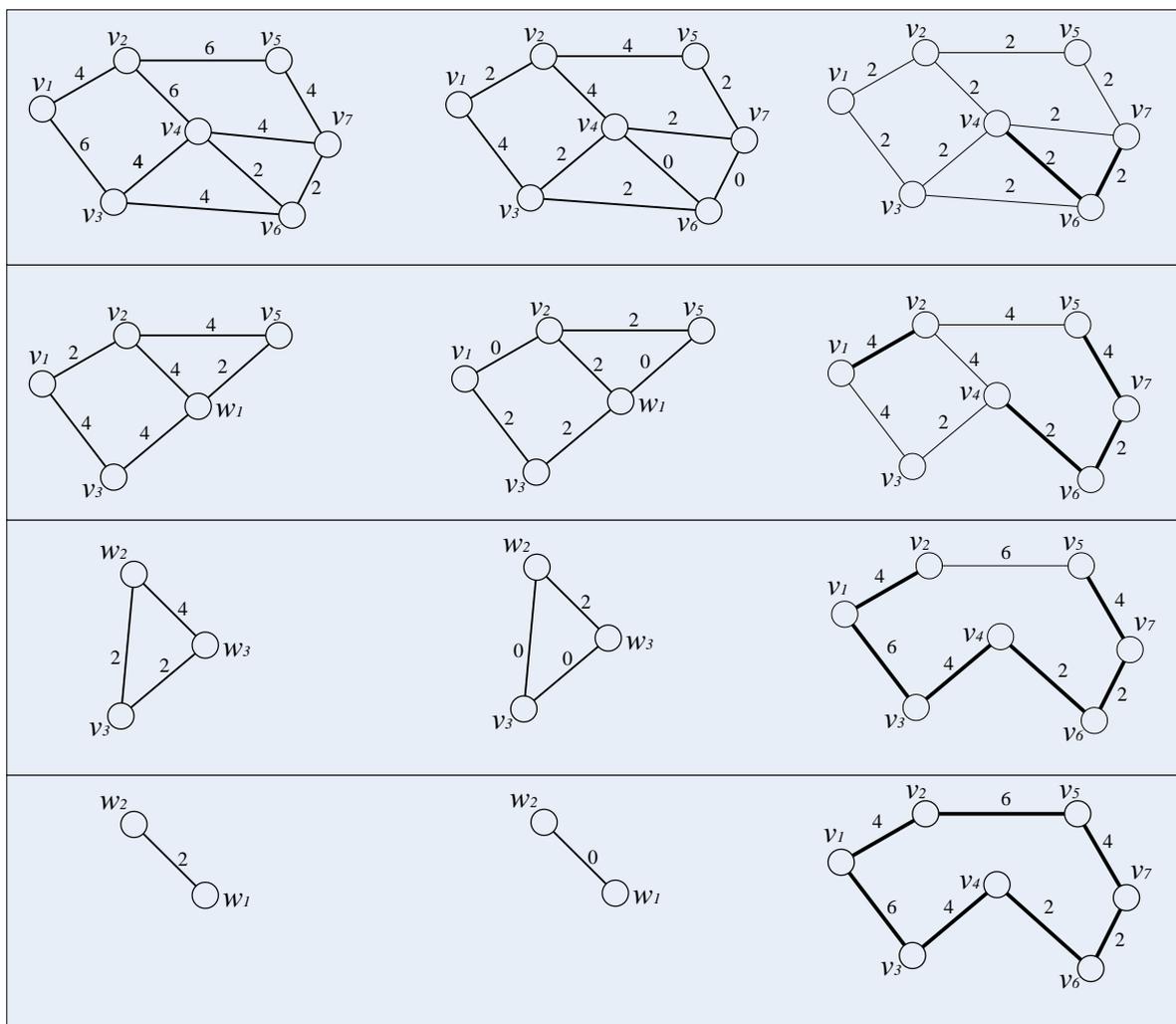


Рис.3. Пример послойной декомпозиции взвешенного графа при определении гамильтонова цикла минимального веса

В настоящей работе предложен к рассмотрению метод, альтернативный методам и алгоритмам решения задачи коммивояжера в путевой форме. В рамках настоящего метода представляется перспективными исследования и разработка алгоритмов, эффективных с точки зрения вычислительной сложности и точности для использования в системах автоматизации и управления.

Список используемых источников

1. Корте Б., Фиген Й. Комбинаторная оптимизация. Теория и алгоритмы / пер. с англ. М. А. Бабенко. М.: МЦНМО, 2015. 720с. ISBN 978 5 4439 0281 4.
2. Асанов М. О. Дискретная математика: графы, матроиды, алгоритмы: учеб. пособие / М. О. Асанов, В. А. Баранский, В. В. Расин. 3-е изд., СПб.: Лань, 2020. 364 с. ISBN 978 5 8114 4998 9.
3. Ху Т. Целочисленное программирование и потоки в сетях: пер. с англ. П. Л. Бузыцкого и др. / под ред. А. А. Фридмана. М.: Мир, 1974. 519 с.

УДК 004.514
ГРНТИ 81.95.33

АНАЛИЗ АКТУАЛЬНЫХ ПРОБЛЕМ РАЗРАБОТКИ ГРАФИЧЕСКИХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ

С. В. Максимова, Т. В. Мусаева

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

В статье проанализированы проблемы разработки графических интерфейсов веб-сайтов, мобильных приложений и информационных систем, актуальные на сегодняшний день: сложность обеспечения когнитивных свойств одного интерфейса для разных категорий пользователей; несовершенство научных знаний о человеческом мозге; малая доступность технологии айтрекинга; адаптивность интерфейсов. Сделаны выводы о возможных путях решения выявленных проблем, обозначены направления, в которых необходимо проведение исследований.

пользовательский интерфейс, графический интерфейс, юзабилити, когнитивный интерфейс, адаптивный интерфейс

С развитием информационных технологий и компьютеризации современного общества, взаимодействие графическими интерфейсами стало неотъемлемой частью нашей жизни [1]. Вследствие чего, существует необходимость в постоянном совершенствовании графических интерфейсов, чтобы они были максимально удобными, интуитивно понятными и эффективными для пользователей.

В ходе проведения анализа научной литературы по теме разработки графических пользовательских интерфейсов были выявлены несколько проблем, существующих сегодня в данной сфере:

- сложность обеспечения когнитивных свойств интерфейса для разных категорий пользователей;
- несовершенство научных знаний о человеческом мозге;
- ограниченная доступность технологии айтрекинга;
- устаревший метод адаптации интерфейсов под мобильные устройства.

Рассмотрим каждую проблему подробно.

1. Сложность обеспечения когнитивных свойств интерфейса для разных категорий пользователей.

Важным качеством графического интерфейса является его когнитивность, то есть интуитивная понятность для пользователя. В то же время, сегодня наибольшую распространенность имеют ресурсы, ориентированные на разнородные категории пользователей – мультипредметные информационные ресурсы [2]. Проблема заключается в сложности обеспечения когнитивных свойств одного интерфейса для разных категорий пользователей

вследствие различий в представлениях последних об окружающем мире (ментальных моделях).

Выходом из ситуации может служить динамическое формирование интерфейса, адаптированное под индивидуального пользователя, в данный момент использующего систему. Уже существуют информационные технологии, в той или иной мере способствующие решению этой задачи – каскадные таблицы стилей, облака тегов, и т.д. Однако упомянутые технологии решают лишь техническую задачу генерации пользовательских интерфейсов, отвечая на вопрос «как сформировать интерфейс», оставляя без ответа вопрос «каким должен быть интерфейс для данного пользователя». Также остается открытым вопрос о технологиях и способах сбора информации о пользователях. Для успешного применения технологий динамической генерации пользовательских интерфейсов необходимы четкие критерии качества интерфейса и соответствующие средства идентификации категорий пользователей. Средства выполнения данных задач могут стать технологии искусственного интеллекта, всё шире распространяющиеся в последние годы.

2. Несовершенство научных знаний о человеческом мозге.

Вся информация о повышении когнитивных и перцептивных качеств графических интерфейсов, управлении пользовательским вниманием и о других аспектах, связанных с качеством интерфейса, основана на знаниях о психофизиологии человека, особенностях человеческого мозга. Примером служат принципы Гештальта, которые были описаны в 1910-20-е годы немецкими психологами Максом Вертгеймером, Вольфгангом Келером и Куртом Коффкой, но успешно применяются при построении графических интерфейсов в настоящее время. Проблема заключается в том, что на данный момент устройство человеческого мозга всё еще остается малоизученной темой. С определённой уверенностью можно сказать – по мере изучения человеческого мозга будут совершенствоваться и графические интерфейсы [3]. Дизайнерам пользовательских интерфейсов необходимо следить за новейшими открытиями в области психологии и нейробиологии, применять каждое новое открытие для повышения их когнитивности.

3. Ограниченная доступность технологии айтрекинга.

Современная дизайнерская деятельность требует дополнительного инструментария для оценки качества графической и мультимедийной продукции, в т. ч. с психологической и эргономической точек зрения. Изучение движения глаз может определить, о чем люди думают, на основе того, куда они смотрят. С помощью когнитивных технологий возможно по миллисекундам восстанавливать, что интересовало человека, на что он посмотрел, что стало предметом его внимания [4]. Пример визуализации результатов айтрекинг-исследования веб-страницы изображены на рис. 1. Данная технология называется айтрекинг – определение ориентации оптической оси глазного яблока в пространстве. Применение технологии айтрекинга на промежуточных этапах разработки графического интерфейса способствует

получению высоких когнитивных и перцептивных качеств готового продукта. Однако, на данный момент существует проблема доступности данного вида исследования. Заказ айтрекинг-исследования веб-сайта или мобильного приложения обойдется от 50 000 рублей. Качественный айтрекер по стоимости обходится от нескольких сотен тысяч рублей. Цены на бюджетные айтрекеры начинаются от 40 000 рублей, однако в данных моделях отсутствует встроенное ПО, обеспечивающее графическую визуализацию результатов исследования, что затрудняет процесс исследования и снижает его результативность. Для обеспечения уверенного развития сферы UI/UX – дизайна необходимо повышать доступность методов айтрекинга.



Рис. 1. Визуализация результатов айтрекинг-исследования новостного портала

4. Устаревший метод адаптации интерфейсов под мобильные устройства.

Современные графические интерфейсы веб-ресурсов, как правило, имеют адаптированные версии под различные устройства: компьютеры, смартфоны, планшеты. Согласно статистике от Global Digital за 2023 год

пользователи всё чаще при выходе в интернет предпочитают смартфоны компьютерам и ноутбукам (рис. 2).

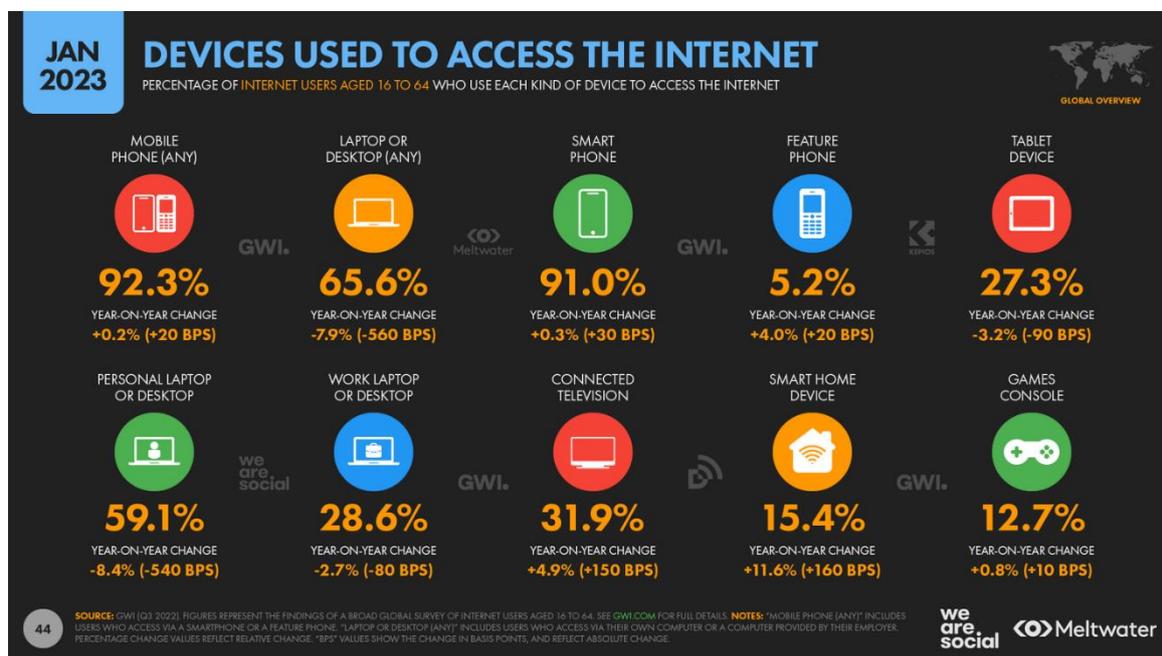


Рис. 2. Глобальная статистика интернета на январь 2023 года

С каждым годом количество таких пользователей всё увеличивается. Около 30% россиян вообще не использует компьютер для выхода в интернет. Проблема заключается в том, что построение дизайна пользовательского интерфейса веб-ресурса чаще всего начинается с десктопной версии, под которую уже адаптируется мобильная (как показано на рис. 3), являясь, по сути, вторичной. Также, зачастую, в мобильных версиях убирают анимационные и графические эффекты, задуманные дизайнером для управления восприятием пользователя, в целях экономии оперативной памяти смартфона. В современных реалиях такой подход не оправдан.

Решением проблемы может служить разработка интерфейса с мобильной версии, в дальнейшем адаптируемая под десктоп. Также, все элементы интерфейса, требующие высоких затрат оперативной памяти не должны превышать возможности мобильного устройства.

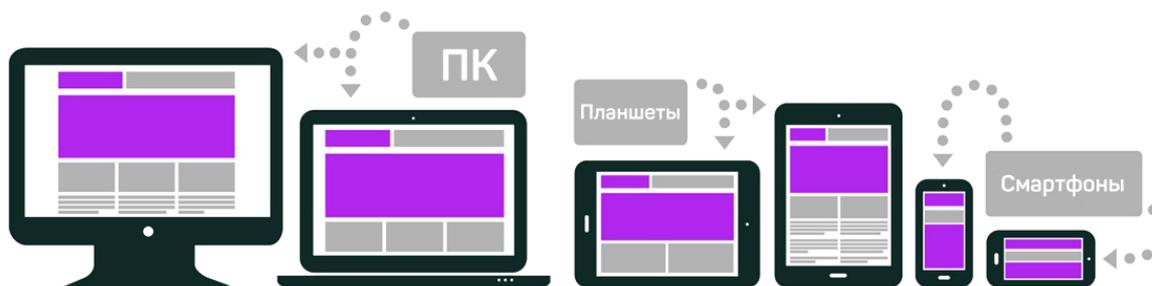


Рис.3. Классический процесс адаптации интерфейса.

Таким образом, в ходе анализа актуальных проблем разработки графических пользовательских интерфейсов были сделаны следующие выводы:

– целесообразна разработка и внедрение технологий динамического формирования пользовательского интерфейса, адаптированного под индивидуального пользователя, в данный момент использующего ресурс. Перспективным помощником в данном вопросе является искусственный интеллект.

– дизайнерам пользовательских интерфейсов необходимо работать и проводить исследования в тесной связке с психологами и нейробиологами, следить за новейшими открытиями в этой сфере.

– основное внимание при разработке большинства современных интерфейсов необходимо уделять мобильной версии интерфейса, адаптируя дизайн под десктоп, а не наоборот.

– необходимо широкое применение методов айтрекинга в разработке графических интерфейсов, в особенности на этапах промежуточных тестирований готового продукта для его дальнейшей доработки. На данный момент эта технология остаётся малодоступной.

– вероятно, основными трендами сферы UI/UX-дизайна в ближайшие годы станут: применение ИИ-технологий для динамического формирования интерфейса; непосредственное участие нейробиологов в разработке дизайна интерфейсов; мобильно-центричная разработка интерфейсов веб-ресурсов.

Список используемых источников:

1. Симонова С. С. Влияние популяризации цифрового пространства на современного человека // Научные записки молодого исследователя. 2021. №5. URL: <https://cyberleninka.ru/article/n/vliyanie-popularizatsii-tsifrovogo-prostranstva-na-sovremennogo-cheloveka> (дата обращения: 05.02.2024)

2. Шишаев М. Г. Методические основы когнитивных интерфейсов мультипредметных ИС // Труды Кольского научного центра РАН. 2015. №3 (29). URL: <https://cyberleninka.ru/article/n/metodicheskie-osnovy-kognitivnyh-interfeysov-multipredmetnyh-is> (дата обращения: 25.02.2024)

3. Подгаецкая О. Ю. Психофизиология графических пользовательских интерфейсов // Информационные технологии в науке, управлении, социальной сфере. 2016. С. 174.

4. Фазылзянова Г. И., Балалов В. В. Айтрекинг: когнитивные технологии в визуальной культуре // Вестник российских университетов. Математика. 2014. №2. URL: <https://cyberleninka.ru/article/n/aytreking-kognitivnyetehnologii-v-vizualnoy-kulture> (дата обращения: 12.02.2024)

УДК 004.056
ГРНТИ 81.93.29

СОВРЕМЕННЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ДАННЫХ

А. А. Маннанов, П. А. Шиян

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

Данная научная статья обсуждает ключевые вопросы в области кибербезопасности и методы защиты данных в современном информационном обществе. В статье рассматриваются современные вызовы и угрозы, с которыми сталкиваются организации и частные лица, и предлагаются методы и стратегии для обеспечения безопасности информации.

кибербезопасность, защита системы кибербезопасности, защита информации, информационная среда, симметричное шифрование, программа, защита данных

Понимание кибербезопасности начинается с основного предположения о том, что в киберпространстве (общее название всех онлайн-овых или электронных платформ) мы все являемся привлекательными целями для атак киберпреступников. Предполагаемыми объектами могут быть наши деньги или данные, а также имена пользователей, пароли, документы, электронные письма, присутствие в Интернете и многое другое. Большинство кибератак носят общий характер и могут случиться с кем угодно, хотя случаются и персонализированные атаки. Одной из основных и распространенных причин кибератак является человеческая ошибка. Эти инструменты могут быть как очень простыми, например, доверие к инструкциям, отправленным в электронном виде в фишинговом электронном письме, так и более сложными, например, преступники, выдающие себя за клиентов, продавцов или даже сотрудников, или специалистов, с целью получения доступа к вашим активам (как финансовым, так и другим) Поэтому существует необходимость в компьютерной безопасности против этих атак [1].

В этом разделе представлены три основные угрозы кибербезопасности, имеющие отношение к цифровой идентификации. Во время пандемии Covid-19 все больше субъектов (учреждений и организаций) были вынуждены использовать киберпространство и перешли в цифровое пространство для выполнения различных операций и транзакций. Это означает, что теперь нам нужны радикально другие и более надежные системы идентификации, поскольку наши существующие системы больше не служат или неадекватны для управления текущей безопасностью и конфиденциальностью. Цифровая идентификация включает в себя все, начиная от политики и процессов, заканчивая технологиями и системами.

Проблемы безопасности и конфиденциальности (цифровая идентификация и защита данных).

Несмотря на то, что цифровая идентификация имеет решающее значение для доверия и инноваций при использовании Интернета, граждане также обеспокоены вопросами конфиденциальности, прав человека и безопасности.

А как насчет права гражданина на неприкосновенность частной жизни и минимальное раскрытие личных данных?

Устранение страхов граждан и пользователей очень важно для развития надежной и успешной экосистемы цифровой идентификации. Если экосистема будет построена так прочно, как должна, она также решит проблему владения и контроля – это очень важно [2].

Фундаментальные понятия

Кибератаки рассматриваются в более широком контексте, чем то, что традиционно называют информационными операциями. Информационные операции комплексно используют основные возможности радиоэлектронной борьбы, психологических, компьютерных сетей, военных хитростей и операций по обеспечению безопасности в координации со специальной поддержкой и соответствующими способностями, а также для проникновения, остановки, уничтожения или захвата человеческих решений, и это один из процессов принятия решений. процессы национальных институтов. Согласно стратегии USNM для операций в киберпространстве, работа компьютерной сети состоит из обеспечения атаки, защиты и использования. Последнее отличается от сетевых атак и сетевой защиты, поскольку этот тип операций больше ориентирован на сбор и анализ информации, чем на прерывание работы сети, и сам по себе может быть прелюдией к атаке. Эти операции могут проводиться в информационно-пропагандистских целях. Операции по использованию компьютерных сетей также могут осуществляться с целью кражи важных компьютерных данных. В таком контексте Trap Sniffers и Doors являются полезными инструментами кибершпионажа. Люки позволяют внешнему пользователю получить доступ к программному обеспечению в любое время без ведома пользователя компьютера. Снифферы — это инструменты для кражи имен пользователей и паролей [3]. Последствия кибервойны могут включать следующее:

- свержение строя власти или катастрофическая угроза национальной безопасности;
- одновременное начало физической войны или задел и содействие началу физической войны в ближайшем будущем;
- катастрофическое разрушение или ущерб имиджу страны на международном уровне;

- катастрофическое разрушение или ущерб политическим и экономическим отношениям страны;
- масштабные человеческие жертвы или опасность для здоровья и безопасности населения;
- внутренний хаос;
- повсеместные нарушения в управлении страной;
- разрушение общественного доверия или религиозных, национальных и этнических убеждений;
- серьезный ущерб национальной экономике;
- масштабное уничтожение или нарушение работы национальных кибер-активов, представлена на рис.1.

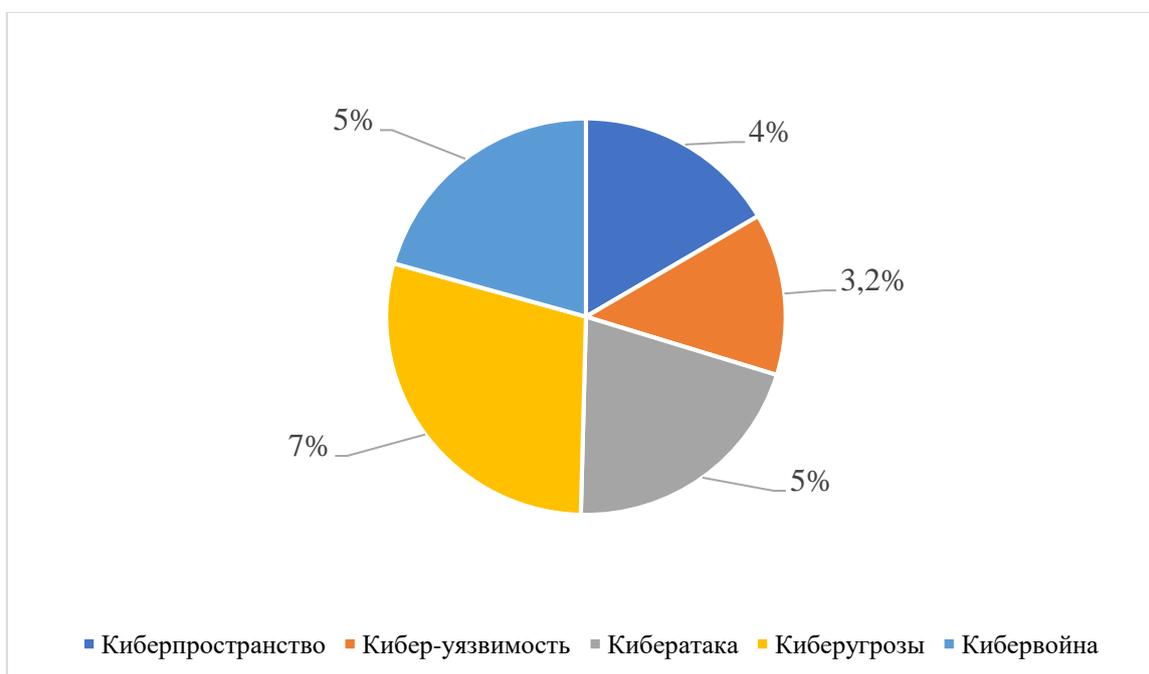


Рис. 1. Виды криптоактивов

Кибербезопасность является важным вопросом в инфраструктуре каждой компании и организации. Короче говоря, компания или организация, основанная на кибербезопасности, может достичь высокого статуса и бесчисленных успехов, поскольку этот успех является результатом способности компании защитить частные и клиентские данные от конкурента. Организации и конкуренты клиентов и частных лиц злоупотребляют. Компания или организация должны в первую очередь обеспечить эту безопасность, чтобы наилучшим образом утвердиться и развиваться. Кибербезопасность включает практические меры по защите информации, сетей и данных от внутренних или внешних угроз. Специалисты по кибербезопасности защищают сети, серверы, интрасети и компьютерные системы. Кибербезопас-

ность гарантирует, что доступ к этой информации имеют только уполномоченные лица. Для лучшей защиты необходимо знать виды кибербезопасности. На рис. 2. показаны различные типы кибербезопасности [4].

Сетевая безопасность

Сетевая безопасность защищает компьютерную сеть от нарушителей, которыми могут быть вредоносные программы или хакерские атаки. Сетевая безопасность — набор решений, которые позволяют организациям защищать компьютерные сети от хакеров, организованных злоумышленников и вредоносных программ.



Рис. 2. Триада CIA

Различные виды кибербезопасности

Безопасность приложений: использование аппаратного и программного обеспечения (например, антивирусных программ, шифрования и брандмауэров) защищает систему от внешних угроз, которые могут помешать разработке приложений.

Информационная безопасность: защищает физические и цифровые данные от несанкционированного доступа, раскрытия, неправильного использования, несанкционированных изменений и удаления.

Операционная безопасность: включает процессы и решения, принимаемые для контроля и защиты данных. Например, разрешения пользователя при доступе к сети или процессам, которые определяют, когда и где информация может храниться или передаваться [5].

Облачная безопасность: защищает информацию в облаке (на основе программного обеспечения) и отслеживает риски атак на месте.

Обучение пользователей: относится к непредсказуемым аспектам кибербезопасности, а именно к отдельным лицам. Случайно занести вирус в систему безопасности может каждый. Научить пользователя удалять подозрительные вложения в электронной почте, не подключаться к анонимным USB-накопителям и решать другие важные вопросы должно быть частью плана корпоративной безопасности любой компании.

Заключение

Киберпространство и связанные с ним технологии являются одним из наиболее важных источников власти в третьем тысячелетии. Характеристики киберпространства, такие как низкие цены на вход, анонимность, уязвимость и асимметрия, создали феномен рассеивания власти, а это означает, что любой хакер может получить доступ к конфиденциальной информации обычных пользователей. Поэтому программисты все чаще в 21 веке разрабатывают приложения и программы для защиты от хакерских атак.

Список используемых источников

1. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Журнал Вопросы кибербезопасности. 2014. №5 (8).
2. Кузнецов С. Кибербезопасность в 21 веке // Открытие системы СУБД. 2013. №5.
3. Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Massachusetts Institute of Technology. 2014. 157 p.
4. Hansen L., Nissenbaum H. Digital Disaster, Cyber Security and the Copenhagen School. University of Copenhagen, New York University // International Studies Quarterly. 2009. № 53. PP. 1155–1175.
5. Безкоровайный М. М., Татузов А. Л. Кибер-безопасность – подходы к определению понятия // Журнал Вопросы кибербезопасности. 2014. №1(2). С. 22–27.

Статья представлена научным руководителем, кандидатом технических наук, ассистентом кафедры ИКД Аль-Нами Б. А.

УДК 004.056.53
ГРНТИ 81.93.29

ОБЗОР УЯЗВИМОСТЕЙ И ТЕНДЕНЦИЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ

А. С. Матвеев, О. А. Найденов, А. И. Парамонов

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

В данной статье освещается интеграция устройств Интернета вещей в различные сферы деятельности, принеся беспрецедентное удобство и эффективность, но также приведшая к огромному количеству проблем в области безопасности. Рассматривается разнообразный спектр уязвимостей безопасности, свойственных экосистемам IoT. Изучаются факторы, такие как слабая аутентификация, уязвимости унаследованных активов, непоследовательные стандарты безопасности и разрывы между мобильными сетями и облаком. Также подробно рассматриваются известные инциденты, такие как ботнет Mirai, утечка данных о кредитных картах компании Target. Кроме того, в статье описывается целый спектр потенциальных решений - от укрепления физической защиты до внедрения надежных протоколов шифрования и использования сетевых брандмауэров. Цель данного исследования - предоставить всестороннее понимание проблем безопасности IoT и предложить жизнеспособные стратегии их устранения.

интернет вещей (iot), информационная безопасность, угроза безопасности, уязвимости iot

Интернет вещей (Интернет of Things, IoT) представляет собой концепцию, которая изменила способы взаимодействия с технологиями. Появление Интернета вещей (IoT) произвело революцию в способах взаимодействия с технологиями, подключив к Интернету огромное количество устройств и систем [1]. Однако эта взаимосвязь породила целый ряд проблем в области безопасности, подчеркивая уязвимости, присущие экосистемам IoT. Сложность этих проблем усугубляется разнообразием устройств, устаревших систем и различных стандартов безопасности, преобладающих в ландшафте IoT [2]. Старые устройства, изначально не рассчитанные на подключение к облаку, не имеют необходимых средств защиты от современных киберугроз. Устаревшие приложения часто не соответствуют современным стандартам шифрования, что делает их уязвимыми для взлома при интеграции в сети IoT [3]. Безопасность IoT еще больше осложняется отсутствием единых стандартов в отрасли. Отсутствие универсальной системы безопасности приводит к появлению различных протоколов и руководств, что затрудняет обеспечение единообразной защиты устройств IoT. Отсутствие стандартизации препятствует безопасному межмашинному обмену данными, усиливая риски в сетях IoT [4].

Обновление встроенного программного обеспечения, крайне важное для устранения уязвимостей в системе безопасности, становится проблемой при развертывании IoT. Возможность удаленного выпуска обновлений не всегда возможна из-за ограничений в скорости передачи данных по сети или возможностях обмена сообщениями. Из-за этого устройства могут быть подвержены известным уязвимостям, что представляет собой значительный риск для безопасности [5].

Разрыв между мобильными сетями и облачными приложениями представляет собой уязвимое место при передаче данных IoT. Хотя сотовая сеть и облачное приложение могут обладать индивидуальными мерами безопасности, передача данных между ними через публичный интернет создает потенциальную уязвимость и подверженность вредоносному ПО [3].

Кроме того, ограниченное управление устройствами препятствует быстрому выявлению и деактивации скомпрометированных устройств. Недостаточная видимость аномального поведения устройств или скомпрометированных состояний делает сети уязвимыми для дальнейшей эксплуатации [3].

Физические уязвимости, особенно в устройствах, которые взаимодействуют с людьми, создают возможности для несанкционированного доступа [6]. Кража SIM-карт с устройств или прямой физический доступ к оборудованию IoT создают риск утечки данных или злоумышленных действий.

Реальные примеры нарушений безопасности IoT подчеркивают серьезность этих проблем. Например, атака ботнета Mirai использовала уязвимые IoT-устройства для организации масштабных атак, которые нарушили работу основных онлайн-сервисов по всему миру [7]. Также инциденты, связанные с взломом сети Target через скомпрометированные IoT-датчики поставщика систем отопления, вентиляции и кондиционирования воздуха [8]. Такие демонстрации, как взлом автомобилей через их системы с поддержкой IoT, также являются ярким напоминанием о критической важности защиты подключенных устройств.

Однако, несмотря на эти проблемы, существуют многогранные стратегии и решения для укрепления безопасности IoT. Физические меры безопасности, такие как устойчивые компоненты и специализированное оборудование, могут защитить устройства от несанкционированного доступа. Использование таких технологий, как eSIM [9], которые являются более безопасными и устойчивыми к физическому взлому, повышает безопасность устройств. Создание надежных протоколов безопасности удаленного доступа, включая возможность блокировки функций SIM-карты для конкретных устройств и удаленного отключения соединений в случае нарушения безопасности, укрепляет основы безопасности IoT.

Развертывание частных сетей или использование собственно созданной VPN сети для создания защищенных каналов связи для IoT-устройств

снижает подверженность воздействию сетей общего доступа и потенциальный перехват передаваемых данных [10].

Механизмы обнаружения аномалий, интегрированные в облачные коммуникационные платформы, позволяют пользователям оперативно выявлять и реагировать на попытки взлома или необычную сетевую активность [10].

Блокировка IMEI, привязывающая функциональность SIM-карты к определенному идентификатору устройства, и протоколы передачи данных с шифрованием, такие как Transport Layer Security (TLS), дополнительно защищают сети IoT от несанкционированного доступа и перехвата данных [11].

Сетевые брандмауэры выступают в качестве передовых защитников, фильтруя вредоносный трафик и предотвращая его попадание в устройства и сети IoT [12]. Кроме того, использование профилей ограниченного подключения позволяет ограничить функциональные возможности устройств только основными функциями, сокращая потенциальные векторы атак.

На фоне этих проблем и решений предприятия несут ответственность за использование безопасных систем для передачи данных, а производители устройств должны уделять приоритетное внимание безопасности на уровне производства. Поставщики услуг, такие как emnify [13], предлагают набор решений, включающий VPN/IPsec, внутриоблачное соединение и встроены SIM-карты, что позволяет с самого начала защитить IoT-устройства от физических и киберугроз.

В заключение, несмотря на сложности безопасности IoT, существуют эффективные подходы и стратегии для снижения рисков. Прежде всего, важно провести аудит и устранить уязвимости в унаследованных системах, чтобы предотвратить потенциальные атаки. Внедрение надежных мер безопасности в устройствах, такие как использование устойчивых компонентов и специализированного оборудования, а также технологий, например, eSIM, помогает защитить устройства от физического и кибер-взлома.

Соблюдение строгих стандартов безопасности играет ключевую роль в формировании основы для безопасной экосистемы IoT. Создание унифицированных протоколов безопасности для взаимодействия устройств, а также обязательная поддержка современных стандартов шифрования в приложениях и устройствах, помогает предотвратить уязвимости и обеспечивает единообразную защиту.

Совмещение технологических достижений с передовым опытом требует сотрудничества заинтересованных сторон, включая производителей, предприятия и поставщиков услуг. Развитие частных сетей или использование собственной созданной VPN сети для обеспечения защищенных каналов связи для IoT-устройств помогает предотвратить несанкционированный доступ и перехват данных. Внедрение механизмов обнаружения аномалий в

облачные коммуникационные платформы позволяет оперативно выявлять и реагировать на попытки взлома или необычную сетевую активность.

Блокировка IMEI, привязывающая функциональность SIM-карты к определенному идентификатору устройства, и использование протоколов передачи данных с шифрованием, таких как Transport Layer Security (TLS), дополнительно усиливает безопасность, предотвращая несанкционированный доступ и перехват данных. Наконец, сетевые брандмауэры играют важную роль в фильтрации вредоносного трафика и предотвращении его проникновения в устройства и сети IoT.

Объединение этих стратегий и решений создает комплексный подход, который способствует укреплению безопасности IoT и защите от потенциальных опасностей в гиперподключенном мире.

Список используемых источников

1. Связь между киберфизическими системами и Интернетом вещей. 2023. URL: <https://goo.su/duehNv>
2. Проблемы безопасности интернета вещей и передовые методы их решения. 2023. URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security>
3. Информационная безопасность в IoT. 2022. URL: <https://habr.com/ru/articles/700800>
4. Интернет угроз: чем опасны для бизнеса IoT-устройства и что с этим делать. 2019. URL: <https://iot.ru/promyshlennost/internet-ugroz-chem-opasny-dlya-biznesa-iot-ustroystva-i-cto-s-etim-delat>
5. Что такое IoT и что о нем следует знать. 2021. URL: <https://habr.com/ru/companies/otus/articles/549550>
6. Угрозы информационной безопасности. 2023. URL: <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti>
7. BOTHET MIRAI. 2022. URL: <https://goo.su/VDRdW>
8. Target Hackers Broke in Via HVAC Company. 2014. URL: <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company>
9. What is an eSIM Card? 2023. URL: <https://www.pcmag.com/how-to/what-is-an-esim-card>
10. Опасности и защита IoT-коммуникаций. 2019. URL: <https://www.connect-wit.ru/opasnosti-i-zashhita-iot-kommunikatsij.html>
11. What are IMEI and TAC numbers & why do they matter. 2020. URL: <https://www.hologram.io/blog/imei-and-tac-what-are-they>
12. What is an IoT Firewall? 2023. URL: <https://goo.su/XUBTNH>
13. Emnify about us. 2023. – URL: <https://www.emnify.com/about>

ГРНТИ 20.01
УДК 004.75

РАЗРАБОТКА СЕРВИСА ДЛЯ ПОДДЕРЖКИ БЛАГОТВОРИТЕЛЬНЫХ ФОНДОВ С ИСПОЛЬЗОВАНИЕМ SMART-КОНТРАКТОВ ETHEREUM

П. В. Матвеев, Ф. В. Филиппов

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

Представлена актуальность разработки сервиса для поддержки благотворительных фондов с использованием smart-контрактов в blockchain-сети Ethereum. Описана структура сервиса поддержки благотворительных фондов. Определен стек технологий для разработки подсистем сервиса. Описан алгоритм автоматизированного сбора средств на smart-контракте и их перевода на blockchain-кошелек благотворительной организации по окончании сбора. Описана разработка интерфейса сервиса с использованием blockchain-кошелька Metamask.

благотворительность, blockchain, smart-контракт, разработка автоматизированной системы

Актуальность разработки сервиса для поддержки благотворительных фондов обусловлена недоверием людей к благотворительным фондам. Согласно статистике ВЦИОМ от 5 сентября 2022 года, 23% от тех, кто не жертвовал деньги на благотворительность, не доверяет благотворительным фондам. На рисунке 1 представлена круговая диаграмма, на которой отображено распределение причин недоверия к благотворительным организациям и фондам [1].

Согласно диаграмме, 3 основные причины недоверия благотворительным фондам:

- непрозрачность, бесконтрольность, деньги неизвестно куда уходят, нет отчетности;
- коррупция, воровство, не доходят деньги до адресата;
- мошенники, мало порядочных людей, обман, недобросовестность.

Реализация сервиса благотворительных сборов с использованием технологии Blockchain может стать ключом решения проблемы прозрачности финансовых переводов, а также позволит обеспечить безопасность и автоматизацию процесса проведения сбора. Полная открытость информации о проведенных транзакциях обеспечивает прозрачность, что повысит доверие пользователей к сервису. Также в blockchain-сетях существует консенсус – процесс подтверждения транзакций группой узлов сети, который позволит обезопасить сборы от подделки транзакций.

Для реализации выбрана сеть Ethereum, так как она популярна и имеет активную поддержку тестовых сетей. Особым преимуществом Ethereum является наличие технологии smart-контрактов – программ, размещаемых прямо в сети, целью которых является обработка проводимых транзакций [2].



Рис. 1. Распределение причин недоверия благотворительным сборам и фондам [1]

Для проведения автоматизированных сборов в smart-контракте были реализованы следующие функции:

- ввод и вывод информации о сборе: название, описание, адрес кошелька нуждающегося, собранная и целевая суммы;
- перевод суммы на smart-контракт;
- автоматизированный перевод собранной суммы на кошелек нуждающегося после набора целевой суммы;
- вывод общей суммы, переведенной пользователем.

Также было принято решение отказаться от использования одного контракта для всех благотворительных сборов, так как это увеличит число транзакций и прозрачность будет утеряна.

Важным пунктом для проведения финансовых транзакций в blockchain-сетях является выбор валюты, которую будет использовать smart-контракт. В сети Ethereum существует два основных типа валюты – токен и эфир.

Эфир (ETH, Ether) – основная валюта сети, ее использование может сильно упростить реализацию переводов для разработчика и сократить сложность контракта. Однако есть очень важная проблема, из-за которой использование ether является недопустимым для проведения долгосрочных сборов – нестабильность валюты. Цены на основную валюту сети Ethereum

слишком нестабильны и могут сильно колебаться как от времени, так и от биржи, на которой был произведен обмен. Поэтому использование эфира не рекомендуется для систем, требующих стабильной финансовой валюты.

Токены – виды активов в сети Ethereum, создаваемые пользователями. Для реализации сервиса наиболее интересными являются стейблкоины. Стейблкоин – токен, стоимость которого основана на реальной валюте и, чаще всего, эквивалентна доллару. Это позволит сервису вести наиболее уверенный учет собранной суммы и представлять ее в традиционной форме – долларах. Однако, это все еще не реальные деньги и подобный токена может либо кратковременно подешеветь или подорожать, либо полностью выйти из оборота и обесцениться, что может привести к серьезным финансовым потерям [3].

Для реализации системы был выбран стейблкоин Tether, так как он является одним из самых популярных и используемых токенов [4].

Также важным аспектом использования smart-контрактов является механизм их размещения и функционирования в сети. Любая операция в сети Ethereum требует уплаты комиссии за газ. Газ – единица стоимости выполнения операции в сети. Обычно цена газа измеряется в gwei – одной миллиардной части эфира. Также существует лимит газа – максимальное количество газа, которое пользователь сети готов оплатить [5]. Стандартный лимит газа для размещения контракта в сети составляет 3 миллиона единиц. Исходя из такого высокого лимита, можно сделать вывод, что размещение множества контрактов требует значительных затрат, что ограничивает их количество.

Были рассмотрены следующие варианты способов добавления новых благотворительных сборов:

- возможность размещения за счет организации или нуждающегося;
- включение стоимости затраченного газа в целевую сумму благотворительного сбора;
- ожидание снижения стоимости газа;
- переиспользование контрактов.

Первое решение противоречит идее благотворительной деятельности сервиса, так как вынуждает фонды или нуждающихся вкладывать деньги в работу проекта.

Второе решение позволит возмещать затраченные суммы и размещать контракты без больших дополнительных вложений. Однако размещение новых контрактов будет приостановлено при исчерпании бюджета на размещение, пока не будет покрыта стоимость одного или нескольких предыдущих контрактов.

Третье решение позволит экономить на размещении контрактов, однако приведет к очередям и глобально не решит проблему с ограниченностью бюджета.

Четвертое решение лишено дополнительных затрат на размещение, однако имеет наиболее серьезную проблему с очередями, если полностью отказаться от вложения дополнительных средств.

Для реализации данного сервиса было выбрано последнее решение, однако стоит рассмотреть возможность его объединения с другими.

Не смотря на выявленные проблемы, сервис для поддержки благотворительных фондов с использованием smart-контрактов Ethereum имеет большой потенциал развития за счет прозрачности системы переводов и использования новых технологий. Рассматриваемый сервис может существовать как самостоятельно, так и стать основой для более крупной системы. Одним из направлений развития может быть использование NFT-токенов для вознаграждения за благотворительные взносы.

Список используемых источников

1. Благотворительность в России: вовлеченность, мотивы, барьеры // ВЦИОМ. 2022. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/blagotvoritelnost-v-rossii-vovlechnost-motivuy-barery> (дата обращения: 23.02.2024)

2. Умные контракты // Ethereum.org. 2023. URL: <https://ethereum.org/ru/smart-contracts> (дата обращения: 23.02.2024)

3. Что такое Ether (ETH)? // Ethereum.org. 2024. URL: <https://ethereum.org/ru/eth> (дата обращения: 23.02.2024)

4. Стабильные монеты // Ethereum.org. 2024. URL: <https://ethereum.org/ru/stablecoins> (дата обращения: 23.02.2024)

5. Газ и комиссии // Ethereum.org 2024. URL: <https://ethereum.org/ru/developers/docs/gas> (дата обращения: 23.02.2024)

УДК 004
ГРНТИ 28.17.23

МОДУЛЬ ПОДВИЖНОСТИ НА ОСНОВЕ ПЛАТФОРМЫ СТЮАРТА

Т. В. Мусаева, К. К. Рамзаев

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

В динамично развивающемся мире появляется большое количество изделий, техники, изучение и использование которых требует специальных высококвалифицированных компетенций сотрудников. Некоторые из них относятся к источникам повышенной опасности или входят в перечень опасных устройств по назначению и функционалу, что предъявляет особые требования при их использовании и обучении. В связи с этим возникает необходимость в новом подходе с использованием современных средств и технологий, применяемым в обучении. В рамках статьи произведен анализ существующих видов устройств подвижности на основе платформы Стюарта, исследованы их системы управления. Сделанные выводы позволят разработать качественную и гибкую систему управления отечественного тренажера. Ожидаемые результаты разработки заключаются в улучшении пользовательского опыта и расширения сферы применения.

платформа Гью-Стюарта, модуль подвижности, шесть степеней свободы, система управления, средство управления тренажером

Платформа Гью-Стюарта – разновидность параллельного манипулятора, в которой используется октаидерайдальная компоновка стоек. Платформа Гью-Стюарта имеет шесть степеней свободы. Механизм устройства, представленный на рисунке 1 имеет шесть независимых ног на шарнирных соединениях. Длины ног можно изменять и, тем самым, можно изменять ориентацию платформы.

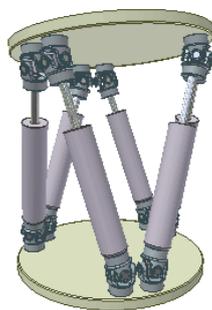


Рис. 1. Платформа Гью-Стюарта

Основная задача тренажёров на основе платформы Стюарта заключается в имитации зрительных и тактильных ощущений, соответствующих физиологическим процессам, возникающим при реальном использовании

различной техники. В настоящее время существует множество различных тренажеров на данной платформе. Важной составляющей подобных тренажеров является модуль имитации движения, который обеспечивает динамическое воздействие на обучаемого [1].

Для анализа были выбраны несколько моделей тренажеров, таких как:

1. PS-6TM-150.
2. PS-6TM-550.
3. 6DOF Motion 1000.
4. SKAS W6s.
5. 6DOF Module AST-1.

Модель PS-6TM-150, самая младшая модель из линейки 6-степенных модулей компании «Motion Systems», представлена на рисунке 2(а).

Область применения устройства PS-6TM-150:

- небольшие авиационные симуляторы;
- симуляторы для индивидуальной тренировки вождения;
- военные и промышленные симуляторы малых и средних размеров;
- симуляторы развлечений для одного пользователя.

На рисунке 2(б) представлена модель PS-6TM-550 – следующая модель компании «Motion Systems».



Рис. 2. а) Модель PS-6TM-150; б) Модель PS-6TM-550

Сферы применения устройства PS-6TM-550:

- авиационные симуляторы средних и малых размеров;
- тренажеры для обучения вождению (для двух человек);
- военные и промышленные симуляторы средних и малых размеров (для двух человек);
- развлекательные симуляторы (для двух человек).

Компания предоставляет систему управления – специализированное приложение «ForceSeatPM» (программное обеспечение), которое может управлять только платформами «Motion Systems». Данное приложение включает в себя множество модулей, которые упрощают пользование тренажерами: диагностика платформы, конфигурация компенсации движения, конфигурация подключения, интеграция игр и диагностика кинематики [2].

На рисунке 3 представлен классический вариант модели гексапода 6DOF Motion 1000, разработанной компанией «Brunner». В данной модели используются линейные актуаторы в качестве основных приводов.



Рис. 3. Модель 6DOF Motion 1000

Сферы использования устройства 6DOF Motion 1000:

- симуляторы для военных;
- авиационные симуляторы различных размеров;
- автомобильные симуляторы различных размеров;
- развлекательные симуляторы,
- испытательные стенды.

У компании «Brunner» также разработано программное обеспечение для собственных платформ, представленное на рисунке 4, которое позволяет настраивать конфигурацию движения для тренажера [3].

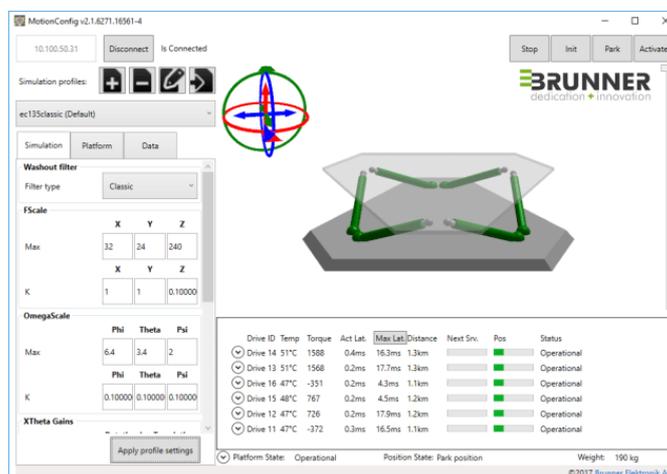


Рис. 4. Программное обеспечение компании «Brunner»

Модель SKAS W6s, представленная на рисунке 5, позиционируется как готовое решение для OEM – производителей (original equipment manufacturer), а также для домашнего использования.

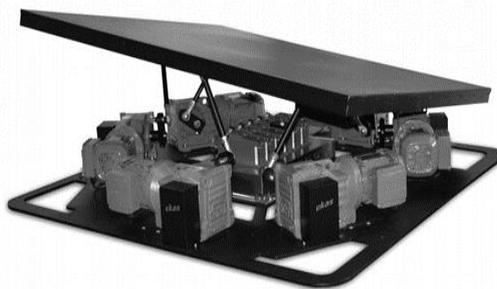


Рис. 5. Модель SKAS W6s

Область применения устройства SKAS W6s:

- компактные автомобильные и авиационные симуляторы;
- тренажеры для практики навыков вождения;
- военные и промышленные симуляторы небольших и средних размеров;
- развлекательные симуляторы.

Конкретная информация о системе управления платформами компании «СКАС» отсутствует [4].

На отечественном рынке представлена разработка тренажера 6DOF Module AST-1 компанией ООО «Автономные системы» г. Санкт-Петербург, представленная на рисунке 6.

Сферы применения отечественного тренажера:

- игровая индустрия;
- киноиндустрия;
- лабораторные исследования.

Доступной системы управления в данной модели для пользователей на данный момент нет [5].

В состав модуля, входит нижняя (неподвижная) рама (поз. 1), группа приводов (поз. 3), верхняя (подвижная) рама (поз. 2). Верхняя и нижняя рамы модуля связаны шестью приводами и системой уравнивающего механизма (поз. 4). Также в состав модуля входит блок управления (поз. 5), содержащий контроллер формирования сигналов на драйвере шаговых двигателей, а также непосредственно сами драйвера. Угловое положение рычага актуатора определяет общее положение верхней рамы модуля.

Проанализировав устройства подвижности иностранных компаний и отечественную разработку, можно сделать выводы:

- все подобные тренажеры имеют схожие сферы применения;
- все они моделируют реальную эксплуатацию дорогостоящей и опасной техники;
- у иностранных тренажеров, у которых уже есть собственные системы управления, сфер применения больше за счет удобства их эксплуатации.



Рис. 6. Модель 6DOF Module AST-1

Иностранные устройства кажутся более развитыми, но стоят очень дорого, на сегодняшний день отечественная разработка выглядит перспективней в условиях импортозамещения. Исходя из этого имеет смысл разработка системы управления для отечественного тренажера в форме веб-приложения, что позволит пользователям обращаться к ней через веб-браузер. Использование такого подхода позволит:

- отказаться от привязки к определенной операционной системе;
- увеличить быстродействие приложения;
- улучшить функционал;
- расширить сферы применения.

Такой подход позволит внедрить в систему управления новый функционал, который будет включать в себя отображение пульса пользователя и анализ его изменения при использовании тренажера, отображение перегрузок, а также может содержать такие же функции, как в приложениях иностранных компаний, но с усовершенствованным интерфейсом. Данное решение позволит улучшить пользовательский опыт и расширит сферы применения, например, использование тренажера для подготовки космонавтов, для отработки экстремальных маневров в автошколах, для обучения военнослужащих управлению военной техникой.

Список используемых источников

1. Терехин Н.А. Система управления манипулятором с шестью степенями свобод. Платформа Гью-Стюрта / Камленок Т.В. // Решетневские чтения: материалы XIV междунаучной конференции в 2 частях. Часть 1. (Красноярск, 10 – 12 ноября 2010 г.). Красноярск: изд-во Сибирского ГАУ им. академика М. Ф. Решетнева, 2010. С. 334–335.
2. MotionSystems. URL: <https://motionsystems.pl/> (дата обращения: 14.03.2024)
3. BRUNNER. URL: <https://www.brunner-innovation.swiss> (дата обращения: 14.03.2024)
4. CKAS. URL: https://www.ckas.com.au/Home_1.html (дата обращения: 14.03.2024)
5. OPTIMOTION6. URL: <https://optimotion.ru> (дата обращения: 14.03.2024)

УДК 004.514
ГРНТИ 20.23.19

АНАЛИЗ ПРОБЛЕМ И ОСОБЕННОСТЕЙ ПЕРСОНАЛИЗАЦИИ ОНЛАЙН-ОБРАЗОВАНИЯ

Т. В. Мусаева, П. А. Титов

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

В статье рассматривается вопрос применения метода персонализированного выбора образовательного курса в онлайн формате с учетом индивидуальных потребностей человека. Проведено исследование, осуществлен анализ российского рынка и популярных платформ онлайн-образования, предлагаемых инструментов, актуальных трендов и перспективных направлений развития. Выявлены основные проблемы и предложения по их решению. Также, исследованы основные индивидуальные и когнитивные особенности человека для определения их влияния на эффективность результата обучения. На основании сделанных выводов предложен метод выбора персонализированных онлайн-курсов с учетом индивидуальных особенностей студентов.

Ключевые слова: онлайн-образование, подбор курсов, индивидуальные особенности, персонализация образования, агрегаторы курсов

Сегодня онлайн-образование становится важнейшей частью системы образования как в России, так и во всем мире. Внедрение и развитие онлайн-образования становится приоритетной задачей государственной образовательной политики, поскольку оно обеспечивает гибкость и доступность в обучении, а также способствует лучшей адаптации к современным вызовам, таким как пандемия или быстро меняющиеся требования рынка труда.

Несмотря на широкое разнообразие учебных материалов, выбор подходящего курса остается сложной задачей. В условиях конкуренции многие платформы предлагают стандартизированные программы, пренебрегая персонализацией для отдельных учеников. Тем не менее, вопрос индивидуального подхода к обучению остается достаточно важным, ведь чем больше курс адаптирован для конкретного ученика, тем выше его эффективность обучения и степень удовлетворенности результатами, выше уровень лояльности к образовательной платформе, что в конечном итоге повышает доходность компании. Следовательно, возникает потребность разработки метода персонализации онлайн-курсов без значительных издержек и изменения формата обучения.

Недавний анализ российского рынка онлайн-образования в 2021 году показал, что более 18 млн. россиян прошли обучение в дистанционном формате, на 6 миллионов превысив число очных студентов за тот же период [1].

График изменения общей выручки рынка за 2022-2023 год представлен на рисунке 1.

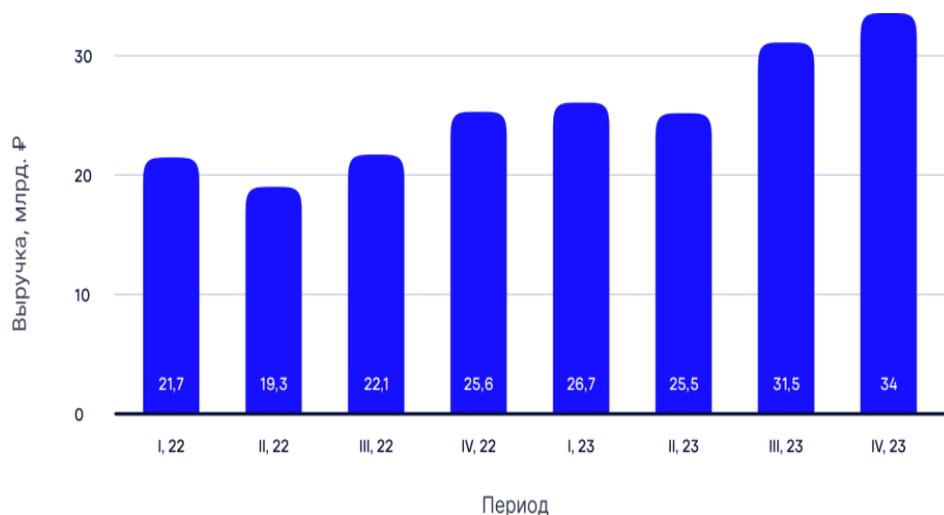


Рис. 1. Объем рынка онлайн-образования за 2022–2023 годы

По мере расширения аудитории образовательных платформ, растет уровень осведомленности пользователей и их понимания цифровых продуктов. Такое повышенное внимание к образовательным программам приводит к росту количества стандартов и требований к ним. Онлайн-школы сталкиваются с необходимостью обновлять свои продукты, повышая качество материалов и образовательной среды, чтобы сохранить свои позиции на рынке. Кроме того, растет спрос на разработку индивидуальных программ обучения, предназначенных для крупных корпораций. Переживая кризисные времена, компании признают необходимость массовой переподготовки сотрудников, и онлайн-образование становится оптимальным инструментом для усиления команды и повышения финансовых результатов [2].

Таким образом, рынок онлайн-образования переходит к конкуренции за качество. Эксперты прогнозируют усиление государственного регулирования в сфере цифрового обучения в ближайшие годы [1]. Ожидается, что изменения в регулировании начнутся в сфере детского онлайн-обучения, а затем затронут и образование для взрослых.

Одним из важнейших шагов в развитии образования является персонализированный подход к процессу обучения. В образовательном процессе принцип персонализации способствует раскрытию личностного потенциала ученика за счет четко подобранной структуры учебной программы, учитывающей комплекс персональных параметров ученика и его уровень подготовки. В контексте электронного обучения концепция персонализации также становится глобальным трендом. Исследование, проведенное американским консорциумом новых медиа, выделяет персонализацию как актуальную сложную проблему высшего образования [3]. Растущий интерес к

персонализации со стороны учащихся объясняется желанием индивидуального подхода к их запросам, а также повышенной потребностью в производительности и комфорте при освоении новых навыков. Преподаватели, отвечая на растущий спрос, внедряют электронные инструменты персонализации, что способствует усилению образовательного процесса.

В статье «Средства персонализации образовательного процесса в рамках электронных курсов» автор выделяет ряд принципов, на которые целесообразно опираться для реализации эффективных средств персонализации электронного обучения [4]:

- использование входной дифференциации контингента обучающихся;
- избыточность и вариативность содержания;
- высокая интерактивность и мультимедийность контента;
- большое разнообразие форм представления информации;
- разнообразие контрольно-измерительных материалов, в т.ч. с автоматической проверкой;
- интуитивно понятный интерфейс;
- наличие дополнительных инструментов и сервисов.

Одним из популярных методов персонализации является концепция адаптивного обучения. Данный подход нередко применялся в образовательных системах разных стран, в том числе и в России. Подобная методика была разработана и протестирована для курса «Общая химия» в МИСиС, что привело не только к улучшению успеваемости студентов, но также "выровняло" различия в их уровнях знаний.

Работа адаптивных образовательных систем строится на использовании двух основных источников данных: модели предметной области и модели студента.

Модель предметной области включает информацию о темах, проектах и других элементах учебного материала. Система создает связи между различными элементами дисциплины, обеспечивая переход между ними.

Модель студента включает в себя текущие знания ученика, информацию о его методах обучения (ошибках, скорости выполнения заданий и др.) и характеристики личности (предпочтения, степень мотивации).

Процесс адаптации может затрагивать различные объекты. Например, компания Pearson в своем отчете «Decoding Adaptive» приводит пример классификации на основе контента, системы тестирования и порядка представления материалов [5].

Однако существуют трудности и недостатки данного подхода. На основании опыта работы нескольких образовательных организаций, выстраивающих адаптивную образовательную систему, выявлен ряд проблем, таких как риск неправильного понимания потребностей учащихся из-за ошибок в

обработке данных, высокие затраты на создание таких систем, невозможность полного учета индивидуальных особенностей пользователей, противоречие между индивидуальным подходом и общим стилем персонализации, а также уменьшение способности учащихся к самоорганизации при использовании адаптивных систем [6].

Тем не менее, и исследователи, и представители бизнеса сходятся во мнении, что за адаптивным обучением будущее. Открытым остается лишь вопрос наиболее безболезненного, массового и экономически выгодного внедрения данной технологии в привычные образовательные системы. Учет личностных и когнитивных особенностей человека в персонализации образования является одним из ключевых факторов, так как они существенно влияют на эффективность онлайн-обучения, особенно в контексте целенаправленного поведения, регулирования активности и управления временем [7]. Среди основных особенностей, влияющих на процесс обучения выделяют уровень подготовки, предварительные знания, стиль и темп обучения, интересы и мотивацию, а также особенности здоровья и специальные потребности.

Помимо перечисленных особенностей следует также учитывать когнитивные стили восприятия информации, имеющие непосредственное отношение к процессу усвоения информации и формированию навыков. М. А. Холодная в своем учебном пособии выделяет следующие стили [8]:

- полезависимость и полenezависимость;
- рефлексивность и импульсивность;
- ригидность и гибкость;
- узость и широта диапазона эквивалентности;
- уровень толерантности к нереалистическому опыту и другие.

Таким образом, для достижения комфортной среды обучения, в дальнейшей разработке метода персонализации онлайн-курсов необходимо учитывать выявленные критерии.

С целью выявления интерфейсных решений с точки зрения подачи учебного материала, а также уровня персонализации обучения, исследованы 10 наиболее популярных платформ онлайн-образования.

Образовательные платформы чаще всего предлагают текстовый и видео форматы для обучения. Текстовый формат обладает большей доступностью и удобством, но менее нагляден по сравнению с видео-форматом. Видео-уроки обеспечивают более наглядную визуализацию учебных материалов и делают процесс обучения более интересным и запоминающимся. Однако у видео есть недостатки, такие как отсутствие возможности копирования информации. Для решения этой проблемы к некоторым видео добавляется текстовое описание. Навигация по видео также может быть затруднительной. Кроме того, видео-уроки могут быть недоступны для слушателей с ограниченными возможностями.

Не менее важным вопросом при реализации цифровых образовательных программ является степень усвоения информации студентом. Вне зависимости от выбора формата подачи, у студента могут возникнуть проблемы с усвоением материала. Для решения данной проблемы онлайн-школы используют разнообразные инструменты, например, тестирование после прохождения урока, включающее небольшое количество вопросов по изучаемой теме.

Помимо проверки остаточных знаний после урока, тестирование может содержать вопросы об эмоциональном состоянии студента. Платформа «Skillfactory» предлагает ученикам выбрать положительные и отрицательные состояния из списка. Данная информация может быть использована в рекомендательных системах платформы или системах мотивации учащихся.

Поддержание уровня вовлеченности и интереса студентов – не менее важных параметр, на который следует обратить внимание. Платформы онлайн-образования применяют различные методы и инструменты для создания динамичной и мотивирующей онлайн-среды. Например, платформа «Учи.ру» предлагает прохождение обучающих материалов в игровом формате. Данное решение позволяет повысить интерес к обучению для детей и подростков, однако не подходит для взрослой целевой аудитории. Более универсальным решением является введение системы достижений и вознаграждений, когда учащиеся получают условные очки за выполнение определенных действий.

На основании анализа популярных образовательных платформ выделены основные механизмы и инструменты, связанные с персонализацией обучения. Безусловно, данные решения способствуют созданию более комфортной и доступной среды обучения. Однако, для обеспечения полноценного персонализированного образования этого недостаточно.

Таким образом, в результате проведенного исследования выявлена проблема отсутствия механизмов персонализации электронного обучения, учитывающих индивидуальные параметры студентов.

На основании научных работ и прикладного опыта образовательных учреждений, обоснована необходимость разработки универсального, массового и экономически выгодного метода персонализации онлайн-курсов под индивидуальные потребности и возможности обучающегося. Суть метода заключается в автоматическом подстраивании формата отображения учебных материалов в зависимости от персональных параметров, заданных пользователем.

Список используемых источников

1. Исследование рынка онлайн-образования. Нетология. URL: https://netology.ru/edtech_research_2022 (дата обращения: 17.01.2024)

2. Суслов И.Д. Перспективы развития российского рынка онлайн-образования в эпоху санкционного кризиса // Вестник Московского городского педагогического университета. Серия: Экономика. 2022. С. 92.

3. Johnson L., Adams Becker S., Cummins M., Estrada V., Freeman A. and Hall C., NMC Horizon Report: 2016 Higher Education Edition // The New Media Consortium. 2016. С. 10.

4. Прохорова М. П., Шкунова А. А., Гуреева Е. П. Средства персонализации образовательного процесса в рамках электронных курсов // Проблемы современного педагогического образования. 2021. С. 185

5. Decoding Adaptive // Pearson, EdSurge. 2021. С. 46.

6. Грачева А. П., Грачева Н. Н. Потенциал и проблемы организации адаптивного обучения на основе использования современных средств информатизации // Вестник Московского городского педагогического университета. Серия: Информатика и информатизация образования. 2015. С. 24.

7. Истратова О. Н., Лызь Н. А. Индивидуальные особенности студентов как фактор эффективности онлайн-обучения // Азимут научных исследований: педагогика и психология. 2020. С. 329.

8. Холодная М. А. Когнитивные стили. О природе индивидуального ума: учебное пособие. 2004. С. 45.

УДК 007.52
ГРНТИ 28.19

ЗАДАЧА ГРУППОВОГО УПРАВЛЕНИЯ, МЕТОДЫ ЕЕ АНАЛИЗА И РЕШЕНИЯ

Е. А. Новиков

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

Рассматривается задача управления группой (роем) агентов. С целью описания предметной области задачи приводится систематизация условий задачи, описываются распространенные методы анализа решений и подходы к решению рассматриваемой задачи. В частности, приводится таксономия, позволяющая разделить различные постановки задач группового управления; описываются методы анализа готового решения; приводятся подходы, реализующие групповые поведения, необходимые для успешного группового управления.

задача группового управления, управление роем, рой роботов, групповая робототехника, мультиагентные робототехнические системы, многоагентная система

Задача группового управления является одной из актуальных задач области робототехники и заключается в определении алгоритма поведения каждого робота группы, который бы позволил достичь всей группе некоторого результата при определенных условиях. В связи с процессами внедрения в экономику робототехнических комплексов, состоящих из множества отдельных роботов, нетрудно заметить необходимость в такой задаче. Говоря точнее, существует потребность в системах, включающих в себя большое число простых мобильных объектах, способных самостоятельно принимать решения на основе собственных расчетов и взаимодействия друг с другом, и достигающих таким образом единой цели [1].

В отличие от задачи управления одним роботом, у задачи группового управления имеются следующие характерные особенности [2]:

- автономность;
- взаимодействие со средой;
- восприятие лишь локальной информации о среде (не знают полного состояния среды);
- отсутствие возможности управления единым устройством и хранения информации в едином хранилище;
- осуществление кооперацию для достижения поставленной задачи.

В связи с большим числом потенциальных применений и различными вариантами постановки данной задачи, правильно будет использовать понятие «класс задач группового управления».

Данная работа направлена на полноценное описание предметной области класса задач группового управления. В частности, в данной работе рассматриваются условия, влияющие на постановку задачи, подходы к решению задачи группового управления, методы анализа решений, а также частные «поведения» коллектива роботов, позволяющие решать определенные подзадачи при решении самой задачи.

Данная работа представляет собой анализ имеющихся работ в области групповой робототехники. Целью работы является описание предметной области задачи группового управления, позволяющее структурированно выделить используемые основные методы, подходы, модели и алгоритмы. Объект исследования данной работы – задача группового управления. Предмет исследования – методы, подходы, модели и алгоритмы, используемые для анализа и решения задачи группового управления.

Говоря о постановке задачи группового управления, необходимо заметить, что условия, в которых оперируют роботы, играют критическую роль при решении задачи [3]. Различные условия приведут к решительно различающимся постановкам задачи и, соответственно, потребуют различных решений; при этом, эти задачи будут одновременно являться задачами группового управления.

В таблице 1 приведены виды условий, влияющих на постановку задачи группового управления [3, 4].

ТАБЛИЦА 1. Виды условий в задачах группового управления

Условие	Описание	Классы условий
Размер коллектива	Число независимых агентов в коллективе	1 агент, пара агентов, ограниченное число агентов, неограниченное число агентов
Радиус связи	Максимальное расстояние, на котором агенты в коллективе могут передавать информацию	Радиус 0, радиус ограничен, радиус неограничен
Топология связи	Информация о том, какие из агентов могут передавать информацию друг другу в пределах радиуса связи	Широковещательная связь, связь по адресу, связь на основе графа
Пропускная способность связи	Количество единиц информации, передаваемых между агентами	Бесконечная пропускная способность, пропускная способность мала, пропускная способность 0

Условие	Описание	Классы условий
Изменение конфигурации коллектива	Возможность изменения состава коллектива	Фиксированная топология, топология изменяется по определенному алгоритму, топология изменяется динамически
Вычислительная способность агентов	Вычислительная модель, используемая каждым отдельным агентом	Конечный автомат, машина Тьюринга
Состав коллектива	Информация о том, идентичны ли агенты между собой	Гомогенный коллектив, гетерогенный коллектив

Стоит заметить, что разделение на классы является весьма условным. Несмотря на это, оно позволяет определить постановку конкретной задачи группового управления достаточно точно, а также позволяет осуществлять классификацию различных задач в классе задач группового управления.

На рисунке 1 приведена классификация подходов [2, 5], используемых для разработки многоагентных моделей, являющихся решением конкретной задачи группового управления.

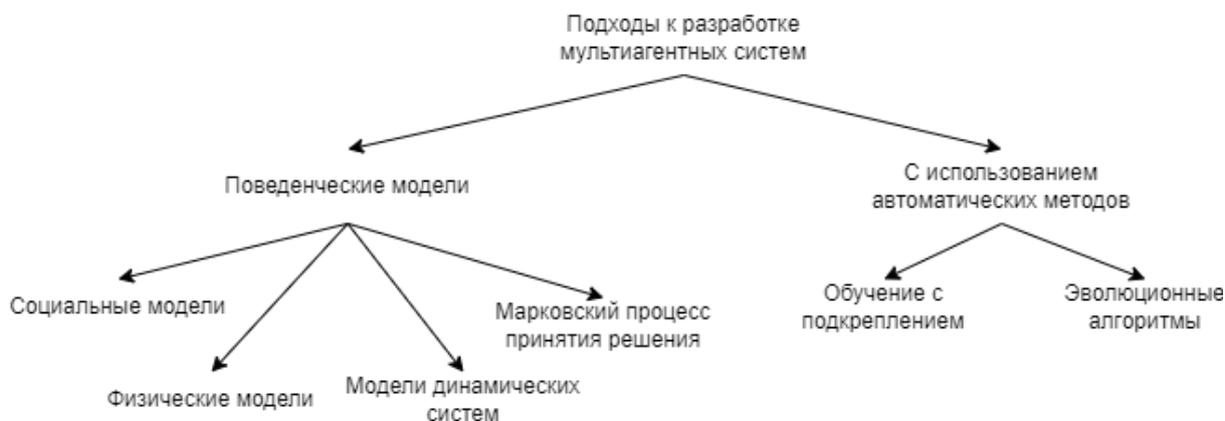


Рис. 1. Подходы решения задачи группового управления

Заметим, что данная классификация является условной, поскольку некоторые виды используемых моделей затруднительно отнести к какой-либо из приведенных категорий [2].

На рисунке 2 приведена классификация методов анализа многоагентных моделей, являющихся решением конкретной задачи группового управления [2].



Рис. 2. Методы анализа решений задачи группового управления

На рисунке 3 приведена классификация видов групповых поведений, которые осуществляются коллективом агентов при решении различных реализаций задачи группового управления [2, 6].



Рис. 3. Виды групповых поведений в задаче группового управления

Из приведенного рассмотрения предметной области можно сделать выводы об обширности задачи группового управления. Данная работа позволяет получить общую информацию о вариантах постановки задачи, о подходах к решению задачи и к анализу имеющихся решений, а также об используемых при решении групповых поведениях в коллективе агентов. Данная работа может использоваться в качестве отправной точки для погружения в предметную область задачи группового управления.

Список используемых источников

1. Зикратова Т. В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 92–100.
2. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective // Swarm Intelligence. 2013. № 7. С. 1–41.
3. Dudek G., Jenkin M., Milios E., Wilkes D. A taxonomy for multi-agent robotics // Autonomous Robots. 1996. № 3. С. 375–397.
4. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с. ISBN 987-5-9221-1141-6.
5. Spears W., Spears D. Physicomimetics: Physics-based swarm intelligence. Berlin: Springer, 2012. 646 с. ISBN 978-3-642-22803-2.
6. Schranz M., Umlauf M., Sende M., Elmenreich W. Swarm Robotic Behaviors and Current Applications // Frontiers in Robotics and AI. 2019. № 7. С. 1–33.

Статья представлена научным руководителем, профессором кафедры ИУС СПбГУТ, доктором технических наук, профессором И. А. Зикратовым.

УДК 004.02
ГРНТИ 50.41.23

DLP-СИСТЕМА КАК ИНСТРУМЕНТ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

А. У. Паскенова

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

На сегодняшний день в связи с повышением количества случаев утечки информации и нарушения ее целостности со стороны сотрудников становится очень актуальной тема защиты от угроз в сфере информационной безопасности. В дополнении к этому большинство предприятий и компаний переходят в разряд оборонно-промышленного комплекса, что делает данную тему еще более актуальной. Кроме того, для формирования качественного нормативно-правового поля необходимо достаточно тщательное и качественное формирование судебной практики в области защиты информации. В решении всех поставленных задач используются DLP-системы, которые, в свою очередь, выполняют роль и функции защиты информации от угроз, инструмента расследования инцидентов, а также формирования типовых инцидентов для предоставления возможности дальнейшего расследования и формирования модифицированного правового поля.

DLP-системы, расследование информационных инцидентов, анализ и перспективы их развития

Системы контроля и предотвращения утечек данных (DLP) становятся все более важным компонентом стратегии информационной безопасности в современных организациях. Одним из ключевых аспектов их применения является использование DLP-систем в качестве инструмента для расследования информационных инцидентов, которые могут привести к серьезным последствиям как для организаций, так и для частных лиц. В данной статье мы рассмотрим роль DLP-системы в расследовании различных инцидентов, также ее возможности и перспективы развития.

DLP-системы играют важную роль в обнаружении, мониторинге и предотвращении утечек конфиденциальной информации. Они предоставляют организациям возможность:

– мониторинга передачи данных: DLP-системы непрерывно отслеживают информационный поток во входящем, исходящем и внутрикорпоративном трафиках, также передачу информации на неподтвержденные устройства, тем самым обнаруживая потенциальные утечки;

– анализа и классификации данных: благодаря автоматической классификации данных по степени конфиденциальности, которая осуществляется DLP-системами, появляется перспектива выявления несанкционированной передачи информации;

– блокирования утечек: при обнаружении подозрительной активности система может немедленно заблокировать передачу данных, предотвращая утечку. В дополнении к этому, система поставит в известность специалиста безопасности;

– сбора доказательств: логи и аудиторские данные, собранные DLP-системой, могут быть использованы в расследовании информационных инцидентов и в судебных процессах, в качестве прямых доказательств нарушения политик безопасности каким-либо пользователем. Данные DLP-системы представляют собой записи с информацией о действиях пользователей, обнаруженных угрозах, действиях пользователей с данными или информацией, а также о попытках доступа к защищенным ресурсам [1].

Приведем в пример сценарий, где DLP-система обнаружила попытку несанкционированной передачи конфиденциальных документов через электронную почту. Именно благодаря DLP-системе, которая провела сбор логов и аудиторских данных, мониторинг исходящего потока трафика, блокировку передачи информации и уведомила офицера безопасности о попытке несанкционированной передачи документа, удалось не только оперативно предотвратить передачу данных, но и собрать необходимые доказательства о том, что произошло, кто был вовлечен и какие данные были скомпрометированы, что являлось ценной информацией для последующего расследования и принятия мер.

Помимо основных возможностей DLP-системы имеют ряд расширенных возможностей, которые активно используются при расследовании инцидентов и приносят существенную пользу в выявлении несанкционированной передачи конфиденциальных данных или ее попытке [1]. Представлены некоторые из них:

– подсистема «Краулер», позволяет выполнять проверку файлов в корпоративной сети на предмет нарушения корпоративных политик безопасности (проверка файлов выполняется с помощью сканера – специального модуля, сканирующего места хранения информации);

– детекторы содержания и шаблоны правил: предоставляют возможность распознавать договоры, идентификационные номера различных документов и иную конфиденциальную информацию в составе большого текста или в виде цифрового изображения, также определять поведение системы в отношении обнаружения, контроля и предотвращения утечек данных;

– контроль приложений и снимки экрана: дает разрешение или запрет на запуск тех или иных приложений на компьютере, исходя из политик безопасности организации, и создает снимок экрана при длительном отсутствии активности от мыши или клавиатуры;

– контроль истории браузера: DLP-системы могут анализировать историю посещенных веб-сайтов, взаимодействие пользователя с онлайн-ресурсами, передачу данных через веб-приложения и другие действия, которые могут повлечь за собой утечку чувствительных данных [2].

Для большего понимания данной темы представлен принцип работы DLP-систем в виде схемы (рис. 1).



Рисунок 1. Схема работы DLP-систем

Таким образом, с развитием технологий машинного обучения и искусственного интеллекта DLP-системы становятся все более эффективными в обнаружении и предотвращении утечек данных. В будущем можно ожидать улучшения алгоритмов роста функций искусственного интеллекта анализа

данных, расширения возможностей автоматизации реакции на инциденты, интеграции с облачными сервисами и мобильными устройствами, а также улучшения пользовательского опыта.

DLP-системы представляют собой важный инструмент в борьбе с утечками данных и расследовании информационных инцидентов. Их возможности по мониторингу, анализу и предотвращению утечек делают их неотъемлемой частью стратегии информационной безопасности любой организации. Дальнейшее развитие DLP-технологий обещает улучшение эффективности и надежности защиты информации.

Список используемых источников

1. Иванов А. Роль DLP-систем в обеспечении информационной безопасности. // Информационные Технологии. 2020.
2. Смирнов Б. Использование DLP-технологий в борьбе с утечками данных. Конференция по Информационной Безопасности. 2019.

Статья представлена заведующим кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, к.т.н. А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ И АТАК В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

И. Е. Пестов, И. А. Смуров, Е.С. Федорова, П. О. Федоров

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

Облачные инфраструктуры становятся все более популярными и все более важными для различных компаний и организаций. Однако, с ростом использования облака возрастает и число потенциальных угроз безопасности, таких как аномалии и атаки на информационные системы. Анализ методов выявления аномалий и атак в облачных инфраструктурах является критически важным для обеспечения безопасности данных и ресурсов в облаке. В этой статье мы рассмотрим различные подходы к обнаружению аномалий и атак в облаке, включая использование статистических методов, машинного обучения, поведенческого анализа, анализа журналов и сигнатурного анализа.

облачные инфраструктуры, угрозы безопасности, атаки, аномалии

Облачные инфраструктуры становятся все более популярными и все более важными для различных компаний и организаций. Однако, с ростом использования облака возрастает и число потенциальных угроз безопасности, таких как аномалии и атаки на информационные системы.

Анализ методов выявления аномалий и атак в облачных инфраструктурах является критически важным для обеспечения безопасности данных и ресурсов в облачных сервисах. В этой статье рассматриваются различные подходы к обнаружению аномалий и атак в облачной инфраструктуре, включая использование статистических методов, машинного обучения, поведенческого анализа, анализа журналов и сигнатурного анализа.

Обнаружение аномалий и атак в облачных инфраструктурах является сложной задачей из-за большого объема данных и высокой скорости их генерации. Однако, в настоящее время существует несколько классических подходов к обнаружению аномалий и атак в системах мониторинга облачных инфраструктур, таких как:

- использование статистических методов для анализа данных и выявления аномалий;
- машинное обучение: использование алгоритмов машинного обучения для анализа данных и обнаружения аномалий или атак;
- поведенческий анализ: изучение поведения пользователей и систем для обнаружения отклонений от нормы;
- анализ журналов: просмотр журналов событий для выявления аномалий или подозрительной активности;

– сигнатурный анализ (использование шаблонов или сигнатур известных атак для обнаружения новых атак) [1].

Статистические методы могут быть эффективно использованы для анализа данных и выявления аномалий в системах мониторинга облачных инфраструктур. Данные методы базируются на анализе статистических показателей, таких как средние значения, дисперсия, квартили. Аномалии могут быть обнаружены путем выявления отклонений от статистических характеристик нормального поведения системы. Наиболее распространены в применении такие статистические методы как:

– Z-оценка, метод основан на использовании Z-оценки для оценки отклонений от среднего значения; аномалии могут быть обнаружены путем анализа значений, которые существенно отличаются от среднего значения;

– Grubbs' тест, используется для обнаружения выбросов в наборе данных, позволяет определять наличие значительных отклонений от общей тенденции данных;

– дисперсионный анализ, может применяться для сравнения дисперсий различных групп данных и выявления отклонений, которые могут свидетельствовать о наличии аномалий;

– контрольные карты, метод контрольных карт используется для мониторинга процессов и обнаружения отклонений от установленных стандартов, может быть применен для непрерывного мониторинга параметров облачной инфраструктуры и выявления аномального поведения;

– квартильный анализ, позволяет выявлять значительные отклонения от медианы и определения областей с наибольшими аномальными значениями [2].

Эти статистические методы могут быть использованы как самостоятельно, так и в сочетании с другими методиками анализа данных и мониторинга, чтобы обеспечить наибольшую эффективность обнаружения аномалий в облачных системах. Также статистические методы выявления аномалий способствуют выявлению трендов и сезонных колебаний в метриках облачной инфраструктуры, определению контрольных границ для метрик мониторинга, что позволяет выявлять аномальные значения, которые выходят за пределы установленных границ, нахождению корреляций между различными метриками мониторинга, что позволяет выявлять аномалии, которые проявляются в виде необычных взаимосвязей между данными.

Зачастую при статических методах мониторинга и обнаружения аномалий применяются анализ временных рядов, позволяющий выявлять аномалии в динамике метрик облачной инфраструктуры, такие как внезапные изменения или выбросы [3].

Алгоритмы машинного обучения (МО) широко используются для анализа данных и обнаружения аномалий или атак в системах мониторинга облачных инфраструктур. Эти системы собирают большое количество данных

о поведении пользователей, приложений и сетей, и могут столкнуться с различными угрозами безопасности, такими как DDoS-атаки, вторжения в систему, несанкционированный доступ и другие вредоносные действия. Для обнаружения таких аномалий и атак, системы мониторинга могут использовать различные методы машинного обучения, включая алгоритмы классификации, регрессии и обнаружения выбросов. Например, алгоритмы классификации могут быть использованы для определения нормального и аномального поведения.

К наиболее распространённым методам машинного обучения можно отнести:

- метод опорных векторов (SVM), может использоваться для обнаружения аномалий путем построения гиперплоскости, которая разделяет нормальное и аномальное поведение в пространстве признаков (объекты, находящиеся далеко от разделяющей гиперплоскости, могут быть классифицированы как аномальные);

- алгоритмы графов принятия решений, графы принятия решений могут быть обучены на основе исторических данных для определения аномальных паттернов или правил, которые указывают на наличие аномалий.

- нейронные сети – различные архитектуры нейронных сетей, включая рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN), могут быть использованы для обнаружения аномалий в облачных системах путем моделирования нормальных временных и пространственных зависимостей [4].

Также используются методы обучения с учителем и без учителя для анализа больших объемов данных и выявления скрытых узоров, которые могут свидетельствовать о потенциальных угрозах безопасности. Кроме того, системы мониторинга облачных инфраструктур могут использовать алгоритмы глубокого обучения для анализа больших и сложных наборов данных.

Поведенческий анализ позволяет выявлять аномальные события или действия, которые могут указывать на угрозы безопасности, такие как несанкционированный доступ, внутренние угрозы или атаки от внешних злоумышленников. Кроме того, этот метод способствует выявлению необычных тенденций в использовании ресурсов облака, что может свидетельствовать о наличии проблем в производительности или эффективности системы. В целом, поведенческий анализ является важным инструментом для обеспечения безопасности и надежности облачных инфраструктур, поскольку он позволяет оперативно выявлять и реагировать на потенциальные угрозы и аномалии, минимизируя риск возникновения серьезных инцидентов безопасности [5]. По своей сути поведенческий анализ представляет собой метод анализа данных, который сфокусирован на изуче-

нии обычного поведения системы или пользователя и выявлении отклонений от эталонного образца. При этом не используются заранее заданные правила или сигнатуры атак, а вместо этого происходит изучение и профилирование нормального функционирования.

Анализ журналов является важной частью мониторинга облачной инфраструктуры. Журналы содержат информацию о событиях, происходящих в системе, и могут использоваться для выявления аномалий и подозрительной активности. Журналы в облачных инфраструктурах обычно представлены в формате `syslog`, который содержит сообщения о различных событиях, таких как системные вызовы, изменения состояния сервисов и ошибки. Они могут быть сгенерированы различными компонентами облачной платформы, включая виртуальные машины, сетевые устройства, балансировщики нагрузки.

Для анализа журналов событий можно использовать различные инструменты мониторинга и анализа, такие как Nagios, Zabbix, Splunk.

Просмотр журналов событий также может осуществляться вручную с помощью специалистов по информационной безопасности. Они могут проанализировать лог-файлы событий, идентифицируя подозрительные активности и принимая меры по предотвращению потенциальных угроз [6].

Таким образом, анализ журналов событий в облачных инфраструктурах является важной составляющей обеспечения безопасности и надежности системы. Он позволяет выявлять угрозы и аномалии, обеспечивая оперативную реакцию на потенциальные проблемы и угрозы.

Сигнатурный анализ является одним из основных методов обнаружения атак в системах облачной инфраструктуры. Данный метод обнаружения угроз, базируется на использовании шаблонов или сигнатур известных атак для их обнаружения в облачных системах мониторинга инфраструктуры. Этот метод заключается в анализе сетевого трафика, системных журналов, поведения приложений и других данных на предмет соответствия уже известным угрозам, представленным в виде сигнатур. Когда система обнаруживает совпадение сигнатуры атаки в данных, срабатывает тревога или инициируются предупредительные действия. Сигнатурный анализ позволяет эффективно идентифицировать зловерное или несанкционированное поведение, такое как попытки взлома, атаки отказа в обслуживании (DDoS), вирусы и другие виды кибератак [7].

Однако у сигнатурного анализа есть и недостатки. Во-первых, он предполагает наличие подробных и актуальных сигнатур угроз, что означает, что система может упустить новые или неизвестные виды атак. Во-вторых, использование только сигнатурных методов может привести к высокому количеству ложных срабатываний, что требует дополнительной проверки и исследования обнаруженных событий. Тем не менее, сигнатурный анализ

все еще остается важным инструментом для определения угроз безопасности облачных инфраструктур, особенно в сочетании с другими методами обнаружения угроз, такими как анализ поведения и машинное обучение [8].

В качестве сравнительного анализа приведенных методов мониторинга и обнаружения аномалий была составлена таблица 1 в которой отражены преимущества и недостатки каждого метода [9].

ТАБЛИЦА 1. Сравнение методов выявления аномалий и атак в облачных инфраструктурах

Метод	Преимущества	Недостатки
Статистические методы	Точность и надежность	Сложность настройки и необходимость большого количества данных
Машинное обучение	Высокая точность обнаружения	Требует много данных для обучения
Поведенческий анализ	Прост в использовании, низкая стоимость	Низкая точность, может пропустить атаки
Анализ журналов	Может обнаружить атаки на ранней стадии	Сложно обрабатывать большие объемы данных, могут быть ложные срабатывания
Сигнатурный анализ	Прост в использовании, низкая стоимость	Ограничен в том, какие атаки может обнаружить, требует обновления сигнатур

Таким образом, существует несколько методов выявления аномалий и атак в облачных инфраструктурах, каждый из которых имеет свои преимущества и недостатки. Использование статистических методов для анализа данных и выявления аномалий позволяет оперировать большим объемом информации, однако может быть сложно определить точные границы аномалий. Машинное обучение предоставляет возможность создания алгоритмов, которые могут обучаться на определенных параметрах, однако требует большого объема размеченных данных для эффективной работы. Поведенческий анализ позволяет учитывать индивидуальное поведение пользователей и систем для выявления отклонений от нормы, однако может выявлять слишком много ложноположительных результатов. Анализ журналов событий может быть эффективным для выявления атак на ранних стадиях, но требует постоянного мониторинга и анализа большого объема данных. Сигнатурный анализ позволяет обнаруживать заранее известные атаки, но неэффективен при выявлении новых или измененных форм атак. Таким образом, для наиболее эффективной защиты облачных инфраструктур

рекомендуется комбинировать различные методы анализа данных и выявления аномалий, чтобы обеспечить наиболее полное и достоверное обнаружение потенциальных угроз [10].

Список используемых источников

1. Красов А. В., Швидкий А. А. Использование возможностей масштабирования облачной инфраструктуры для оптимизации процесса создания лабораторных стендов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. / Под. ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. СПб.: СПбГУТ, 2015. С. 1580–1584.
2. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39–47.
3. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и в образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 329–334.
4. Красов А. В., Ушаков И. А., Щипцов Д. И. Анализ уязвимостей и релевантных решений в области обеспечения безопасности sdn-сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 611–616.
5. Красов А. В., Ушаков И. А., Федоров В. А. Сравнительный анализ существующих решений мониторинга sdn-сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 606–611.
6. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Научные технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70–76.
7. Виткова Л. А., Мустафаев Р. А., Сахаров Д. В., Хомин И. И. Использование big data в процессах обеспечения безопасности информационной сферы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. / Под ред. С.В. Бачевского. СПб.: СПбГУТ, 2018. С. 186–191.
8. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6. № 3. С. 1–9.
9. Богданова Л. Н., Виткова Л. А. Обзор алгоритмов обнаружения аномальной сигнализации в iot // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2020. № 1. С. 47–51.
10. Ахрамеева К. А., Виткова Л. А., Голузина Д. Р. Методы искусственного интеллекта и анализа распространения информации в ходе инцидентов и кризисов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб., 2020. С. 422–426.

УДК 004.896
ГРНТИ 28.17.33

МНОГОАСПЕКТНЫЕ МОДЕЛИ ГЕОГРАФИЧЕСКИХ ОБЪЕКТОВ

П. А. Прокофьев

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

Рассмотрена общая структура геореляционных баз данных. Представлены многоаспектные модели географических объектов, позволяющие описывать природные и антропогенные объекты в рамках единой многоаспектной среды. Результаты данной работы могут быть использованы для реализации программного обеспечения, позволяющего решать задачи геоинформационного моделирования, анализа, планирования и управления пространственно-распределёнными объектами в рамках географического региона.

ГИС, картография, географические объекты, базы данных, многоаспектные модели

В настоящее время широко распространён подход к хранению геоинформационной информации, основанный на базах геоданных (рисунок 1), которые, в свою очередь, являются развитием реляционных баз данных [1].

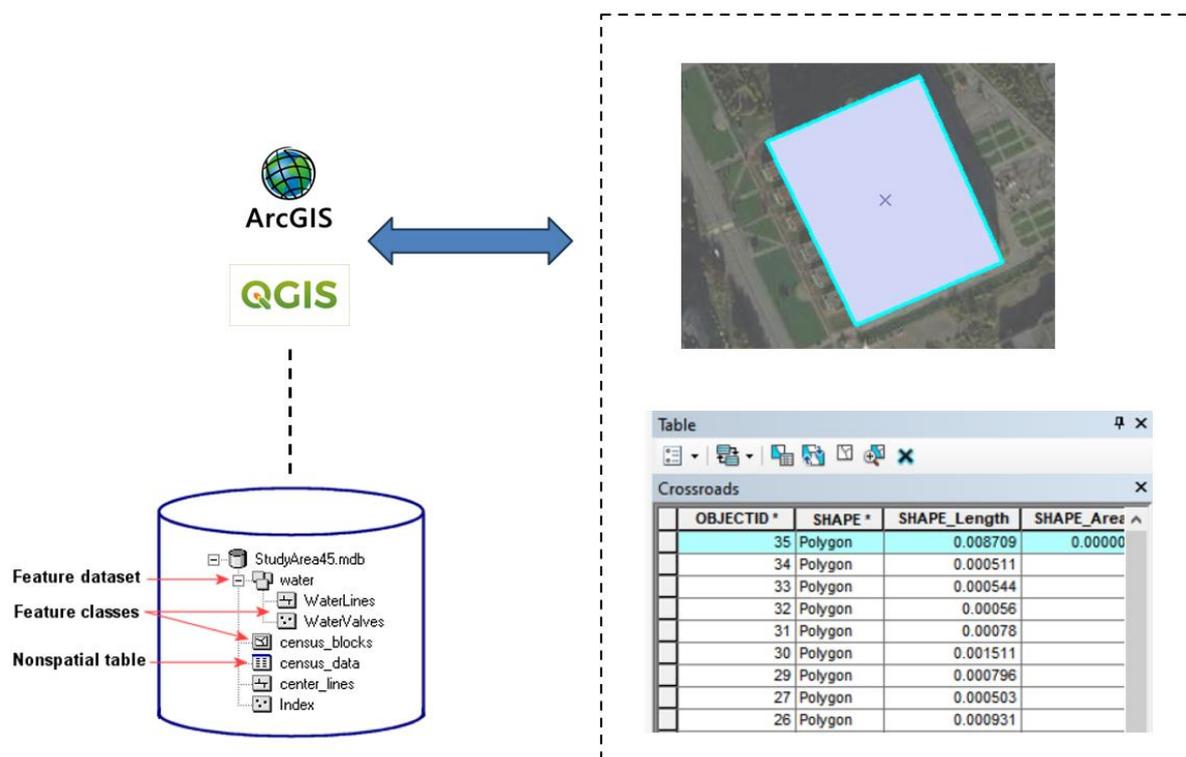


Рис. 1. Геоинформационные базы данных

Следствием такого подхода является то, что атомарной единицей, с которой работает пользователь, является слой (таблица атрибутов). Это обобщение накладывает ограничения на возможности работы с географическими объектами. Так, например, в данных системах тяжело учитывать особенности каждого объекта по отдельности.

В данной статье предлагается новый подход к организации геоданных – многоаспектные модели географических объектов, основанный на [2, 3]. Согласно данному подходу, модель географического объекта можно представить следующим образом:

$$m_o \sqcap \langle T_o, G, D, P_1, P_2, Eval, Valid \rangle, \quad (1)$$

где m_o – модель географического объекта; T_o – тип географического объекта; t – временная метка, для которой актуальна модель; P_1 – первичные параметры объекта; P_2 – вторичные (вычисляемые) параметры объекта; $Eval$ – правила вычисления вторичных параметров объекта; $Valid$ – правила валидации объекта.

Кроме того, следует учесть, что некоторые объекты могут менять свои параметры в зависимости от сезона. Так, водоёмы могут менять площадь поверхности, а животные – менять места обитания. Поэтому введём формализм S_i , обозначающий сезон. Тогда модель (1) можно представить в виде набора исходных моделей, описывающих один и тот же объект в разные сезоны.

$$m_o \sqcap \bigcup_{i=1}^n \langle S_i, T_o, G_i, D_i, P_{1i}, P_{2i}, Eval, Valid \rangle,$$

Геометрия представляет собой множество фигур (в частном случае – одну), для каждой из которых задаётся тип координатной системы CRS, тип геометрического объекта TG (точка, линия, полигон), а также набор координат x_i и y_i :

$$G \sqcap \bigcup_{i=1}^n \left\langle CRS, T_G, \bigcup_{j=1}^m (x_j, y_j) \right\rangle.$$

$$T_G \in (poly, line, point)$$

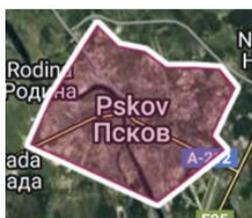
$$CRS \in (CRS_1, CRS_2, \dots, CRS_N)$$

Формализм представления параметров P_1 имеет разные типы, которым в цифровом представлении могут соответствовать такие типы данных как *enum*, *bool*, *int*, *float* и другие.

Вторичные параметры вычисляются с применением операторов *Eval* на основе первичных параметров и прочей необходимой информации, например геометрии. Результат работы операторов *Eval* также может быть использован для валидации объекта в операторах *Valid*. Например, объект может считаться не валидным, если не удалось вычислить вторичные параметры.

С использованием описанных моделей можно представить природные и антропогенные объекты разного рода, относящиеся к тем или иным географическим аспектам. Примеры некоторых объектов приведены на рисунке 2.

N	Сезон	Геометрия	Тип	Описание
1	июль-ноябрь		Река	-
2	март-июнь		Река	Затапливаются деревни N1, N2



Население
189 315



Геометрия

Тип

Описание

- Равнинный;
- Холмистый;
- **Низкогорный;**
- Среднегорный;
- Высокогорный

В юго-западной части город окаймлён отрогами Навагирского хребта, подходящими к городу с северо-запада. Самая высокая точка на территории Новороссийска – 447м

Рис. 2. Примеры представления географических объектов

Достоинством данного подхода является возможность работы непосредственно с географическими объектами, учитывая особенности каждого из них по отдельности (в отличие от работы со слоями в геоинформацион-

ных базах данных). При этом предлагаемый подход не исключает возможность объединить параметры одного типа в группу. Это открывает новые возможности для работы с геоинформационными системами.

Список используемых источников

1. Архитектура базы геоданных. URL: <https://pro.arcgis.com/ru/pro-app/latest/help/data/geodatabases/overview/the-architecture-of-a-geodatabase.htm> (дата обращения 03.12.2023)
2. Прокофьев П.А. Метод многоаспектного геоинформационного моделирования географического района // Информация и Космос. 2023. № 4. С. 121–126.
3. Верховая Г. В. Метод многоаспектного геоинформационного моделирования географического района / Г.В. Верховая, С.В. Акимов, С.П. Присяжнюк // Информация и Космос. 2021. № 4. С. 123–129.

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

УДК 004.65
ГРНТИ 50.41.21

ТРАНСЛЯЦИЯ ОПЕРАЦИЙ РЕЛЯЦИОННОЙ АЛГЕБРЫ В КОМАНДЫ ЯЗЫКА SQL С УЧЕТОМ ОГРАНИЧЕНИЙ ДЛЯ ОПЕРАЦИЙ

Д. Е. Пшеничникова, О. Ю. Сабинин

Санкт-Петербургский политехнический университет Петра Великого

В данной статье рассматривается возможность трансляции операций реляционной алгебры в команды языка SQL. Проводится обзор восьми операций реляционной алгебры и их ограничений. Предлагается способ перевода операций реляционной алгебры на язык SQL. Рассматривается алгоритм проверки ограничения: совпадения схем отношений.

операции реляционной алгебры, язык SQL, пакет DBMS_SQL

Трансляция операций реляционной алгебры в команды языка SQL является актуальной темой, так как это позволяет разработчикам и аналитикам использовать известные и понятные концепции реляционной алгебры для формулирования запросов и операций с базой данных с использованием языка SQL. Вместо написания сложных SQL запросов, которые могут быть трудными для понимания и отладки, можно использовать более простые и логические операции реляционной алгебры, такие как проекции, селекции, объединение, пересечение и разность множеств. Это позволяет разработчикам выразить свои идеи и требования к данным более ясно и лаконично.

Однако, при трансляции операций реляционной алгебры в SQL, нужно учитывать ограничения и особенности языка SQL, такие как синтаксические правила, типы данных, агрегатные функции и индексы. Некоторые операции реляционной алгебры могут не иметь непосредственного эквивалента в языке SQL, и требуется некоторое преобразование или комбинация операторов SQL для достижения того же результата.

Анализ возможностей операций реляционной алгебры

Реляционная алгебра содержит более 8 операций для работы с отношениями, где отношения R – это некоторое подмножество декартового произведения доменов, представляющих собой наборы записей. Далее отношение будет называться таблицей базы данных, поскольку в данном контексте это более точное определение. Таблицы будут обозначены F и S . В данном ра-

боте будут рассмотрены основные 8 операций реляционной алгебры: декартовое произведение, выборка, проекция, объединение, разность, соединение, пересечение, деление.

Выборка представляет собой отбор строк таблицы, которые соответствуют заданным условиям. Синтаксис записи данной операции в реляционной алгебре:

$$R = \sigma_{\theta\text{-предикат}}(F),$$

$$R = F [\theta\text{-предикат}] \text{ или}$$

$$R = F \text{ WHERE } \theta\text{-предикат},$$

где предикат — это условие выборки.

Проекция позволяет отобразить только нужные столбцы таблицы:

$$R = \Pi X, Y, \dots, Z (F) \text{ или } R = F [X, Y, \dots, Z].$$

В результирующем отношении все кортежи (строки) должны быть уникальными. Декартовое произведение двух отношений представляет собой конкатенацию каждого кортежа (строки таблицы) первого отношения с каждым кортежем второго отношения. При наличии одинаковых атрибутов в отношениях их необходимо или переименовать, или использовать полные названия.

Синтаксис операции: $R = F \times S$ или $R = F \text{ TIMES } S$.

Объединение представляет собой набор кортежей, которые есть или у первого отношения, или у второго или у обоих сразу, при этом в результирующем отношении повторения кортежей не должно быть. Схемы результирующего и исходных отношений должны быть одинаковые.

Синтаксис: $R = F \cup S$ или $R = F \text{ UNION } S$.

Пересечение позволяет отобразить одинаковые строки двух отношений:

$$R = F \cap S \text{ или } R = F \text{ INTERSECT } S.$$

Схемы результирующего и исходных отношений должны быть одинаковые. Разность представляет собой отбор кортежей (строк таблицы), которые принадлежат первому отношению, но не принадлежат второму. Схемы результирующего и исходных отношений должны быть одинаковые.

Синтаксис: $R = F \setminus S$ или $R = F \text{ MINUS } S$.

Операция соединения разделяется на два вида: тета-соединение и естественное соединение. Тета-соединение – это декартовое произведение с выборкой по условию необходимых кортежей:

$$F[Fx \theta Sy]S \text{ или } F \bowtie_{\theta} Fx \theta SyS.$$

Естественное соединение происходит по общему атрибуту, если общих атрибутов нет, то результат равен результату декартового произведения. Синтаксис естественного соединения: $R = F \bowtie S$ или $R = F \text{ JOIN } S$.

Операция деления представляет собой отбор кортежей (строк) первого отношения, которые соответствуют комбинации всех кортежей второго отношения. Все атрибуты второго отношения должны входить в первое отношение.

Синтаксис: $R = F \div S$ или $R = F \text{ DIVIDEBY } S$.

Следует иметь в виду, что в операциях реляционной алгебры можно использовать и сложные условия, образуемые с помощью логических операторов AND, OR, NOT.

Сопоставление операций реляционной алгебры и языка SQL

В реляционной алгебре операции можно обозначать символом или словом. В ходе тестовых попыток записи и чтения строк с различным синтаксисом операций реляционной алгебре, выяснилось, что не все кодировки символов операций реляционной алгебры могут быть корректно считаны. Следовательно, обозначать операции стоит только словами, такими как: WHERE, UNION, MINUS и т.д. Большинство операторов языка SQL совпадают с операциями реляционной алгебры (таблица 1).

ТАБЛИЦА 1. Сопоставление операций реляционной алгебры и языка SQL

Операция	Реляционная алгебра	Язык SQL
Выборка	$F \text{ WHERE } \theta\text{-предикат}$	SELECT * FROM F WHERE θ
Проекция	$F [X, Y, \dots, Z]$	SELECT X, Y, ..., Z FROM F
Декартовое произведение	$F \text{ TIMES } S$	SELECT * FROM F CROSS JOIN S
Объединение	$F \text{ UNION } S$	SELECT * FROM F UNION SELECT * FROM S
Пересечение	$F \text{ INTERSECT } S$	SELECT * FROM F INTERSECT SELECT * FROM S
Разность	$F \text{ MINUS } S$	SELECT * FROM F MINUS SELECT * FROM S
Тета-соединение	$F[F_x \theta S_y]S$	SELECT * FROM F JOIN S ON $F_x \theta S_y$
Естественное соединение	$F \text{ JOIN } S$	SELECT * FROM F NATURAL JOIN S
Деление	$F \text{ DIVIDEBY } S$	SELECT X FROM F MINUS SELECT X FROM (SELECT X, Y FROM F CROSS JOIN S MINUS SELECT * FROM F), где X – столбцы, которые мы определяем, а Y – столбцы делителя

Операция деление не имеет прямого эквивалента в языке SQL. Однако, можно использовать блок операторов SQL, чтобы достичь функциональности этой операции.

Для выполнения операции деления применяется следующий подход: сначала берется декартово произведение двух таблиц - первой и второй. Затем находится разность этого произведения и первой таблицы [1]. В конце берется разность проекций по столбцам, не входящим в делитель, первой таблице и результата предыдущих действий.

Для выполнения операций разности, пересечения и объединения таблиц необходимо, чтобы таблицы имели одинаковую структуру. Чтобы проверить схемы отношений, была создана функция (рис.1) на основе пакета DBMS_SQL Oracle [2].

```
1. CREATE OR REPLACE FUNCTION check_shem (t1 varchar2, t2 varchar2)
   RETURN boolean
2. AS
3.   cur_id_1  INTEGER;
4.   cur_id_2  INTEGER;
5.   col_count_1 INTEGER;
6.   col_count_2 INTEGER;
7.   col_tab_1 DBMS_SQL.DESC_TAB;
8.   col_tab_2 DBMS_SQL.DESC_TAB;
9. BEGIN
10.  cur_id_1 := DBMS_SQL.OPEN_CURSOR;
11.  cur_id_2 := DBMS_SQL.OPEN_CURSOR;
12.  DBMS_SQL.PARSE(cur_id_1, t1, DBMS_SQL.NATIVE);
13.  DBMS_SQL.PARSE(cur_id_2, t2, DBMS_SQL.NATIVE);
14.  DBMS_SQL.DESCRIBE_COLUMNS(cur_id_1, col_count_1, col_tab_1);
15.  DBMS_SQL.DESCRIBE_COLUMNS(cur_id_2, col_count_2, col_tab_2);
16.  IF col_count_1 != col_count_2 THEN
17.    RETURN false;
18.  END IF;
19.  FOR i IN 1..col_count_1 LOOP
20.    IF
21.      replace(col_tab_1(i).col_name, '_2', '') != replace(col_tab_2(i).col_name, '_2', '')
22.    THEN
23.      RETURN false;
24.    END IF;
25.    RETURN true;
26.  END LOOP;
27.  DBMS_SQL.CLOSE_CURSOR(cur_id_1);
28.  DBMS_SQL.CLOSE_CURSOR(cur_id_2);
29. END;
```

Рис. 1. Пример функции проверки совпадения схем таблиц

Описание алгоритма проверки совпадения схем отношений:

- на вход программы поступают SQL-запросы для двух таблиц;
- строки 10-11: открываются курсоры таблиц;
- строки 12-13: производится SQL-запрос, данные которого записываются в курсор;
- строки 14-15 получаем метаданные таблиц (количество и название столбцов);

- строки 16-18: сравнение количества столбцов таблиц, если количество разное, то схемы точно не совпадают и дальнейшая проверка не нужна;
- строки 19-26: цикл, который проверяет совпадение имен атрибутов между двумя таблицами. Если названия атрибутов не совпадают, это означает, что схемы таблиц различны, и функция вернет значение false. В противном случае, если названия атрибутов совпадают, это указывает на одинаковые схемы таблиц, и функция вернет значение true;
- строки 27-28: закрываются курсоры.

Аналогичную функцию (рис. 1) можно использовать для переименования одинаковых названий атрибутов в случаях операций декартового произведения и тета-соединения, а также для определения входят ли атрибуты второго отношения в первое отношение для операции деления.

Заключение

В данной статье был произведен обзор восьми операций реляционной алгебры и предложены способы их трансляции в команды языка SQL. Кроме того, был рассмотрен алгоритм, который позволяет проверять совпадение схем отношений. На основе этого алгоритма можно разработать функции для согласования имен атрибутов и проверки наличия или совпадения атрибутов между отношениями.

Список используемых источников

1. Малиев А. Разработка языка реляционной алгебры и реляционного исчисления и транслятора на язык SQL // Вестник Воронежского государственного технического университета. 2009. URL: <https://cyberleninka.ru/article/n/razrabotka-yazyka-relyatsionnoy-algebry-i-relyatsionnogo-ischisleniya-i-translyatora-na-yazyk-sql/viewer> (дата обращения 17.12.2013)
2. Feuerstein S., Beresniewicz J., Dawes C. Oracle PL/SQL Built-ins Pocket Reference: O'REILLY, 1998. 35 с

УДК 004.05
ГРНТИ 20.15.05

ВЫЯВЛЕНИЕ ПОТРЕБИТЕЛЬСКИХ ПРЕДПОЧТЕНИЙ С ЦЕЛЬЮ СОВЕРШЕНСТВОВАНИЯ МАРКЕТИНГОВОЙ ДЕЯТЕЛЬНОСТИ

О. В. Раковский, Е. Н. Чухарева

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

Анализ потребительских предпочтений является важным инструментом для совершенствования маркетинговой деятельности. Он позволяет выявить наиболее востребованные товары и услуги, определить целевую аудиторию, адаптировать продукцию под потребности потребителей и улучшить качество обслуживания. Результаты анализа помогают компаниям разработать эффективные маркетинговые стратегии и повысить уровень удовлетворенности клиентов.

маркетинговая деятельность, целевая аудитория, потребности

В мире большого количества предложений товаров и услуг, а также постоянно меняющихся рыночных условий, понимание и учет потребительских предпочтений становится необходимым фактором для успешного ведения бизнеса. Современные компании все чаще обращаются к методам анализа и выявления потребительских предпочтений с целью адаптации своих маркетинговых стратегий под ожидания и потребности своей целевой аудитории. В данной статье рассматривается важность выявления потребительских предпочтений для совершенствования маркетинговой деятельности и методы, которые могут быть использованы компаниями в этом процессе.

Современный рынок представляет собой динамичную и конкурентную среду, где успешность бизнеса во многом зависит от того, насколько хорошо компании знают своих потребителей и умеют адаптироваться к их потребностям. В этом контексте выявление потребительских предпочтений становится ключевым элементом маркетинговой стратегии. Для эффективного развития и продвижения товаров и услуг необходимо не только предложить что-то уникальное и качественное, но и грамотно адаптировать это предложение к запросам рынка. Выявление потребительских предпочтений является ключевым элементом успешной маркетинговой стратегии. Понимание того, что заставляет потребителей делать выбор в пользу определенного продукта или услуги, позволяет компаниям адаптировать свои предложения таким образом, чтобы они лучше соответствовали ожиданиям своей аудитории. Это может способствовать увеличению конкурентоспособности компании на

рынке и повышению уровня удовлетворенности клиентов. Ниже представлена схема выявления потребительских предпочтений (рис. 1).



Рис. 1. Выявление потребительских предпочтений

Существует ряд методов, которые могут быть использованы компаниями для выявления потребительских предпочтений. Один из наиболее распространенных методов — это анкетирование и опросы. Путем опросов компании могут получить информацию о предпочтениях потребителей относительно конкретных продуктов, ценовой политики, качества обслуживания и других аспектов, влияющих на их покупательское поведение.

Другим эффективным методом является анализ данных о поведении потребителей в онлайн среде. С использованием современных технологий аналитики компании могут контролировать действия пользователей на сайтах, в приложениях и социальных сетях. Таким образом, можно получить необходимую информацию, какие продукты и услуги больше всего интересуют аудиторию.

Для выявления потребительских предпочтений также могут использоваться группы по интересам и персональные интервью. Такие методы позволяют получить более углубленное понимание мотивирующих причин у потребителей, восприятия ими продукции компании и факторов, влияющих на окончательное решение о покупке. Полученные в результате анализа потребительских предпочтений данные могут быть использованы компаниями для корректировки своих маркетинговых стратегий. На основе этих данных могут быть внесены изменения в продуктовую линейку, ценовую политику, каналы распространения и коммуникационные стратегии с целью лучшего соответствия ожиданиям и потребностям аудитории [1–4].

Кроме того, понимание потребительских предпочтений позволяет компаниям подстроить рекламную информацию под клиента, делая ее более привлекательной и адаптированной на целевую аудиторию. Все это позволяет повышать эффективность маркетинговых кампаний, а также способствовать переходу категории потенциальных клиентов в реальных покупателей.

Выявление потребительских предпочтений играет важную роль в современной рыночной деятельности. Понимание предпочтений и мотивации посетителей позволяет компаниям реализовывать более целенаправленные маркетинговые стратегии и повышать уровень удовлетворенности клиентов[5]. Для этого используются различные методы и инструменты анализа, а также последующего использования полученных результатов для оптимизации бизнес-процессов, с закономерным ожиданием роста конкурентоспособности на рынке.

Для анализа ситуации на современном рынке проводятся маркетинговые исследования потребительского рынка. Это позволяет учесть социальные, культурные, психологические факторы, влияющие на покупательскую мотивацию потенциальных потребителей выпускаемой продукции.

Таким образом задача по проведению маркетинговых исследований является чрезвычайно актуальной для любой фирмы, даже не очень крупной. Выход подобных экономических отношений на уровень международных привел к тому, что соответствующие исследования стали необходимыми для деятельности любой фирмы, нацеленной на получение экономической прибыли. Руководство такой фирмы должно проводить ориентацию ее деятельности на большее соответствие нуждам потребителей, учитывая их предпочтения в выборе товаров и отношения к товарам конкурирующих фирм.

Необходимо также учитывать, что при проведении соответствующих исследований важно гарантировать, что полученная информация является максимально точной и достоверной. Иначе будет существовать риск принятия неверного решения, которые не только могут свести результаты к нулю, но и привести к экономическим потерям.

Список используемых источников

1. Мальцева С. В. Инновационный менеджмент: учебник для академического бакалавриата / под ред. С. В. Мальцевой. М.: Издательство Юрайт, 2014. 527 с.
2. Буреш О. В., Жук М. А. Интеллектуальные информационные системы управления социально-экономическими объектами. М.: Красанд, 2012. 192 с.
3. Финн В.К. Интеллектуальные системы и общество. М.: КомКнига, 2007. 352 с.
4. Остроух А. В., Николаев А. Б. Интеллектуальные информационные системы и технологии: Монография. СПб.: Лань, 2019. 308 с.
5. Бондаренко И. Б., Раковский О. В. Анализ потенциального охвата потребителей информационно-телекоммуникационных услуг // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. Т. 2. С. 347–350.

УДК 004.05
ГРНТИ 20.15.05

РАЗРАБОТКА СИСТЕМЫ АНАЛИЗА СТУДЕНЧЕСКОЙ УСПЕВАЕМОСТИ

О. В. Раковский, И. А. Чухарев

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

В данной статье обсуждается важность анализа успеваемости студентов. Для того, чтобы обеспечить успешное обучение, необходимо учитывать множество факторов, которые могут влиять на результаты студентов. Например, такими факторами являются баллы при поступлении, форма обучения, посещаемость занятий, результаты экзаменов. Основная цель такого анализа заключается в улучшении качества обучения и контроля за ходом учебного процесса.

анализ, учебный процесс, студенты, оценка, факторы

В современном образовательном процессе, где акцент смещается от простой передачи информации к формированию навыков и аналитического мышления, важно иметь эффективные инструменты для анализа и оценки студенческой успеваемости. Разработка системы анализа студенческой успеваемости становится ключевым элементом, позволяющим образовательным учреждениям не только отслеживать прогресс студентов, но и предоставлять персонализированную поддержку в учебном процессе.

В условиях современного образования студенты сталкиваются с различными вызовами, требующими от них не только усвоения знаний, но и умения их применять. В связи с этим растет значимость систем, способных анализировать процесс учебы, выявлять слабые места и предоставлять рекомендации для повышения успеваемости.

Прежде чем приступить к разработке системы анализа студенческой успеваемости, необходимо провести тщательный анализ требований, учитывая разнообразные аспекты образовательного процесса. Это включает в себя не только оценки и результаты студентов на экзаменах и тестах, но и участие в проектах, исследовательских работах, степень вовлеченности в учебный процесс, а также факторы, влияющие на мотивацию и учебные привычки.

Перед разработчиками стоит задача создать систему, которая будет учитывать разнообразные аспекты студенческой активности. Это включает в себя оценки за тесты и экзамены, участие в проектах и практиках, активность на занятиях и внеаудиторных мероприятиях, а также обратную связь от преподавателей и сверстников.

Система анализа студенческой успеваемости должна включать в себя ключевые элементы такие как:

- автоматизация сбора информации об успеваемости студентов из всех возможных источников; промежуточные оценки, контрольные, сданные лабораторные и практические работы и прочее;
- анализ успеваемости каждого студента по каждому предмету для выявления тенденций и закономерностей;
- понятное представление выявленных и проанализированных данных для понимания как студентами, так и преподавателями. Это необходимо для оценки текущей ситуации для принятия своевременных мер;
- использование машинного обучения для помощи и консультаций студентов для помощи им в принятии мер по улучшению личной успеваемости.

На рис. 1 представлена схема взаимодействия данной системы с деканатом и преподавателями.

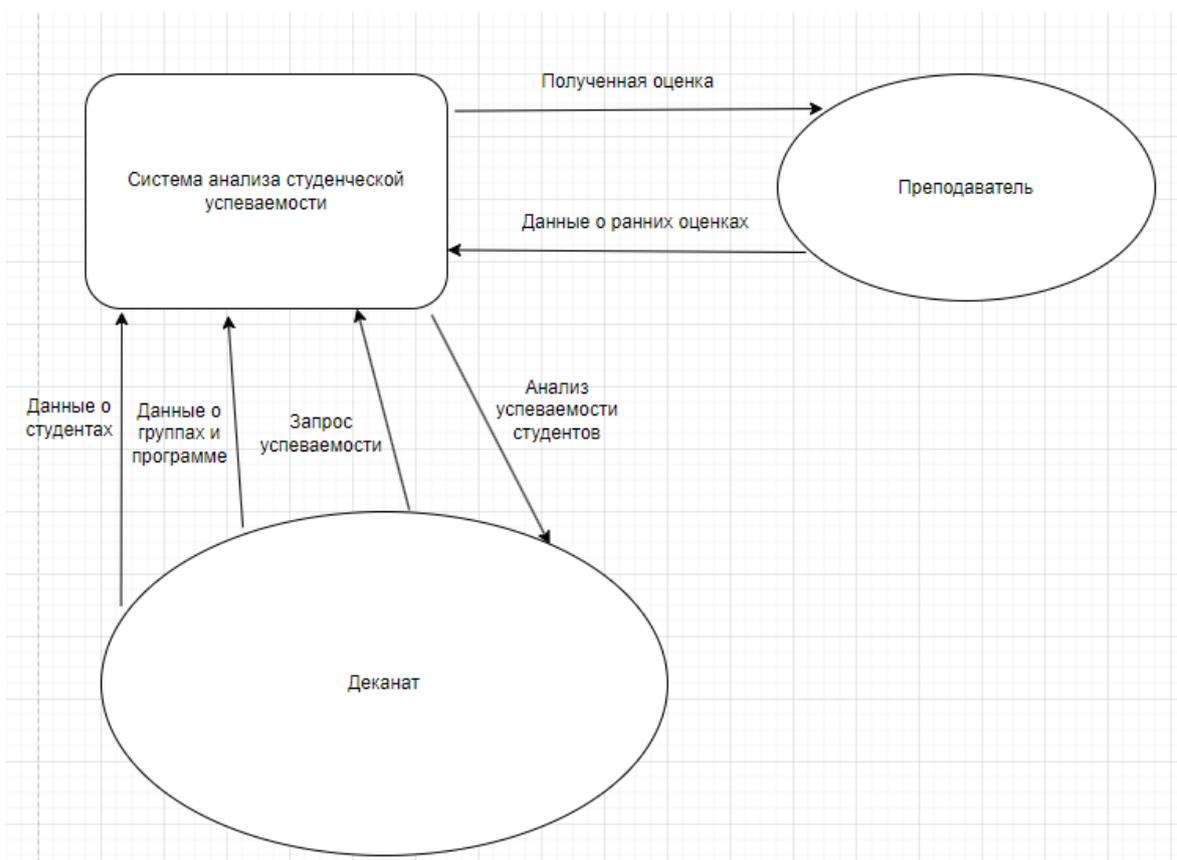


Рис. 1. Схема взаимодействия

Развитие подобных систем ведет к улучшению образовательных сред, удовлетворяющих потребности современных учащихся. Также это позволит

выпускать специалистов наилучшим образом, подготовленных к будущей высококвалифицированной рабочей деятельности [1–3].

Подобная система позволяет студентам следить за собственной успеваемостью, преподавателям глобально оценивать, как усвоение материалов целым потоком, так и личные достижения каждого из студентов для выставления корректных оценок. Также образовательные учреждения могут отслеживать учебную ситуацию и оптимизировать образовательные процессы для улучшения общего качества образования.

Разработка системы анализа студенческой успеваемости - важный шаг в совершенствовании образовательного процесса. Она позволяет студентам и преподавателям более эффективно взаимодействовать, а также создает условия для наиболее качественного обучения и развития личности каждого обучающегося. Внедрение подобных систем требует всестороннего подхода и комплексного анализа потребностей образовательного студентов, преподавателей и заведений в целом, однако потенциальные выгоды для образования и обучающихся оправдывают усилия.

Список используемых источников

1. Евгеньев Г. Б. Интеллектуальные системы проектирования: Учебное пособие / Евгеньев Г. Б. М.: МГТУ им. Баумана, 2012. 410 с.
2. Антамошин А. Н. Интеллектуальные системы управления организационно-техническими системами / А.Н. Антамошин, О.В. Близнова, А.В. Бобов, Большак. М.: РиС, 2016. 160 с.
3. Советов Б. Я. Интеллектуальные системы и технологии: Учебник для студентов учреждений высшего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. М.: ИЦ Академия, 2013. 320 с.

УДК 004.021
ГРНТИ 20.23.19

АЛГОРИТМ ПЕРСОНАЛИЗИРОВАННОЙ РЕКОМЕНДАЦИИ ДОСУГОВЫХ МЕСТ ДЛЯ ТУРИСТОВ

П. О. Ромадова

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

В статье описан алгоритм рекомендации мест, интересных туристам. Для создания списка подходящих объектов посещения рассматриваются предпочтения пользователя. Осуществляется это методом фильтрации контента, проверяется схожесть векторов описания мест. Итог работы алгоритма – ранжированный список от наиболее до наименее подходящих мест для пользователя в соответствии с его предпочтениями.

контентная фильтрация, рекомендательные системы, алгоритм, туризм

Рекомендательные системы стали неотъемлемой частью жизни человека. Они встречаются при выборе товара на маркетплейсе, просмотре кино, общении в социальных сетях. Каждая сфера ориентируется на определенные характеристики товара или человека для создания наилучшего алгоритма выдачи необходимого контента.

Предметной областью статьи является туризм. Целевая аудитория представлена туристами. Рассматривается пользователь с индивидуальным запросом и база данных с описанием достопримечательностей. Совпадение с предпочтениями отражают рекомендации, полученные на основе контента. Преимущество подхода состоит во времени использования – на холодном старте, когда данные о пользователе отсутствуют. Основная информация содержит описания мест. Благодаря этому, алгоритм легко масштабируется и работает [1].

За основу были взяты данные с сайта администрации Санкт-Петербурга, содержащие описания выставочных залов, религиозных сооружений и парков.

При регистрации выполняется опрос интересов. Он состоит из набора слов, которые относятся к определенным видам объектов туризма. В каждой категории подсчитывается, сколько терминов выбрал пользователь. Вычисляется процентное соотношение каждой категории от общего числа выбранных слов. Это станет входным параметром алгоритма, а также файлы в формате .csv, содержащие информацию об достопримечательностях, и название объекта для поиска.

Блок-схема алгоритма представлена на рис. 1. Реализация делится на 3 этапа.



Рис. 1. Блок-схема алгоритма

На первом необходимо подготовить данные. Функция библиотеки `pandas` читает данные из файлов и помещает их в дата фреймы. Из структуры убираются лишние столбцы, остаются только “ID”, “Название”, “Тип”, “Описание”, “Вид объекта”, “Тип учреждения”, “Историческая справка”, “Заметки”. Поскольку структура списков не стандартизирована, дата фрейм дорабатывается вручную. Для работы с библиотеками текст переводится в нижний регистр. Дополнительно убираются стоп-слова, которые не содержат значимой информации. К ним относят союзы, предлоги, вводные слова и другое. Исключаются не буквенно-цифровые знаки. Проводится лемматизация: процесс, когда слово приводится к первоначальной словарной форме. Данные всех файлов проходят обработку и объединяются в один документ. В дальнейшем не придется выполнять первый этап снова, можно будет пользоваться общим файлом и пополнять его.

Второй этап состоит из работы с отформатированным текстом. Считывается общий файл и происходит векторизация столбца “Описание” при помощи библиотеки `sklearn.feature_extraction.text` [2]. В описании конкретного объекта подсчитываются слова, вошедшие в набор слов, собранных со всего общего файла. Таким образом строится вектор достопримечательности. Для меры близости между векторами используется косинусное сходство. Метод подходит для измерения близости двух объектов. В итоге получится матрица значений сходств описаний, к ней необходимо добавить столбцы “ID” и “Вид объекта”. По вертикали и горизонтали подписать названия достопримечательностей.

На третьем этапе происходит формирование списка. Исходя из названия, введенного пользователем, выбирается соответствующий столбец. Далее значения ранжируют от большего к меньшему.

Рассмотрим работу алгоритма на следующем примере. Пусть итоговый список рекомендаций содержит 10 объектов, а введенное пользователем название “музей современного искусства эрарта”. Соотношение категорий достопримечательностей в списке определяют проценты, полученные от пользователя. Они составят 0,6 выставочные залы, 0,3 сады и парки и 0,1 религиозные объекты.

В результате наибольшее совпадение было с государственным музеем городской скульптуры и его новым выставочным залом. Остальные рекомендации составили: 6 выставочных залов, 1 храм, 3 парка. Проведен эксперименте с 10 другими названиями мест, среднее значение степени соответствия месту поиска составило 0,17, и первые три результата обычно относились к той же категории, что и выбранная достопримечательность.

Алгоритм прост в реализации, трудности возникают при работе с исходными данными. Они чаще всего неоднородные, из-за этого надо вносить

корректировки: вручную дополнять информацию или вводить коэффициенты, если проблема в определенной категории [2]. При оценке места или поиске клиентом достопримечательности, такой вид рекомендаций уместен и позволит удержать пользователя в краткосрочной перспективе. Поскольку эти предложения консервативны, клиент будет получать похожий материал, который не будет качественно отличаться, не смотря на изменение предпочтений со временем [3]. Для улучшения необходим сбор данных пользователя. В формате оценки посещенного места. В дальнейшем на основе этого можно построить систему коллаборативной фильтрации и предсказывать оценки пользователя для рекомендации. Последним этапом будет гибридный подход, который соединит контентную и коллаборативную фильтрацию [4, 5].

Возможный сценарий использования алгоритма в сфере туризма. Быстрые рекомендации на основе локации. Если пользователь решил посетить Казанский собор, добавив параметр локации, можно выбрать наиболее подходящие места в округе церкви. Скорость достигается за счет того, что матрица косинусного сходства создана пользователем при первом использовании, и к ней можно обратиться за данными без временных затрат.

Список используемых источников

1. Linden G., Smith B., York J. Amazon.com Recommendations Item-to-Item Collaborative Filtering // e IEEE Computer Society. 2003. № 3. С. 77–80.
2. Орельен Ж. Прикладное машинное обучение с помощью Scikit-Learn, Keras и TensorFlow. Концепции, инструменты. М.: ООО "Диалектика", 2020. 1040 с. ISBN 978-5-907203-33-4.
3. Меньшикова Н. В., Портнов И., В. Николаев И. В. Обзор рекомендательных систем и возможностей учета контекста при формировании индивидуальных рекомендаций // Academy: электрон. научн. журн. 2016. URL: <https://cyberleninka.ru/article/n/obzor-rekomendatelnyh-sistem-i-vozmozhnostey-ucheta-konteksta-pri-formirovanii-individualnyh-rekomendatsiy> (дата обращения: 02.02.2024)
4. Исламова С. А., Липатникова Н. В. Обзор рекомендательных систем // MODERN SCIENCE. 2019. № 4–3. С. 174–176.
5. Преображенский Ю. П., Коновалова В. М. Анализ подходов к формированию систем // Вестник Воронежского института высоких технологий. 2019. № 4(31). С. 88–90.

Статья представлена научным руководителем, доцентом кафедры ИСАУ СПбГУТ, кандидатом технических наук, доцентом А. Г. Любимовым.

УДК 339.187
ГРНТИ 50.49

АНАЛИЗ РАЗВИТИЯ CRM-СИСТЕМ

Е. А. Рубан, Г. Н. Смородин, Д. Е. Шаненко

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

Проведен анализ возможностей и перспектив развития CRM-систем в информационной экосистеме корпорации. Отмечены основные достоинства и недостатки CRM-систем с учетом мнений ведущих аналитиков информационных систем и тенденций развития корпораций. Детально показана структура CRM-системы и решения на основе искусственного интеллекта, позволяющие существенно оптимизировать поведение CRM-системы.

CRM-системы, управление отношениями с клиентами, облачные технологии, бизнес-процессы

CRM-системы (Customer Relationship Management) – это программное обеспечение, которое помогает автоматизировать рутинные задачи и управлять взаимоотношениями с клиентами. Согласно исследованию "The Impact of CRM Systems on Customer Satisfaction and Loyalty" (Влияние систем управления взаимоотношениями с клиентами на удовлетворенность и лояльность клиентов), внедрение CRM систем значительно улучшает обслуживание клиентов, что приводит к повышению их удовлетворенности и лояльности [1, 2].

Основные функции CRM-системы в информационной экосистеме представлены в таблице 1.

ТАБЛИЦА 1. Основные функции CRM-системы

Функция	Описание
Сбор и хранение данных о клиентах	Сбор информации о клиентах, их предпочтениях, покупках, контактных данных и других важных аспектах. Эти данные хранятся в единой базе данных, доступной сотрудникам компании. Это позволяет организации лучше понимать своих клиентов и предоставлять им персонализированный сервис.
Управление взаимодействиями с клиентами	CRM-система позволяет отслеживать все взаимодействия с клиентами, такие как звонки, письма, встречи и т. д. Это помогает сотрудникам компании быть в курсе всех деталей общения с клиентами и предоставлять им быстрое и эффективное обслуживание.

Функция	Описание
Автоматизация бизнес-процессов	Автоматизация рутинных задач, связанных с работой с клиентами. Например, она может автоматически генерировать отчеты о продажах, уведомления о новых возможностях для продажи или напоминания о встречах с клиентами. Это помогает сотрудникам компании сосредоточиться на более важных задачах.
Анализ данных и прогнозирование	CRM-система позволяет анализировать данные о клиентах и прогнозировать их поведение. Например, она может помочь определить наиболее перспективных клиентов для продажи нового продукта или услуги. Таким образом, CRM-система помогает организации принимать более обоснованные решения и улучшать свою маркетинговую стратегию.

На основе приведенных функций выделяются достоинства и недостатки CRM-систем, представленные в таблице 2 [3].

ТАБЛИЦА 2. Достоинства и недостатки CRM-систем

Достоинства	Недостатки
CRM-системы позволяют компаниям более эффективно управлять взаимодействием с клиентами, отслеживать их предпочтения и поведение, а также предоставлять персонализированный сервис. Это помогает улучшить удовлетворенность клиентов и повысить их лояльность.	Внедрение и поддержка CRM-системы может быть дорогостоящим процессом. Это включает в себя не только стоимость покупки и настройки системы, но и обучение сотрудников и постоянную поддержку.
CRM-системы увеличивают продуктивность, автоматизируя многие задачи, связанные с управлением клиентской базы данных, маркетингом и продажами. Это позволяет сотрудникам компании сосредоточиться на более важных и стратегических задачах.	Внедрение CRM-системы может быть сложным процессом, особенно для крупных компаний с большим объемом данных и сложными бизнес-процессами. Неправильное внедрение может привести к проблемам и недостаточной эффективности системы.
CRM-системы предоставляют компаниям ценные данные о клиентах и их поведении, а также позволяют проводить анализ этих данных. Это помогает компаниям прогнозировать спрос и принимать более обоснованные решения.	CRM-системы требуют актуальных и точных данных для работы. Если данные в системе устаревают или неточны, это может привести к неправильным аналитическим выводам и принятию неверных решений.

Стимулируя инновации и разработку новых функций, улучшающих взаимодействие с клиентами и повышающих производительность компаний, достоинства и недостатки CRM-систем оказывают значительное влияние на их тенденции развития и предполагаемое будущее [4], представленные в таблице 3.

ТАБЛИЦА 3. Тенденции развития CRM-систем

Тенденция	Описание
Интеграция с другими системами	В будущем CRM-системы будут все более интегрироваться с другими бизнес-системами, такими как ERP (системы планирования ресурсов предприятия), системы управления проектами и системы управления контентом. Это позволит компаниям иметь более полное представление о клиентах и лучше координировать свои бизнес-процессы.
Аналитика и искусственный интеллект	Развитие аналитических возможностей CRM-систем позволит компаниям получать более глубокие и полезные данные о своих клиентах. Использование искусственного интеллекта позволит автоматизировать и улучшить процессы прогнозирования и принятия решений на основе этих данных.
Мобильность	С развитием мобильных технологий все больше компаний будет использовать мобильные CRM-приложения для управления взаимоотношениями с клиентами. Это позволит сотрудникам работать с CRM-системой в любом месте и в любое время.
Персонализация	В будущем CRM-системы будут все больше фокусироваться на персонализации взаимодействия с клиентами. Они будут позволять компаниям создавать индивидуальные клиентские профили, предлагать персонализированные предложения и обеспечивать более удовлетворительный опыт обслуживания.
Облачные CRM-системы	Облачные CRM-системы будут продолжать набирать популярность, так как они обеспечивают более гибкую и доступную альтернативу традиционным локальным установкам. Компании будут все больше предпочитать облачные CRM-системы из-за их удобства и возможности масштабирования.

В настоящее время, с развитием технологий, внедрение искусственного интеллекта (ИИ) в CRM-системы становится обязательным элементом для организаций, стремящихся оставаться конкурентоспособными. Ключевые решения на основе искусственного интеллекта для CRM-систем [5] представлены в таблице 4.

ТАБЛИЦА 4. Ключевые решения на основе искусственного интеллекта для CRM-систем

Решение	Описание
Анализ данных с использованием машинного обучения системами	Прогнозирование поведения клиентов: ИИ в CRM-системах может использовать алгоритмы машинного обучения для анализа истории взаимодействий клиентов и предсказания их будущих предпочтений и поведения. Это позволяет более точно адаптировать маркетинговые стратегии и персонализировать предложения.
	Сегментация аудитории: ИИ помогает автоматизировать процесс сегментации клиентской аудитории на основе различных параметров, что дает возможность более эффективного таргетинга и персонализации коммуникации.
Автоматизация и оптимизация процессов	Автоматизированные чат-боты: ИИ-чат-боты в CRM обеспечивают мгновенные ответы на запросы клиентов, улучшая обслуживание и сокращая время реакции. Они могут также проводить предварительные квалификационные беседы, что экономит время сотрудников и повышает общую эффективность коммуникации.
	Автоматическая обработка запросов: ИИ может автоматизировать процессы обработки запросов, включая обращения через электронную почту, социальные сети или веб-формы. Это позволяет более быстро и эффективно реагировать на запросы клиентов.
Персонализация и кастомизация	Персонализированные рекомендации: используя алгоритмы машинного обучения, CRM с ИИ может предоставлять персонализированные рекомендации и предложения для каждого клиента на основе его предпочтений, истории покупок и поведенческих данных.
	Адаптивные стратегии взаимодействия: ИИ позволяет CRM системам реагировать на изменения в поведении клиентов и динамике рынка, адаптируя стратегии взаимодействия в реальном времени.
Аналитика и отчетность	Прогнозирование продаж: ИИ в CRM может использоваться для прогнозирования будущих продаж на основе анализа исторических данных, текущих трендов и внешних факторов, что позволяет компаниям более точно планировать свою деятельность.
	Выявление тенденций и паттернов: искусственный интеллект способен выявлять скрытые тенденции и паттерны в данных, что помогает в принятии более обоснованных стратегических решений.

Специфика применения искусственного интеллекта в CRM-системах заключается в использовании передовых алгоритмов машинного обучения и автоматизации для оптимизации процессов управления клиентским опытом, предоставляя компаниям инструменты для более эффективного взаимодействия с клиентами и принятия обоснованных стратегических решений [6].

В заключение можно отметить, что анализ развития CRM-систем является важным и актуальным направлением исследований в сфере управления отношениями с клиентами.

С развитием технологий и изменением потребностей бизнеса, CRM-системы становятся все более сложными и функциональными, позволяя компаниям эффективнее управлять своими клиентскими отношениями. В последние годы наблюдается увеличение внимания к персонализации и автоматизации процессов в CRM-системах.

Отслеживание и анализ данных о клиентах становится все более важным в контексте развития маркетинговых стратегий и повышения уровня обслуживания.

Однако, развитие CRM-систем также сталкивается с определенными вызовами. В частности, при проектировании и эксплуатации CRM-систем необходимо учитывать вопросы конфиденциальности и защиты данных клиентов. Безопасность становится все более важным аспектом в разработке CRM-систем, особенно в свете ужесточения законодательства о защите персональных данных.

Список используемых источников

1. Куликова М. М., Исабекова О. А. Актуальность внедрения CRM-систем // Московский экономический журнал. 2018. № 4. URL: <https://cyberleninka.ru/article/n/aktualnost-vnedreniya-crm-sistem> (дата обращения: 24.02.2024)
2. Леденева С. В., Гавриленко Т. Ю. Обзор рынка CRM-систем // International journal of professional science. 2019. № 5. URL: <https://cyberleninka.ru/article/n/obzor-rynka-crm-sistem> (дата обращения: 24.02.2024)
3. Кириллов Н. И. Преимущества и недостатки CRM систем с открытым исходным кодом // International scientific review. 2017. № 5 (36). URL: <https://cyberleninka.ru/article/n/preimuschestva-i-nedostatki-crm-sistem-s-otkryтым-ishodnym-kodom> (дата обращения: 24.02.2024)
4. Свиридова Е. В. Анализ мирового рынка CRM-систем, перспективы его развития, тренды на российском рынке // Вестник АГТУ. Серия: Экономика. 2017. № 3. URL: <https://cyberleninka.ru/article/n/analiz-mirovogo-rynka-crm-sistem-perspektivy-ego-razvitiya-trendy-na-rossiyskom-rynke> (дата обращения: 24.02.2024)
5. Тюрина Д. А., Крюкова А. А. AI-технологии в революции CRM-систем // Индустриальная экономика. 2023. № 4. URL: <https://cyberleninka.ru/article/n/ai-tehnologii-v-revolyutsii-crm-sistem> (дата обращения: 24.02.2024)
6. Городецкая О. Ю., Гобарева Я. Л. CRM - система как стратегия управления бизнесом компании // ТДР. 2014. № 4. URL: <https://cyberleninka.ru/article/n/crm-sistema-kak-strategiya-upravleniya-biznesom-kompanii> (дата обращения: 24.02.2024)

УДК 004.83
ГРНТИ 28.23.01

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОГРАММНОЙ ИНЖЕНЕРИИ

А. П. Соловьев, Н. А. Сорокин, С. С. Тихонов

Военная академия связи имени маршала советского союза С. М. Буденного

В контексте технологического прогресса и распространения искусственного интеллекта, рассматривается его влияние на программную инженерию. Подчеркивается, что автоматизация различных этапов жизненного цикла программного продукта благодаря искусственному интеллекту значительно сокращает время разработки кода. Подчеркивается роль машинного обучения в анализе данных, оптимизации производительности и создании моделей для прогнозирования трендов. Кроме того, рассматриваются успешные примеры использования искусственного интеллекта в различных областях, таких как здравоохранение, финансы и техническая поддержка; конкретные проекты, такие как GitHub Copilot и Tesla Autopilot. Заключительно подчеркивается, что гибкость и адаптация программистов к возможностям искусственного интеллекта становятся ключевыми компетенциями в эпоху стремительного развития технологий.

искусственный интеллект, программная инженерия, чат-боты, информационные технологии

В современном мире, пронизанном технологиями, искусственный интеллект (ИИ) становится неотъемлемой частью многих отраслей, включая программную инженерию. Развитие ИИ привносит новые подходы, инструменты и возможности, меняя типичные методы программной разработки и улучшая их эффективность. Давайте рассмотрим роль и влияние искусственного интеллекта на процессы программной инженерии.

Искусственный интеллект позволяет автоматизировать многие этапы жизненного цикла программного продукта. Начиная от анализа требований и проектирования до тестирования и обслуживания, также ИИ может значительно сокращать время разработки кода. Автоматическое обнаружение ошибок, оптимизация производительности и генерация кода – все это становится возможным благодаря технологиям искусственного интеллекта. Области, в которых методы ИИ оказались полезными в исследованиях и практике разработки программного обеспечения, можно охарактеризовать как «Вероятностная разработка программного обеспечения» [1].

Программисты все чаще используют машинное обучение для анализа данных и принятия более обоснованных решений, так искусственный интеллект помогает создавать модели, предсказывать тренды и улучшать алго-

ритмы, что особенно полезно в областях, где большие объемы данных требуют быстрого и точного анализа. Таким образом ИИ может помочь разработчикам в отладке и обслуживании программных приложений. Анализируя журналы, отчеты об ошибках и отзывы пользователей, алгоритмы ИИ могут выявлять основные причины проблем и предлагать потенциальные решения, экономя время и усилия [2]. Помимо этого, ИИ внедряется в процессы тестирования, что позволяет создавать более продуманные и эффективные тестовые сценарии. Это улучшает обнаружение дефектов, сокращает время, которое затрачено на тестирование, и повышает общую надежность программного продукта. Использование ИИ в анализе требований и прогнозировании рисков позволяет менеджерам и управляющим более эффективно управлять проектами. Моделирование и анализ данных позволяют предвидеть возможные проблемы и предпринимать меры еще на стадии разработки требований, снижая будущие риски, связанные с проектом.

Искусственный интеллект стимулирует появление новых парадигм программной инженерии. Например, разработка через нейронные сети может изменить способы создания программ, а алгоритмы машинного обучения могут создавать код, основанный на опыте и данных. Так крупнейшие мировые IT-корпорации строят новую парадигму разработки с 2016 года (Microsoft, IBM, Google) и активно используют ИИ-инструменты (иногда собственного производства) [3]. Интеграция искусственного интеллекта с экспертными знаниями программистов создаст сильные симбиотические связи. Такие экспертные системы на основе ИИ могут использовать опыт программистов для решения сложных задач и предоставления рекомендаций по возможному решению каких-либо проблем.

Если рассматривать ИИ в процессах обучения, то он привносит инновации в область обучения и развития программистов. Персонализированные системы обучения на основе ИИ могут адаптироваться к потребностям каждого разработчика, предоставляя рекомендации по усилению конкретных навыков. Это улучшает эффективность обучения и ускоряет процесс вхождения новых сотрудников в команду разработки.

Успешным использованием искусственного интеллекта в различных областях можно считать:

- 1) здравоохранение
 - диагностика и обнаружение заболеваний с использованием алгоритмов машинного обучения на основе медицинских изображений;
 - персонализированная медицина и прогнозирование эффективности лечения на основе анализа генетических данных.
- 2) финансовая сфера
 - анализ рынка и прогнозирование трендов с использованием алгоритмов машинного обучения;

– автоматизированные системы рекомендаций для инвестиций, основанные на анализе данных о портфеле и рыночной конъюнктуре.

3) техническая поддержка и обслуживание клиентов

– использование чат-ботов с искусственным интеллектом для автоматизации ответов на часто задаваемые вопросы и предоставления поддержки;

– анализ данных обратной связи клиентов для улучшения процессов обслуживания.

4) образование и обучение [4]

- пошаговые персонализированные учебные и диалоговые системы;
- исследовательские или интеллектуальные игровые среды обучения;
- анализ письменных работ;
- чат-боты [5–6];
- аналитические и рекомендательные системы;
- тренажерно-обучающие системы [7].

Если же говорить про конкретные проекты программной инженерии с использованием искусственного интеллекта, то к ним можно отнести:

– GitHub Copilot, разработанный с использованием технологий OpenAI, представляет собой инструмент автозаполнения кода с использованием искусственного интеллекта на базе GPT (Generative Pre-trained Transformer) для предоставления рекомендаций и кодирования;

– Google DeepMind's AlphaGo, созданный компанией DeepMind (дочерней компанией Google), применял глубокое обучение и нейронные сети для обучения игре в Го; продемонстрировал способность искусственного интеллекта к обучению сложным стратегическим искусствам;

– Tesla Autopilot, использует технологии машинного обучения и нейронных сетей для автоматизации вождения, активно собирает и обрабатывает данные с датчиков и камер на автомобиле для принятия решений в реальном времени;

– IBM Watson for Code, использует искусственный интеллект для анализа кода и предоставления рекомендаций по улучшению, это помогает программистам работать более эффективно и создавать более качественный код;

– Microsoft Visual Studio IntelliCode, встроенный в среду разработки Visual Studio от Microsoft, использует машинное обучение для предоставления интеллектуальных рекомендаций при написании кода, учитывая стили и предпочтения разработчика;

– DeepCode – это платформа для статического анализа кода с использованием методов машинного обучения, предоставляет рекомендации по улучшению кода, обнаруживая потенциальные ошибки и улучшая его структуру;

– Facebook Prophet, применяется для прогнозирования временных рядов и на основе этого помогает инженерам в области планирования и оптимизации ресурсов.

В заключение можно сказать, что искусственный интеллект существенно повлиял на процессы программной инженерии. Это сказалось не только улучшением эффективности и качеством разработки, но и появлением новых направлений для индустрии программной разработки. Гибкость и адаптивность программистов в использовании возможностей ИИ становятся ключевыми компетенциями в эру, где технологии стремительно развиваются.

Список используемых источников

1. Harman M. The Role of Artificial Intelligence in Software Engineering. URL: https://m.moam.info/the-role-of-artificial-intelligence-in-software-engineering_5a2857a91723dd4ce80e653d.html (дата обращения 8.01.24)

2. Электроникаплюс. Искусственный интеллект в разработке программного обеспечения. URL: <https://electronicaplus.ru/blog/138-iskusstvennyj-intellekt-v-razrabotke-programmnogo-obespecheniya> (дата обращения 8.01.24)

3. Habr. Перспективы развития ИИ-инструментов в софтверной инженерии. URL: <https://habr.com/ru/articles/750546>

4. Рябов Г.А., Тихонов С.С., Кривоногова Е.В. Основные возможности использования искусственного интеллекта в высшем образовании // Тенденции развития науки и образования. 2022. № 91-2. С. 26–30.

5. Федоренко А. В., Черепанов Д. А., Васильев Н. А. [и др.] Чат-бот по отбору и сопровождению кандидатов для поступления в научную роту. Свидетельство о государственной регистрации программы для ЭВМ № 2023684786 Российская Федерация / Федоренко А. В., Черепанов Д. А., Васильев Н. А. [и др.]; № 2023684177; заявл. 03.11.2023; опубл. 20.11.2023.

6. Васильев Н. А. Использование чат-ботов на основе искусственного интеллекта в маркетинге / Н. А. Васильев, А. А. Пшигусов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 2. С. 438–443.

7. Островский Ю. Н., Тихонов С. С., Виткевич Н. Л. Модель интеллектуальной информационно-образовательной системы военного вуза в условиях цифровой трансформации образования // Педагогические технологии: тенденции развития и опыт внедрения в образовательный процесс. Материалы научно-методической конференции: сб. науч.ст. СПб., 2023. С. 119–126.

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛИРОВАНИЕ АТАК НА ОСНОВЕ MICROSOFT KUBERNETES THREAT MATRIX

Д. П. Спиридонов, Е. В. Федорченко

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

²Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

На сегодняшний день использование Kubernetes в области информационных технологий получило широкое распространение. Данная платформа позволяет развернуть и наладить облачную инфраструктуру. В работе рассматривается возможность моделирования атак на основе Microsoft Kubernetes Threat Matrix. Моделирование атак позволяет оценить уязвимость системы Kubernetes к известным атакам, а также определить набор необходимых средств защиты и минимизировать ущерб от возможных атак.

Microsoft Kubernetes Threat Matrix, Kubernetes, Docker, Моделирование атак, bas

В настоящее время Kubernetes становится все более популярной средой для развертывания и управления контейнерами Docker и выполнения их балансировки. Однако, с ростом популярности Kubernetes, увеличивается количество угроз безопасности для этой среды. Моделирование атак на основе Microsoft Kubernetes Threat Matrix (рис.1) является инструментом анализа информационной безопасности среды Kubernetes [1].

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access Kubernetes API server	Access cloud resources	Images from a private registry	Data destruction
Compromised image in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Collecting data from pod	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Exposed sensitive interfaces	Application credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container	Container service account			Access managed identity credentials	Instance Metadata API	Writable hostPath mount		
	Sidecar injection	Static pods			Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Рис. 1. Матрица атак Microsoft Kubernetes

Kubernetes является проектом с открытым исходным кодом, предназначенным для управления кластером контейнеров Linux как единой системой. Он представляет из себя программную платформу для гибкой работы распределенных систем. Kubernetes предоставляет следующий функционал [2]:

- масштабирование и обработка ошибок, возникающих в инструментах;
- шаблоны развертывания большого количества контейнеров;
- выявление контейнеров с высоким уровнем трафика и балансировка нагрузки и распределение сетевого трафика;
- автоматическое монтирование системы хранения по выбору;
- размещение контейнеров на узлах таким образом, чтобы наиболее эффективно использовать ресурсы;
- перезапуск отказавших контейнеров, замена и завершение работы контейнеров, которые не проходят определенную пользователем проверку работоспособности.
- управление конфиденциальной информацией и конфигурацией.

Kubernetes это не монолитное решение, поэтому указанный функционал является дополнительным и подключаемым.

Рассмотрим существующие методы проведения атак в Kubernetes.

1. Сканеры на наличие уязвимостей. Для сканирования на наличие уязвимостей существуют как платные решения, так и с открытым исходным кодом (open source). Например, сканер grype [3] предназначен для сканирования образов контейнеров на наличие уязвимостей и позволяет находить уязвимости в исходных файлах программного обеспечения. Kube-hunter [4] является проектом с открытым исходным кодом (open source) и в отличие от предыдущего решения в первую очередь анализирует и оценивает защиту кластера с точки зрения злоумышленника.

2. Тесты на проникновение (или пентесты). Выполняются вручную сотрудниками компании или внешними консультантами, которые пытаются оценить защищенность инфраструктуры организации путем ее взлома при помощи применения тактик и техник, описанных в матрице:

- использование учетных данных от облачного сервиса;
 - скомпрометированный образ, куда заранее был загружен вредоносный код, позволяющий совершать действия вредоносного характера, например, удаленный доступ в кластер, поэтому вопрос контроля целостности относится к образам ничуть не менее, чем к важным исполняемым файлам;
 - файл `kubeconfig` содержит все данные для подключения к кластеру.
- Если никакие методы защиты не внедрены, злоумышленник получает доступ.

- уязвимое приложение в кластере;
- открытый дашборд – это инструмент для визуализации и анализа информации. Для управления кластерами некоторые используют дашборды; в

отдельных случаях их даже делают доступными из глобальной сети и это можно использовать для проведения DDoS атаки.

Однако у данных методов есть существенные недостатки: трудоемкость, большие сроки проведения и отсутствие автоматизации. Эти недостатки отсутствуют у метода моделирования и проведения кибератак Breach and Attack Simulation (BAS).

BAS является инструментом для моделирования и оценки, позволяющим произвести комплексное тестирование защиты инфраструктуры в реальном времени.

Определим функциональные и нефункциональные требования к методике на основе BAS для Kubernetes.

Функциональные требования: возможность моделировать различные типы атак; возможность моделировать многошаговые атаки; возможность оценивать эффективность защитных механизмов и мер безопасности.

Нефункциональные требования представляют собой описание характеристик, которые не связаны напрямую с работоспособностью основных функций методики в Kubernetes, но влияют на способность системы выполнять поставленные задачи без затрагивания большого количества ресурсов, предоставляя пользователю понятную среду: оптимизация вычислительных мощностей; простота эксплуатации программного обеспечения.

Таким образом моделирование атак с использованием BAS позволяет быстрее и качественнее оценить безопасность, уязвимости, а на основе полученных данных разработать методы по защите. В дальнейшей работе планируется рассмотреть имитацию целенаправленных атак и оценку защищенности с использованием данного метода.

Список используемых источников:

1. Microsoft Kubernetes Threat Matrix. URL: <https://microsoft.github.io/Threat-Matrix-for-Kubernetes>
2. Документация по Kubernetes. URL: <https://kubernetes.io/ru/docs/home>
3. Scanner gype. URL: <https://github.com/anchore/gype>
4. Kube-hunter. URL: <https://github.com/aquasecurity/kube-hunter>

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, Е. В. Федорченко.

УДК 004.05
ГРНТИ 20.15.13

КРИПТОВАЛЮТЫ И БЛОКЧЕЙН: ОТВЕТСТВЕННОСТЬ И ПОТЕНЦИАЛ В ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

К. М. Стрелец, А. П. Шабанов

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

В статье поднимается вопрос о роли и потенциале криптовалют и блокчейн технологий в цифровизации государственного управления и предоставлении государственных услуг. Исследуются преимущества криптовалют, включая улучшение прозрачности и снижение издержек, а также преимущества блокчейн технологий, такие как надежность данных и улучшенная система идентификации. Рассматриваются кейсы из различных стран и выделяются вызовы, стоящие перед интеграцией этих технологий в государственный сектор.

цифровизация, государственное управление, блокчейн, технологии распределенного реестра, криптовалюты, цифровые валюты, электронный документооборот, электронное голосование

В современном мире можно проследить четкую тенденцию роста интереса к цифровизации государственного управления. За последние годы в Российской Федерации значительно выросла популярность единого государственного портала «Госуслуги», который ощутимо повысил качество и скорость государственных и муниципальных услуг для физических и юридических лиц. С другой стороны, в современном мире также наблюдается усиливающийся интерес к блокчейн технологии и областям их применения. Одним из главных преимуществ этих технологий является высокая надежность. Вследствие этого возникает закономерный вопрос о потенциале использования блокчейн технологии в области государственного управления, где надежность системы является ключевым фактором работы.

Актуальность данной темы определяется государственными потребностями в постоянном совершенствовании системы государственного управления и предоставлении государственных услуг. В современном информационном обществе, где цифровые технологии играют ключевую роль, возникает необходимость в поиске инновационных решений для оптимизации и улучшения работы государственных органов. В этом контексте криптовалюты и блокчейн технологии представляют собой перспективные инструменты, которые могут эффективно применяться для повышения прозрачности, безопасности и эффективности государственного управле-

ния. Тема оценки их ответственности и потенциала в цифровизации государственного управления становится все более актуальной в свете стремления государств к созданию современных и адаптивных систем управления, способных эффективно отвечать на вызовы современного мира.

На основе определения, которое дал Кембриджский словарь [1], будем рассматривать блокчейн как систему, используемую для создания цифровой записи всех событий изменения данных или их обмена, которая постоянно растет с добавлением новых блоков. Блокчейн технологии обладают рядом преимуществ:

- децентрализованность, т. е. отсутствие единого центра принятия решений;
- невозможность отмены транзакции;
- прозрачность системы;
- высокая надежность системы в силу децентрализованности.

На основе представленных преимуществ можно выделить несколько основных областей применения блокчейн технологии в рамках государственного управления. Во-первых, технология может использоваться для реализации электронного голосования. Такое решение обеспечит прозрачность и достоверность результатов выборов. Однако такое применение блокчейн технологии будет дорогостоящим в силу большого количества транзакций. Как сообщает ЦИК Российской Федерации [2] на прошедших выборах президента РФ явка составила 77,49%, а это 87,5 млн человек: в среднем 337,5 потенциальных транзакций в секунду. Таким образом, при применении блокчейн-технологии для реализации системы электронного голосования получится дорогая в обслуживании и создании, но неприступная и прозрачная система. Это можно наглядно видеть на следующей гистограмме (см. рис. 1).

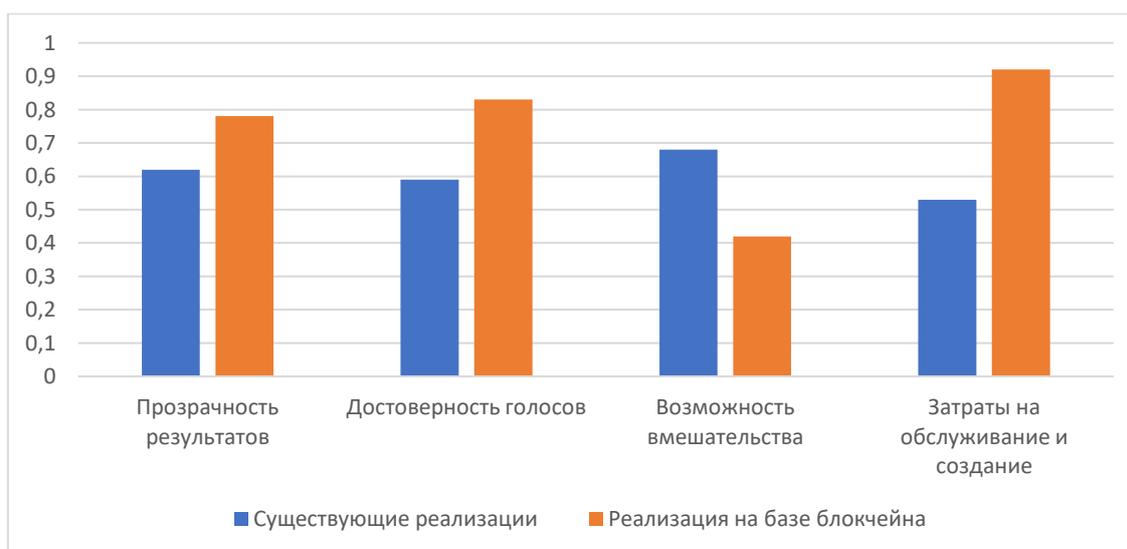


Рис. 1. Сравнение разных реализаций электронных выборов

В «Дорожной карте развития «сквозной» цифровой технологии «Системы распределенного реестра» выделяется [3], что внедрение технологии распределенного реестра (блокчейн технологии, в частности) в сферу государственного медицинского обслуживания представляет собой перспективное направление развития. Это позволит значительно повысить безопасность процессов хранения и передачи персональных медицинских данных. Такое решение несет в себе в целом большое количество положительных результатов для медицины в России: начиная от уменьшения бюрократии и заканчивая сокращением оборота контрафактных лекарств. Однако внедрение блокчейн технологии в сферу государственного медицинского обслуживания может повлечь за собой не только технические и финансовые, но и правовые, кадровые и организационные трудности. Таким образом, на данный момент подобное решение, как минимум, требует строгого планирования, а, как максимум, может восприниматься со скепсисом. Более подробный анализ предложенной реализации представлен на диаграмме (см. рис. 2).

Если говорить о блокчейн технологии, то будет тяжело игнорировать ее влияние на финансовую систему. Конечно, ведь наибольший потенциал эта технология имеет в рамках формирования цифровых валют. На данный момент уже проходит тестирование «цифрового рубля», который должен встать на один уровень с наличной и безналичной формами рубля. Новую цифровую валюту будет выпускать и регулировать Центральный Банк России, а обменный курс к рублю составит 1:1.

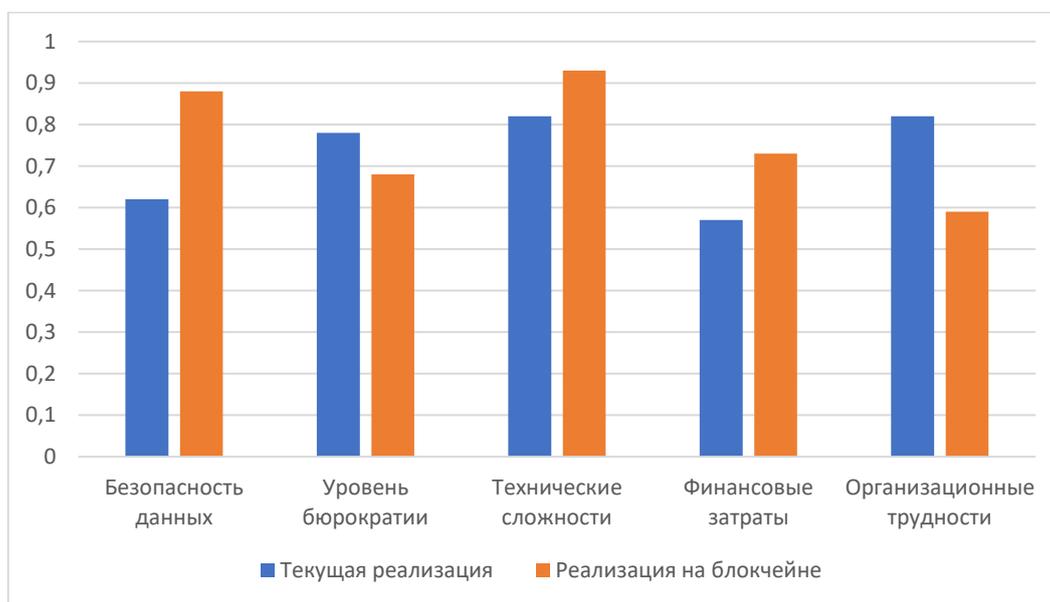


Рис. 2. Сравнение разных реализаций хранения и передачи данных для сферы государственного медицинского обслуживания

Цифровой рубль должен стать еще одним средством для платежей и переводов. Главной его особенностью станет полная свобода от ограничений банков: комиссий и лимитов [4]. Такое решение позволит упростить и удешевить процесс переводов средств, а также операции купли-продажи не только для рядового гражданина, но и для предприятий малого и среднего бизнеса. В отличие от уже существующего USDT (United States Dollar Tether) [5] Цифровой рубль будет являться платежным инструментом и полностью обеспечиваться Центральным Банком Российской Федерации.

Невероятно требовательными к целостности и безопасности данных, как деньги, могут быть еще и документы. Электронные подписи, печати и документы уже входят в повседневную жизнь и для достижения лучшей защиты от злоумышленников и большей прозрачности и надежности было бы правильно рассмотреть перспективу внедрения технологии системы распределенного реестра в государственный документооборот. Помимо очевидных достоинств (см. рис. 3) такое решение позволит упростить сам процесс документооборота за счет автоматизации отслеживания подтверждения подлинности документов, а также снизить издержки, благодаря исключению посредников, увеличению эффективности за счет прозрачности и уменьшению риска мошенничества и ошибок. При всех возможных достоинствах пока что правовая основа для регулирования блокчейн технологий в сфере документооборота не определена. Что важнее, возникает острый вопрос о сохранении конфиденциальности большого количества документов из-за прозрачности блокчейн технологии. Все эти недостатки не позволяют использовать технологию системы распределенного реестра в государственном документообороте даже в ближайшем будущем.

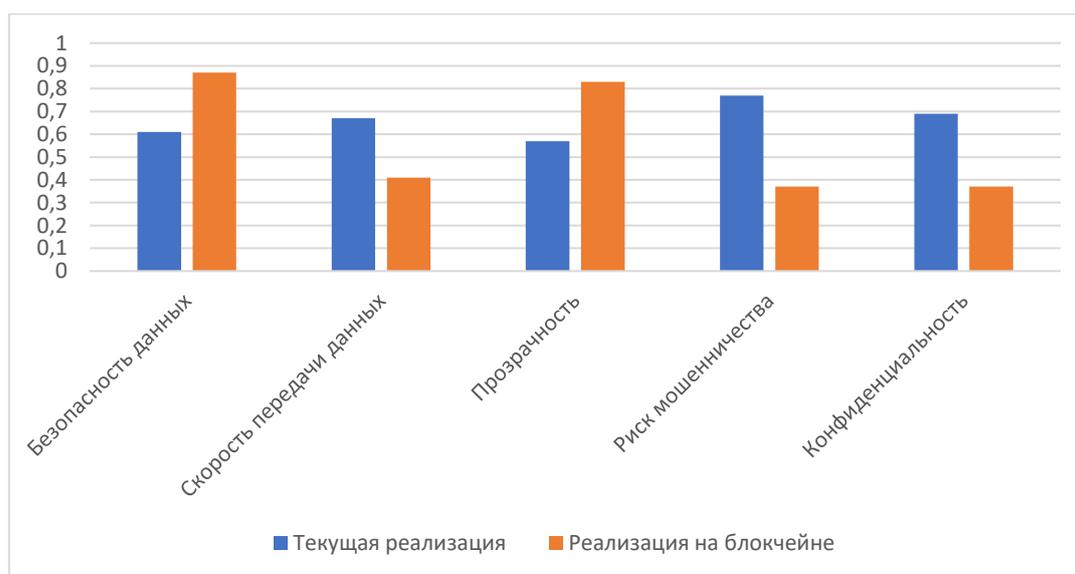


Рис. 3. Сравнение разных реализаций государственного документооборота

Использование блокчейн технологии в государственном управлении представляет собой перспективное направление развития, которое может привести к значительным улучшениям в прозрачности, безопасности и эффективности государственных систем. Преимущества такого внедрения включают децентрализацию, невозможность отмены транзакций, открытость и высокую надежность системы. Однако, несмотря на перспективы, отсутствие правовой базы и вопросы конфиденциальности данных требуют серьезного внимания со стороны законодателей и специалистов в области информационной безопасности. Таким образом, внедрение блокчейн технологии в государственное управление имеет значительный потенциал для улучшения качества услуг и оптимизации процессов, однако требует внимательного рассмотрения ограничений и разработки соответствующих правовых и технических механизмов для обеспечения безопасности и конфиденциальности данных002E.

Список используемых источников

1. Cambridge Advanced Learner's Dictionary & Thesaurus: Cambridge University Press (дата обращения 24.03.2024)
2. ЦИК РФ. «ЦИК России утвердила результаты выборов Президента Российской Федерации». URL: <http://www.cikrf.ru/news/сес/54817> (дата обращения: 24.03.2024)
3. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации «Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра». URL: <https://digital.gov.ru/ru/documents/6670> (дата обращения: 26.03.2024)
4. Банк России. «Цифровой рубль». URL: <https://cbr.ru/fintech/dr> (дата обращения 26.03.2024)
5. Binance Academy – «Что такое USDT?». URL: <https://academy.binance.com/ru/articles/what-is-tether-usdt> (дата обращения 28.03.2024)

Статья представлена научным руководителем, заведующим кафедрой ИСАУ СПбГУТ, доктором технических наук, профессором Г.В. Верховой.

УДК 004.93
ГРНТИ 49.03.05

ВЕРИФИКАЦИЯ АНОМАЛИЙ ПРИ ОБРАБОТКЕ ПАНОРАМНЫХ ИЗОБРАЖЕНИЙ

А. К. Трофименков

Академия Федеральной Службы Охраны России

Синтез панорамных изображений, сгенерированных из видеокадров, полученных с камеры беспилотных летательных аппаратов, показывает, что возникают искажения в ходе работы алгоритма склейки исходных снимков в панораму. Процедуру установления достоверности обнаруженных аномалий можно рассматривать как их верификацию.

аномалии, нечеткие множества, обнаружение, панорамные изображения, фильтрация

Методы пространственной фильтрации лежат в основе улучшения полученных изображений за счет верификации аномалий, которая обусловлена наличием ложных срабатываний при их детектировании [1-3]. При этом используется пиксельная обработка изображения [4], последовательно исследуя окрестность каждой точки изображения.

В общем случае процесс пространственной обработки, можно представить выражением:

$$g(x, y) = T[f(x, y)],$$

где $f(x, y)$ – входное изображение, $g(x, y)$ – обработанное изображение, T – оператор над f , определенный в некоторой окрестности точки (x, y) . Оператор T может быть применим к одному изображению или же к набору изображений.

Пространственный фильтр состоит из области окрестности (например, 3x3 пикселя) и заданной операции. Фильтрация создает новый пиксель, значение которого зависит от оператора фильтра, а координаты совпадают с координатами центра окрестности.

В случае поэлементной обработки, при которой результирующее значение элемента зависит лишь от яркости соответствующего исходного элемента, выполняется преобразование вида $g(x, y) = 1$ при $f(x, y) \geq U$ или $g(x, y) = 0$ при $f(x, y) < U$, где U – некоторое "пороговое" значение яркости [5]. Для этого производится анализ гистограммы яркостей. В случае одного объекта на гистограмме должно быть два максимума. Порог U выбирается между этими двумя максимумами, хотя на практике характерен некоторый

разброс яркостей. Но, выполнение таких условий сильно ограничивает возможности по решению задачи обнаружения границ однородных областей.

Решая задачу в определениях "четкого" множества любой элемент либо принадлежит, либо не принадлежит заданному множеству, поэтому функция принадлежности принимает лишь два возможных значения – ноль или единица. Таким образом, все уровни яркости ниже пороговой величины U устанавливаются равными 0 (черный цвет), а все выше и равные пороговой величине – равными самому высокому значению – 1 (белый цвет).

Для уточнения и совершенствования существующей информационной модели предлагается использовать математический аппарат нечетких множеств для пространственной фильтрации изображений.

При определении нечеткого множества обычно задают значения функции принадлежности [5–8]. В качестве функции принадлежности можно, например, выбрать эмпирическую функцию $m(x)$:

$$m(x) = (1 + x^2)^{-1}.$$

Величина порога для принятия решения предлагается выбрать равной 0,5 с возможностью дальнейшей её модификацией. Если разность яркости соседних пикселей небольшая, то область изображения будет считаться однородной. Если величина отклонения яркости будет превышать установленное значение, то принимается решение о границе однородной области. Дополнительная проверка с помощью специальной процедуры верификации неоднородностей в ПО позволяет усовершенствовать информационную модель обнаружения аномалий на панорамных изображениях.

Применение подхода, основанного на аппарате нечетких множеств, с выбранной функцией принадлежности и величиной порога может привести к снижению вероятности ложных срабатываний на 20% в процессе верификации. Следовательно, совершенствование информационной модели обнаружения аномалий заключается в применении "мягких" решений в условиях неопределенности и неоднозначности при обработке больших массивов данных [9].

Для каждого уникального случая потребуется проводить дополнительную настройку алгоритма, добиваясь наилучших результатов по верификации аномалий, что также позволит выбрать функцию принадлежности и порог срабатывания. Применение "мягких" решений и математического аппарата нечетких множеств позволяют производить обнаружение участков локальной стационарности элементов (объектов) изображения. Результаты исследования показывают значительный эффект для верификации аномалий в панорамных изображениях. Для осуществления подобной процедуры необходима база эталонных изображений и система обучения для достижения целей обработки. Использование математического аппарата нечетких

множеств для осуществления верификации аномалий позволит автоматизировать процесс обработки панорамных изображений и развивать переход к системам искусственного интеллекта.

Список используемых источников

1. Архипов П. О., Цуканов М. В. Информационная технология детектирования аномалий при аэрофотосъемке территорий с объектами жилищно-коммунального хозяйства // Высокие технологии и инновации в науке: сборник статей Международной науч. конф., Санкт-Петербург, июль 2019 г. СПб.: ГНИИ «Нацразвитие», 2019. С.138–144.
2. Архипов П. О., Цуканов М. В. Алгоритмическая модель метода детектирования аномалий при аэрофотосъемке объектов жилищно-коммунального хозяйства // Информационные системы и технологии. 2019 № 6(116). С. 39–45.
3. Архипов П. О., Цуканов М. В. Алгоритмическая модель обнаружения аномалий на разновременных панорамах // Системы высокой доступности. 2021. Т. 17. № 2. С. 5–10. DOI: 10.18127/j20729472-202102-01
4. Архипов П. О., Трофименков А. К., Цуканов М. В., Носова Н. Ю. Исследование методов детектирования ключевых точек при создании панорамных изображений // Системы и средства информатики. 2022. Т. 32 № 2 С. 92–104. DOI: 10.14357/08696527220209
5. Архипов П. О., Трофименков А. К., Цуканов М. В. Применение нечетких множеств в задаче обнаружения аномалий на сравниваемых панорамах // Системы высокой доступности. 2023. № 2. С. 46–54. DOI: 10.18127/j20729472-202302-04
6. Гонсалес Р., Вудс Р. Цифровая обработка изображений. 3 изд., испр. и доп. М.: ТЕХНОСФЕРА, 2012. 1104 с.
7. Методы компьютерной обработки изображений / под ред. В.А. Сойфера, 2 изд., испр. М.: ФИЗМАТЛИТ, 2003. 784 с.
8. Коньшева Л. К., Назаров Д. М. Основы теории нечетких множеств: учебное пособие. СПб.: Питер, 2011. 192 с.
9. Trofimenkov A. K., Tsukanov M. V., Nosova N. Y. Modification of an algorithmic model for detecting anomalies on panoramas of different times obtained from unmanned aerial vehicles // Modern informatization problems in simulation and social technologies (MIP-2022'SCT): Proceedings of the XXVII-th International Open Science Conference (Yelm, WA, USA, January 2022) / Editor in Chief Dr. Sci., Prof. O.Ja. Kravets. Yelm, WA, USA: Science Book Publishing House, 2022. PP.183–186.

УДК 656.073.7
ГРНТИ 50.49.31

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ЭЛЕМЕНТНОЙ БАЗЫ РАДИОЭЛЕКТРОНИКИ

М. В. Фёдорова, О. К. Югай

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

В последнее время, благодаря активному развитию IT технологий, стремительно развивается сфера цифрового учёта и контроля в различных сферах человеческой деятельности. Высокая степень автоматизации позволяет сокращать рабочее время, что служит существенным стимулом повышения производительности труда, а также избежать ряд ошибок, свойственных человеку, и как следствие – максимизировать прибыль и минимизировать трудовые затраты. В статье рассмотрено специально разработанное web-приложение, функционал которого позволяет вести учёт наличия у производителя комплектующих для производства радиоэлектронных устройств.

цифровой учет, автоматизация, производительность труда, трудовые затраты, web-приложение

При выборе стека разработки было рассмотрено два актуальных на данный момент времени набора технологий. Рассмотрим альтернативный стек технологий:

1. Angular с TypeScript – фреймворк, разработанный Google для построения веб-приложений, используется для разработки SPA (Single Page Application) и обеспечивает высокую производительность приложений. TypeScript обеспечивает статическую типизацию для JavaScript и имеет возможность интеграции с Angular, что позволяет сократить количество ошибок в коде и упростить его отладку [1].

2. Vuex – библиотека для управления состоянием в приложениях Vue.js. Она предоставляет централизованное хранилище для всех компонентов приложения и обеспечивает однонаправленный поток данных.

3. Tailwind CSS – набор готовых компонентов и классов CSS (Cascading Style Sheets) для быстрой разработки современного пользовательского интерфейса. Он позволяет создавать пользовательские стили без необходимости написания CSS, что существенно ускоряет работу и упрощает те её аспекты, которые связаны с созданием адаптивного дизайна.

4. Express.js – оптимизированный и гибкий веб-фреймворк для Node.js. Он позволяет легко создавать серверные приложения и обрабатывать HTTP-запросы, прост в изучении и может использоваться в том числе и начинающими специалистами.

Далее обоснуем выбор итогового стека технологий:

1. React с TypeScript – является обновлением DOM (Document Object Model) и упрощает создание компонентов построения пользовательского интерфейса. TypeScript имеет статическую типизацию, что повышает читаемость кода и уменьшает количество ошибок на этапе разработки, в сравнении с классическим JavaScript.

2. Redux – единое хранилище для управления состоянием приложения, оно делает управление данными предсказуемым и централизованным. Данная особенность позволяет избегать ошибок при построении приложений с большим объемом состояния и сложной логикой взаимодействия компонентов. Именно таким является рассматриваемое приложение.

3. Bootstrap – предоставляет готовые стили и компоненты, что ускоряет создание современного и адаптивного дизайна веб-приложений. За счёт использования сеточной системы значительно упрощается работа по расположению элементов пользовательского интерфейса. Встроенные шаблонные элементы обладают адаптивностью, за счёт чего программист экономит время разработки, не теряя его на создание адаптивную вёрстку.

4. Django – высокоуровневый веб-фреймворк, в котором оптимизирован процесс создания веб-приложений на Python. Включение ORM (Object-relational mapping), маршрутизации и административного интерфейса позволяет избежать больших трудовых затрат на создание данных функций и сосредоточить работу программиста на описании и создании архитектуры баз данных, создании методов.

Выбор итогового стека React с TypeScript, Redux, Bootstrap и Django был обусловлен их широким распространением, высоким уровнем автоматизации ряда процессов, специализацией на обработке больших объёмов информации и включённом в шаблоны компонентов адаптивном дизайне, что делает его оптимальным для разработки современных и высокопроизводительных веб-приложений [2].

Процесс разработки веб-приложения с использованием технологий React с TypeScript, Redux, Bootstrap и Django может быть разделен на несколько основных этапов.

Далее рассмотрим общий план разработки и функциональности приложения.

1. Анализ требований:

- определить функциональные и нефункциональные требования к вашему приложению;
- разработать структуру базы данных (ERD (Entity-Relationship Diagram) -модель);
- определить основные сущности и их взаимосвязи.

2. Проектирование интерфейса:

- создать макет пользовательского интерфейса приложения;
- определить основные страницы, компоненты и их внешний вид;

- учесть принципы адаптивности дизайна и удобства использования.
- 3. Настройка окружения разработки:
 - установить необходимые инструменты и зависимости, такие как Node.js, npm (или yarn), TypeScript, Redux DevTools, Django, и другие;
 - создать базовую структуру проекта путём запуска одного из стандартных скриптов в консоли или же путём взаимодействия с выбранной средой разработки.
- 4. Разработка фронтенда (React с TypeScript и Redux):
 - создать компоненты и страницы, учитывая структуру макета;
 - использовать Redux для управления состоянием приложения, создать действия и редьюсеры;
 - реализовать взаимодействие с бэкендом через API (Application Programming Interface), написанный на Django;
 - интегрировать Bootstrap для стилизации компонентов и обеспечения адаптивности.
- 5. Разработка бэкенда (Django):
 - определить модели данных на основе структуры базы данных (ERD-модели).
 - создать Django API для обработки запросов от фронтенда;
 - реализовать CRUD-операции (Create, Read, Update, Delete) для основных сущностей;
 - обеспечить аутентификацию и авторизацию пользователя.
- 6. Интеграция фронтенда и бэкенда:
 - связать фронтенд и бэкенд через API. Проверить, что данные успешно передаются и обрабатываются;
 - логировать возможные ошибки и убедиться, что приложение обрабатывает ответы от сервера.
- 7. Тестирование:
 - написать модульные тесты для компонентов, действий и редьюсеров в React;
 - создать интеграционные тесты для проверки взаимодействия между фронтендом и бэкендом;
 - провести тестирование на уровне пользовательского интерфейса, проверяя весь функционал приложения.
- 8. Отладка и оптимизация:
 - использовать инструменты отладки такие как Redux DevTools и инструменты разработчика браузера для выявления и устранения ошибок;
 - оптимизировать производительность приложения, устраняя лишние затратные процессы и упрощая запросы к бэкенду.
- 9. Документация:
 - создать документацию для кода, API и структуры базы данных;
 - описать процесс установки и запуска приложения.

10. Развертывание:

- развернуть бэкенд на сервере с использованием Django;
- разместить фронтенд на хостинге или CDN (Content Delivery Network);
- проверить, что приложение успешно работает в реальной среде.

11. Поддержка и обновление:

- обеспечить непрерывное обслуживание и мониторинг приложения;
- регулярно обновлять зависимости и исправлять возможные ошибки.

Отдельно следует отметить, что при разработке фронтенда следует создавать универсальные компоненты, которые возможно интегрировать в других частях приложения, что облегчает как навигацию внутри структуры проекта, так и способствует упрощению внедрения адаптивности в страницы приложения [3].

В процессе разработки веб-приложения фронтенд и бэкенд части должны взаимодействовать для обмена данными. Для этого широко используется API (Application Programming Interface) – набор методов и структур данных, который определяет способы взаимодействия между различными компонентами программного обеспечения [4].

В данном случае, при использовании React TS для фронтенда и Django для бэкенда, взаимодействие осуществляется через HTTP-запросы и RESTful API. Это происходит следующим образом:

1. Определение эндпоинтов.

В Django определяют URL-маршруты (endpoints), которые будут обрабатывать запросы от фронтенда. Каждый эндпоинт связан с определенной функциональностью, например, получение списка компонентов, добавление нового устройства и т. д.

2. HTTP-запросы с фронтенда.

С клиентской части отправляются HTTP-запросы к определенным эндпоинтам с использованием функций, предоставляемых библиотекой Axios. Когда пользователь выполняет действие (например, нажимает кнопку), фронтенд посылает соответствующий запрос на бэкенд.

3. Обработка запросов на бэкенде.

В Django создаются соответствующие функции-обработчики для каждого эндпоинта, которые выполняют необходимые действия, такие как получение данных из базы данных или изменение состояния.

4. Передача данных.

Данные передаются между фронтендом и бэкендом в формате JSON. Фронтенд отправляет запросы с определенными параметрами, и бэкенд отвечает данными в формате JSON, которые затем обрабатываются на фронтенде.

Фронтенд может затем использовать полученные данные для обновления интерфейса или выполнения других действий [5].

Использование API для взаимодействия между фронтендом и бэкендом позволяет четко разделить функциональность приложения и обеспечивает гибкость в расширении и изменении системы.

В современном мире, где технологические инновации играют ключевую роль в различных сферах, разработка автоматизированной системы учета элементной базы радиоэлектроники становится крайне актуальной задачей. Реализация стека технологий, включающего React с TypeScript, Redux, Bootstrap и Django, позволяет не только повысить эффективность процессов учета, но и улучшить надежность и точность данных.

Перспективы дальнейшего развития этой системы включают в себя ее последующее совершенствование и интеграцию с новыми технологиями для обеспечения более высокой производительности и функциональности.

Список используемых источников

1. Крупина Т.А. Обработка и хранение данных в Web-приложении. Гуманитарные научные исследования, 2016. № 9. URL: <https://human.snauka.ru/2016/09/16589> (дата обращения 21.02.2024)
2. Bootstrap Documentation. URL: <https://getbootstrap.com/docs/5.0/getting-started/introduction> (дата обращения 21.02.2024)
3. Django Documentation. URL: <https://docs.djangoproject.com/en/4.0/> (дата обращения 20.02.2024)
4. Крупина Т. А., Щербакова С. М. Современные средства разработки интернет-сайтов и Web-приложений // Гуманитарные научные исследования. 2016. № 9. URL: <https://human.snauka.ru/2016/09/16590> (дата обращения 22.02.2024)
5. TypeScript Documentation. URL: <https://www.typescriptlang.org/docs> (дата обращения 21.02.2024)

УДК 656.073.7
ГРНТИ 50.49.31

СИСТЕМА АВТОМАТИЗАЦИИ УЧЕТА ТОВАРОВ И УПРАВЛЕНИЯ ГРУЗОПЕРЕВОЗКАМИ

М. В. Фёдорова, Д. В. Яковлев

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

В последнее время, благодаря цифровизации, отрасль транспортной логистики уходит от привычной бумажной работы и активного участия человека в процессе управления перевозками и складского учета. Автоматизированные системы включают в себя специализированное программное обеспечение и аппаратную часть для оптимизации распределительных процессов внутри организации. Внедрение данных систем позволяет улучшить коммуникацию между различными подразделениями, сократить время на проведение операций, эффективнее распределять материальные ресурсы и оценивать эффективность сотрудников. В статье рассмотрено спроектированное и разработанное программное обеспечение, которое предоставляет функционал двух подсистем – управления транспортом и складского учета, а также организует взаимодействие между ними.

автоматизация, грузоперевозки, интеграция, мониторинг, REST

Активное развитие цифровых технологий в последнее время не обошло стороной отрасль транспортной логистики. Внедрение автоматизированных систем в транспортные компании предоставляет ряд преимуществ:

- непрерывный обмен информации посредством специализированных систем позволяет улучшить коммуникацию между подразделениями;
- сокращение времени на проведение операций, благодаря их автоматизации по заданным алгоритмам;
- повышение уровня прозрачности операций при логировании и создании записей о процессах, фиксируемых в автоматизированной системе;
- повышение эффективности при распределении материальных ресурсов, за счет оперативного доступа к базам данных, хранящих актуальное цифровое представление всех необходимых ресурсов организации [1];
- оценка эффективности сотрудников, благодаря возможности отслеживать активность сотрудника по действиям, совершаемым им в системе на протяжении рабочего дня;
- снижение доли бумажного документооборота в организации за счет формирования, отправки и хранения документов в электронном виде [2];
- предоставление возможности оперативно реагировать на рыночные изменения, используя обращения к внешним источникам, обработку полученной информации и предоставление её в графическом виде [3].

Проектируемая система автоматизации учета товаров и управления грузоперевозками, описываемая далее, должна предоставлять заказчику все эти преимущества, а также решать определенный круг задач по автоматизации логистических процессов, таких как:

- организация обработки запросов на перевозку грузов с внешней системы, решающей задачи по работе с клиентом;
- отслеживание товаров на складах, их учет и возможность предоставления актуальной информации;
- распределение задач по перевозке груза оператором системы, который назначает водителей на заказы на основе данных о водителях и транспортных средствах;
- отслеживание процесса перевозки груза оператором системы, поддержка водителей на протяжении всего маршрута;
- составление отчетов по различным этапам, что обеспечивает прозрачность производимых операций.

Главная особенность предлагаемой системы заключается в том, что она полностью интегрируема, что позволяет встроить её в уже существующее программное обеспечение организации. На рис. 1 представлены основные подсистемы (внутренние и внешние), использующиеся при работе, а также их взаимодействие.

Первый этап: внешняя система формирования задач для грузоперевозок после обращения клиента отправляет HTTP-запрос в систему управления грузоперевозками.

Второй этап: система управления грузоперевозками принимает запрос и в свою очередь, посылает запрос к системе учета товаров для получения данных о необходимых товарах. Система учета товаров отвечает на этот запрос и посылает запрос системе распределения задач на складе для подготовки товара к отправке. По итогам данного этапа система создает задачу на перевозку груза с необходимыми данными о товаре и клиенте.

Третий этап: оператор системы управления грузоперевозками назначает на задачи водителей, распределяет необходимые материальные ресурсы для выполнения задачи.

Четвертый этап: задача добавляется в мониторинг, оператор получает возможность сопровождать перевозки груза на протяжении всего маршрута.

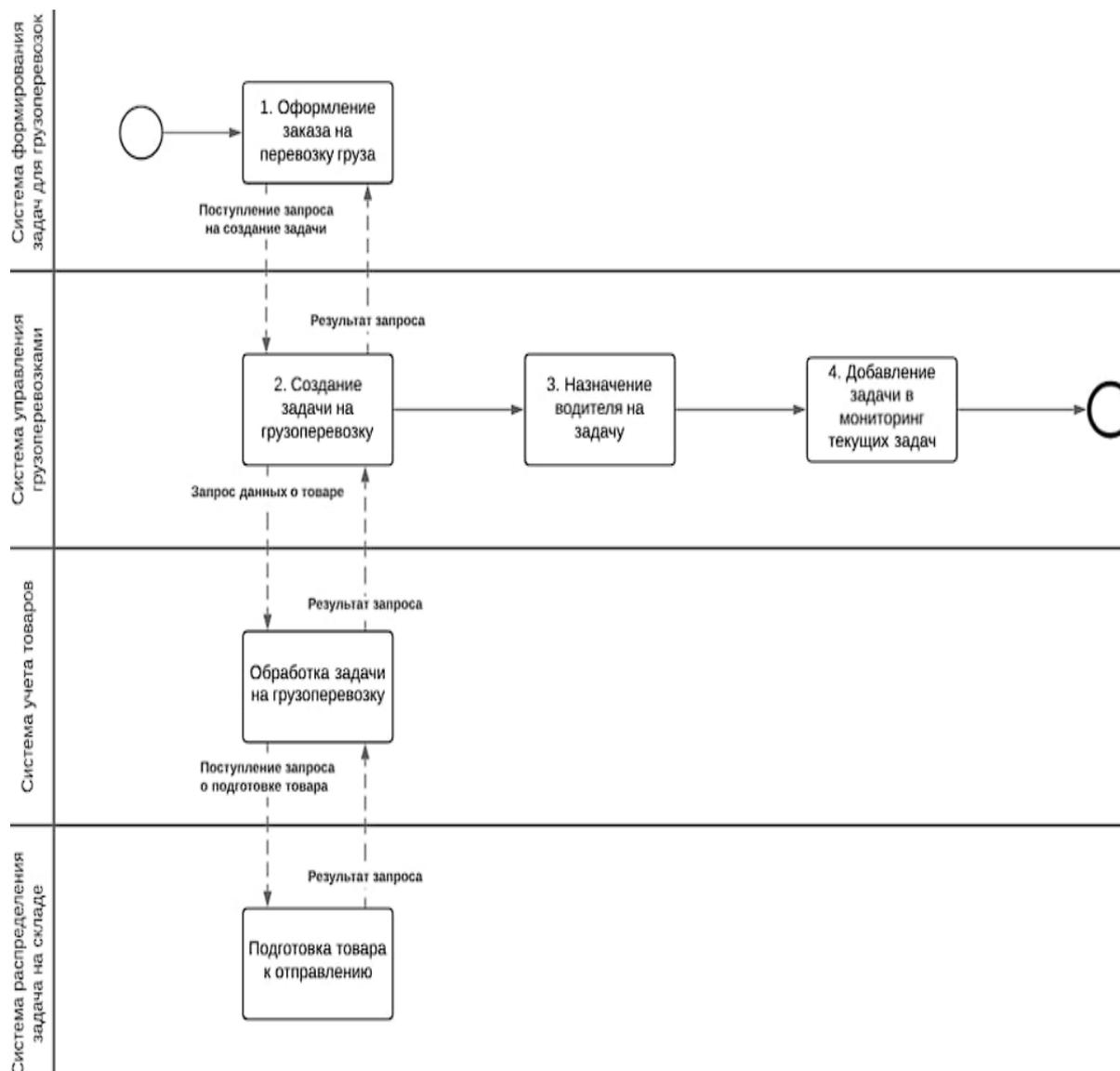


Рис. 1. Схема бизнес-процесса системы управления учетом товаров и управления грузоперевозками

Физическая модель данных системы управления грузоперевозками представлена основной сущностью, которой оперирует система – сущность «задача» (рис. 2). Остальные сущности связаны с задачей при помощи уникальных идентификаторов, носят информативный характер и позволяют сопровождать процесс грузоперевозки.

Физическая модель данных системы учета товаров представлена основной таблицей «товар», которая связана с остальными информативными сущностями «склад», «тип продукта», «адрес», «сотрудник» и «контакт» при помощи ссылочных атрибутов и уникальных идентификаторов (рис. 3).



Рис. 2. Физическая модель данных системы управления грузоперевозками

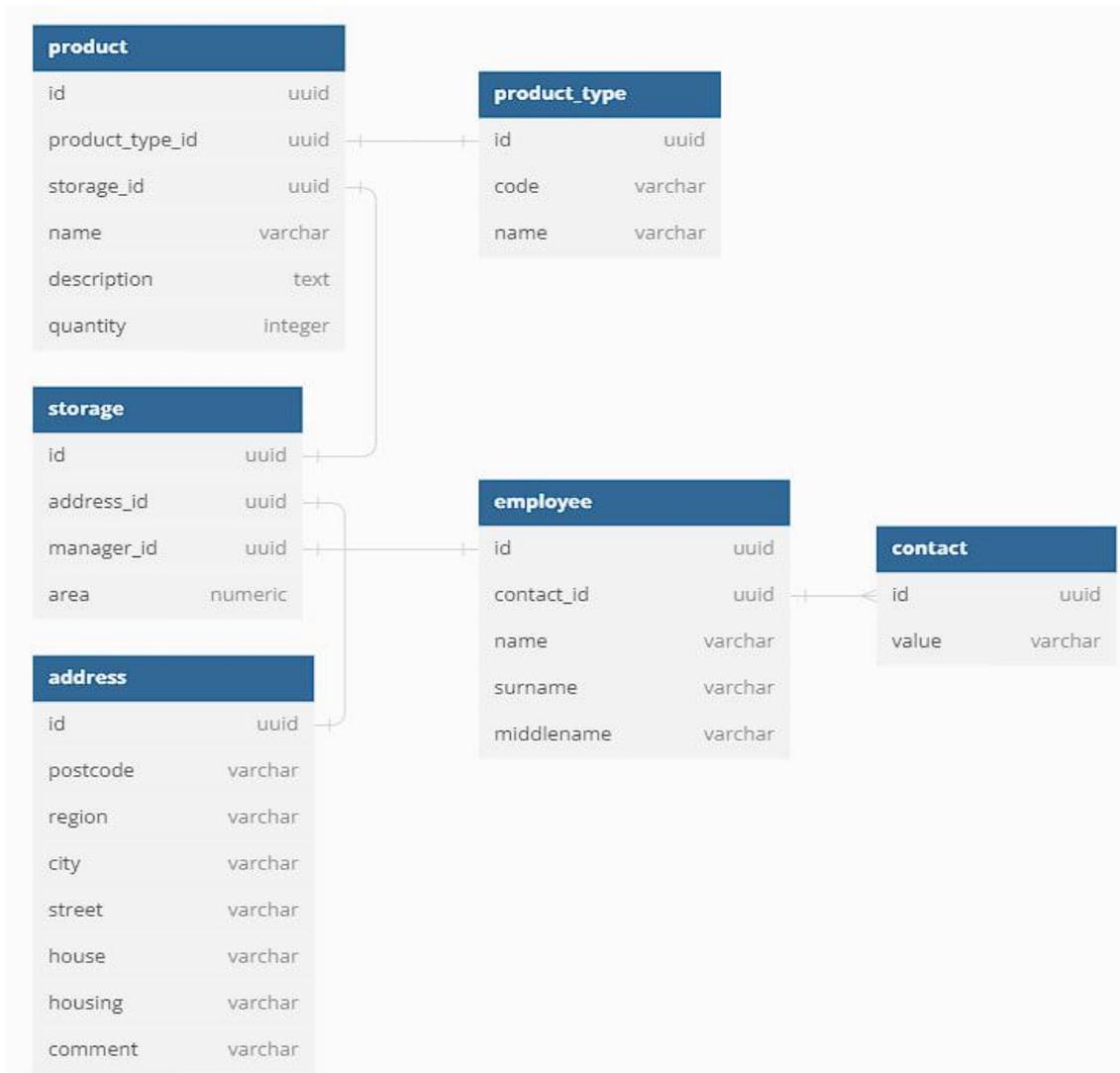


Рис. 3. Физическая модель данных системы учета товаров

Взаимодействие между системами осуществляется при помощи HTTP-запросов. Пример GET-запроса, а также ответ на него, представлен на рис. 4 и рис. 5.

Интеграция системы в существующие решения – несложная задача, реализуемая при помощи REST-сервисов. При необходимости расширения системы новыми подсистемами, можно настроить их взаимодействие в соответствии с существующим API.

[Адрес_rest_сервиса?productId=1&productQuantity=100&storageId=1](#)

Рис. 4. Пример GET-запроса от системы грузоперевозок к системе учета товаров

```
"product": {  
  "id": 1,  
  "name": "test",  
  "product_type": "test",  
  "description": "test",  
  "quantity": 100,  
  "storage": {  
    "id": 1,  
    "area": 1.5,  
    "address": {  
      "id": 1,  
      "region": "test",  
      "city": "test",  
      "street": "test",  
      "house": "test"  
    },  
    "manager": {  
      "id": 1,  
      "name": "test",  
      "surname": "test",  
      "middlename": "test",  
      "contacts": [  
        {  
          "id": 1,  
          "value": "+77773332222"  
        },  
        {  
          "id": 2,  
          "value": "+73333332222"  
        }  
      ]  
    }  
  }  
}
```

Рис. 5. Пример ответа на GET-запрос

Список используемых источников

1. OMNICOМ. Четыре ключевых направления в транспортной цифровизации. URL: <https://omnicomm.su/about/news/chetyre-klyuchevykh-napravleniya-v-transportnoy-tsifrovizatsii> (дата обращения 15.03.2024)

2. Ассоциация РОСЭУ. Цифровизация логистики: планы и перспективы. URL: <https://xn--n1adei3c.xn--p1ai/news/tsifrovizatsiya-logistiki-plany-i-perspektivy> (дата обращения 17.03.2024)

3. 4logist. Цифровизация логистики. URL: <https://www.4logist.com/czifrovizacziya-logistiki> (дата обращения 17.03.2024)

УДК 004.738.5
ГРНТИ 20.23.00

ПРОБЛЕМА АКТУАЛЬНОСТИ ПОИСКОВОЙ ВЫДАЧИ В ЭЛЕКТРОННЫХ БИБЛИОТЕЧНЫХ РЕСУРСАХ

О. О. Хамзина

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

С ростом объема научных публикаций в электронной форме становится все сложнее эффективно искать актуальную информацию. Эта статья исследует проблемы многокритериального поиска в научных электронных библиотечных ресурсах с учетом даты публикации как важнейшего критерия. В статье анализируется влияние многокритериального подхода на эффективность поисковой выдачи, выявляются основные проблемы и предлагаются перспективные пути их решения.

поисковые системы, анализ поисковых систем, многокритериальный поиск

С развитием информационных технологий и цифровизацией научных публикаций доступ к научной информации стал более удобным и быстрым. Однако, с ростом объема доступной информации возникают новые проблемы, связанные с эффективностью поиска. Многокритериальный подход к поиску в научных библиотеках играет ключевую роль в современной научной деятельности. Его важность заключается в том, что он позволяет учитывать не только один критерий при формировании результатов запроса, но и ряд других параметров, значительно повышая точность и релевантность поиска. В контексте электронных научных библиотек, где объем доступной информации постоянно растет, многокритериальный подход становится необходимостью для эффективного извлечения нужной информации из этого огромного объема данных.

Использование многокритериального подхода в электронных научных библиотеках помогает искать более релевантную информацию по нескольким ключевым параметрам одновременно. Например, помимо ключевых слов и авторства, можно учитывать такие факторы, как индекс Хирша [1], рейтинг научного цитирования [2] и дату публикации. Эти факторы являются наиболее значимыми при оценке научной работы, и используются как основные критерии в формировании поисковой выборки электронных научных библиотек. Многокритериальный поиск позволяет исследователям получать более точные и информативные результаты по своим запросам, исключая неактуальные материалы.

Актуальность совершенствования существующих поисковых систем в электронных научных библиотеках выражается в том, что с каждым годом объемы научных статей и публикаций стремительно растут. Это создает

проблему для исследователей, которым все труднее ориентироваться в массе доступной информации и выделить наиболее актуальные и значимые источники. В таких условиях становится необходимым использование более точных поисковых систем, способных учитывать множество критериев при формировании результатов запросов. Именно многокритериальный подход может предоставить исследователям возможность делать более осознанный выбор и обеспечивает более эффективный поиск в условиях постоянно растущего объема научной информации.

Одним из ключевых недостатков существующих систем научных библиотек является их ограниченность в использовании многокритериального подхода к поиску. В настоящее время лишь некоторые поисковые системы, включая Google Scholar [3] и Scopus, реализуют многокритериальный подход в поиске научной информации. Однако, в российском контексте приоритет отдается российским библиотекам, таким как РИНЦ (Российский индекс научного цитирования) и научным порталам национальных университетов, которые, к сожалению, не всегда в полной мере используют многокритериальный подход. Так, например, крупнейшая российская электронная научная библиотека eLibrary.Ru не реализует качественный поиск литературы.

Даже те научные библиотеки, в которых реализован многокритериальный поиск, среди других критериев отдают предпочтение количеству цитирований публикации. Однако в ситуации, когда количество публикаций постоянно растет, хочется отметить такой фактор, как дата публикации. Преимущества внедрения даты публикации в многокритериальный поиск неоспоримы и обусловлены несколькими ключевыми факторами [4].

Во-первых, учет даты публикации позволяет исследователям ориентироваться на последние научные данные. Это особенно важно в быстро развивающихся областях науки, где регулярно появляются новые открытия и исследования. Приоритетный учёт даты публикации позволяет исключить устаревшие и неактуальные источники, обеспечивая исследователям доступ к самой свежей и релевантной информации.

Во-вторых, внедрение даты публикации в многокритериальный поиск способствует более точной оценке развития конкретной научной области. Путем анализа публикаций по временной шкале исследователи могут отслеживать эволюцию темы, выявлять новейшие тенденции и оценивать динамику научных исследований. Это помогает не только в актуализации научных знаний, но и способствует формированию стратегических направлений в дальнейших исследованиях.

Также следует отметить, что учет даты публикации позволяет исследователям выявлять самые значимые и важные работы в конкретный период вре-

мени. Некоторые научные достижения могут иметь особую важность в определенный исторический момент, и их учет при поиске информации позволяет сфокусироваться на ключевых моментах развития науки и технологий.

Таким образом, внедрение даты публикации в многокритериальный поиск обогащает научный поиск, предоставляя исследователям более актуальные и релевантные материалы, а также способствует более глубокому анализу и пониманию динамики развития научных областей.

Однако стоит отметить, что не для всех областей науки источники с последней датой публикации являются одинаково важными. В фундаментальных науках, в которых основные принципы и знания являются постоянными, актуальность даты публикации может иметь меньшее значение, так как основные законы и теории в этих областях остаются неизменными (например, работы Эйлера и Коши в математике или Ньютона и Ома в физике актуальны по сей день, несмотря на то, что были опубликованы несколько веков назад).

В быстроразвивающихся же областях науки дата публикации, напротив, играет ключевую роль. К таким областям, например, относятся медицина, биология, и информационные технологии. В медицине и биологии последние исследования могут существенно повлиять на разработку новых методов лечения, а также на создание лекарств и проведение диагностики заболеваний. В информационных технологиях данные быстро теряют свою актуальность, поэтому новейшие публикации важны для понимания реального состояния отрасли. Это позволяет сделать вывод, что в данных областях науки актуальность даты публикации является ключевым фактором для обеспечения релевантности информации.

Результаты данного анализа подчеркивают важность разработки поисковой системы, основанной на многокритериальном подходе, где ключевым параметром будет дата публикации. Хотя научные электронные библиотеки являются неотъемлемой частью научного процесса, поиск релевантных материалов в них осложнен как огромным объемом информации, так и несовершенством поисковых систем. Многокритериальный подход в поисковых системах позволит исследователям учитывать не только количество цитирований или полнотекстовый поиск, но и иные параметры, в частности дату публикации, что сделает выборку более точной и релевантной. Это наиболее актуально для таких быстро развивающихся областей науки, как медицина, биология и информационные технологии, где использование даты публикации позволит исследователям ориентироваться на самые свежие и актуальные источники. Таким образом, разработка поисковой системы, где основным критерием будет дата публикации, сможет существенно упростить использование электронных научных библиотек и обеспечить доступ к наиболее релевантной информации.

Список используемых источников

1. Назаренко М. А. Индекс Хирша как ключевое слово в современных научных исследованиях / М. А. Назаренко // Современные наукоемкие технологии, 2013. № 4. С. 116–117.

2. Кара-Мурза С. Г. Цитирование в науке и подходы к оценке научного вклада // Вестник Академии наук СССР. 1981. Т. 51, № 5. С. 68–75.

3. Beel J., Gipp B. Google Scholar's Ranking Algorithm: An Introductory Overview // Proceedings of the 12th International Conference on Scientometrics and Informetrics, Rio de Janeiro, Brazil, 2009. V. 1. PP. 230–241.

4. Beel J., Gipp B. Google Scholar's Ranking Algorithm: The Impact of Articles' Age (An Empirical Study) // Proceedings of the 6th International Conference on Information Technology: New Generations, Las Vegas, USA. PP. 160–164.

Статья представлена заведующим кафедрой БИС СПбГУТ, кандидатом технических наук, доцентом Ю. М. Боромянским.

УДК: 004.021
РНТИ 20.23.25

ГДЕ МАШИННОЕ ОБУЧЕНИЕ ОКАЖЕТ НАИБОЛЬШЕЕ ВЛИЯНИЕ?

И. И. Чупахин, П. А. Шиян

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

В данной статье будет проведен сравнительный анализ применения машинного обучения в различных сферах нашей жизни. Будет рассмотрена статистика применения машинного обучения на основе развития технологий и мощностей вычислительных систем.

машинное обучение, искусственный интеллект, естественный язык, компьютерная система, искусственные нейронные сети

В современном мире машинное обучение с каждым годом оказывает существенное влияние на различные сферы нашей жизни, и его применение охватывает множество профессий.

Медицина: машинное обучение применяется для обнаружения и диагностики различных заболеваний, предсказания и оценки рисков, а также для более точного определения эффективных методов лечения. Примеры профессий, затронутых машинным обучением в медицине, включают врачей, медицинских исследователей и специалистов по обработке медицинских данных. Транспорт: машинное обучение играет ключевую роль в развитии самоуправляемых автомобилей и систем управления транспортными потоками, что может существенно улучшить безопасность и эффективность транспортной инфраструктуры. Профессии, затронутые машинным обучением в сфере транспорта, включают инженеров-разработчиков автоматических устройств управления транспортом, аналитиков данных и специалистов по безопасности транспорта. Финансы: машинное обучение помогает в обнаружении финансовых мошенничеств, автоматизации предсказания рыночных тенденций, прогнозировании ценных бумаг и оптимизации инвестиционных стратегий. Профессии, затронутые машинным обучением в сфере финансов, включают финансовых аналитиков, трейдеров и специалистов по управлению рисками. Производство: машинное обучение применяется для улучшения процессов производства, прогнозирования отказов оборудования, анализа данных о качестве продукции и оптимизации цепей поставок. Профессии, затронутые машинным обучением в сфере производства, включают инженеров-производственников, специалистов по операциям и логистике [1].

Базовым элементом применения машинного обучения в области медицины является обширность имеющихся данных в этой сфере. Благодаря прогрессу в сфере цифровой медицинской записи, изображений, геномики и других информационных источников, машинное обучение стало ключевым инструментом для изучения данных и выведения новых знаний, что способствовало почти шестидесятидвукратному увеличению его применений в медицине в течение последних 15 лет (с 2008 по 2023 год). С помощью машинного обучения медицинские специалисты могут диагностировать и прогнозировать широкий спектр заболеваний. Алгоритмы могут обработать значительные объемы пациентских данных и на основе этого предугадать вероятность развития заболевания. Такие системы также применимы для автоматического определения отклонений на медицинских сканах, анализа генетических данных и формулирования персонализированных методик лечения. Внедрение машинного обучения представляет собой перспективу значительного усовершенствования продуктивности здравоохранения [2]. Автоматизация разнообразных операций, таких как обработка данных и создание медицинских отчетов, освобождает время врачей, позволяя им посвящать больше внимания пациентам и принять более обоснованные медицинские решения. Но в то же время, адаптация машинного обучения в сфере медицины сталкивается с определенными трудностями, включая вопросы конфиденциальности медицинских данных, отсутствие стандартизации и регулирования, а также недоверие и сопротивление со стороны некоторых врачей и пациентов, как демонстрируется на рис. 1.

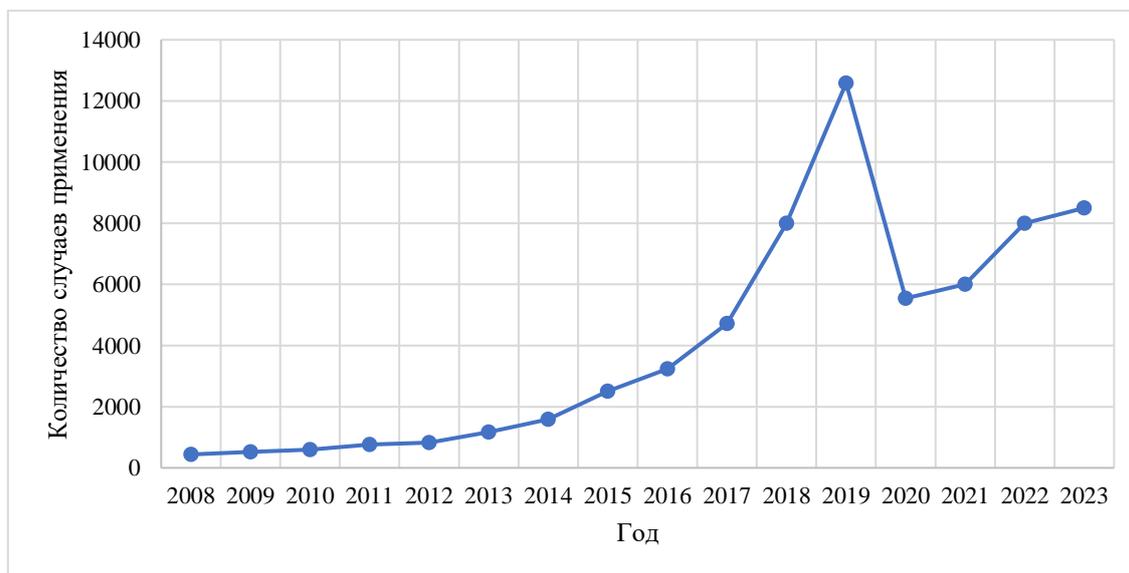


Рис. 1. Применение машинного обучения в сфере медицины

Транспортный сектор генерирует обширный объем данных, включая сведения о движении транспортных средств, расписаниях, численности пассажиров и других релевантных аспектов. Эти данные могут быть

задействованы в процессе тренировки моделей машинного обучения. Благодаря развитию более продвинутых компьютеров и применению облачных технологий, обработка и анализ массивных наборов данных, характерных для городских транспортных систем, стали осуществимы. С этим связано появление и усовершенствование алгоритмов машинного обучения, способных эффективно функционировать с данными из транспортных и навигационных систем, а также предсказывать поведение транспортного потока в определенные моменты времени. В частности, машинное обучение используется в транспорте для совершенствования систем управления движением и маршрутизации, анализа и предсказания потоков трафика и определения наиболее оптимальных маршрутов. Созданы различные интеллектуальные вспомогательные системы вождения авто и автоматизированное управление на железнодорожном транспорте [3]. Алгоритмы машинного обучения могут анализировать пассажиропотоки и прогнозировать потребность в транспортных услугах в разные промежутки времени, способствуя тем самым планированию ресурсов и оптимизации услуг от транспортных компаний. В области безопасности транспортных сетей машинное обучение также находит применение в разработке систем детектирования и предотвращения инцидентов, а также анализе данных с систем видеонаблюдения. Технологии машинного обучения обеспечивают разработку и улучшение алгоритмов для автоматического управления транспортными средствами, включая автономные функции, как система FMS, используемая в самолетах типа Boeing 777, и проекты беспилотных автомобилей, осуществляемые зарубежными компаниями вроде Uber, Tesla и Google. Кроме того, российские инженеры тоже вносят свой вклад в данную область – так, компания "Яндекс" с 2017 года занимается разработкой собственных автономных систем, которые уже установлены на некоторые автомобили, как показано на рис. 2.



Рис. 2. Беспилотный автомобиль Яндекс

В отличие от зарубежных стран, в России беспилотные автомобили лишь начинают набирать свою популярность. Согласно статистике, предоставленной сайтом «Коммерсантъ» (рис. 3), в России каждый третий из опрошенных (30%) в восторге от идеи применения беспилотных автомобилей в нашей стране, 13%, в свою очередь, настроены против идеи внедрения подобного вида транспорта.



Рис. 3. Результаты опроса

Финансовая индустрия хранит колоссальный объем информации, охватывающий такие аспекты, как котировки акций, экономические индикаторы, отчетность компаний, новостные потоки и прочее. Применение техник машинного обучения способствует более глубокому и эффективному изучению и интерпретации данных массивов. Особенности и быстро меняющаяся природа финансовых рынков делает интеграцию машинного обучения особенно актуальной. Колебания стоимости акций и других финансовых инструментов требуют реализации продвинутых алгоритмов машинного обучения для верного предсказания их поведения [4]. Машинное обучение способно повысить точность и ускорить процесс анализа данных для создания точных прогностических моделей. Передовые достижения в области компьютерных технологий, рост вычислительных возможностей и доступность целевых аппаратно-программных комплексов обеспечивают возможность использования многогранных алгоритмов машинного обучения в оперативном режиме. Алгоритмическая торговля, как пример использования машинного обучения, представляет собой применение математических моделей для формирования более выгодных инвестиционных стратегий. Обычный трейдер должен выстроить математическую модель, изучить деловые новости, оценить рынок и торговую активность в данный момент времени чтобы выявить все факторы, которые могут заставить ценные бумаги вырасти или упасть в цене. В отличие от людей, алгоритмическая торговля

способна ежедневно обрабатывать огромное количество данных и совершать тысячи сделок. По данным McKinsey, до 2025 года прогнозируется, что алгоритмы ИИ будут применяться в финансовой сфере совокупно на сумму \$1,2–1,5 триллиона в год [5].

Промышленный сектор порождает обширный пласт данных, включая информацию о технологических процессах, сенсорные данные, контроль за качеством изделий, управление логистическими потоками и многое другое [6]. Прогресс в области технологий обусловил возможности сохранения и анализа подобных данных, что заложило фундамент для использования техник машинного обучения. Инновационные подходы в машинном обучении, включая нейросети и методы глубокого обучения, наряду с увеличением вычислительных способностей компьютеров, открыли двери для внедрения сложных моделей и анализа масштабных наборов данных. Задействование машинного обучения способствует автоматизации изготовительных процедур и налаживанию рабочих операций, что может повлечь за собой сокращение издержек, улучшение качества товаров и увеличение общей эффективности производственных предприятий, однако это также может иметь последствия в виде уменьшения числа рабочих мест на фабриках. Кроме того, минимизация времени простоев является одним из ключевых мотивов интеграции машинного обучения в промышленность. Простои могут происходить из-за сбоев, поломок или несвоевременной поставки сырья. Таковы ошибки могут обойтись бизнесам в сумму, превышающую десятки миллионов рублей. В качестве примера, GE Oil & Gas привлекает методы машинного обучения. Изобретенная компанией платформа регистрирует информацию с сенсоров, мониторящих процессы добычи углеводородов, последующим этапом является создание расписания диагностических проверок, что способствует предотвращению серьезных технических сбоев еще до их возникновения [7]. Система также оказалась полезной для повышения объема добычи газа на 2–5% у Кувейтской Национальной нефтяной корпорации и позволила нефтяной компании «Petronas» в Малайзии сократить затраты на обслуживание на 10%.

В данной статье был проведён анализ использования машинного обучения в различных сферах. На основе данной информации можно сделать вывод, что применение машинного обучения становится всё более широким и значимым. Ожидается, что данная тенденция будет продолжаться и в будущем, поскольку компании становятся всё более заинтересованными в использовании технологических инноваций для повышения эффективности и прогнозирования финансовых затрат. Развитие технологий играет основополагающую роль во внедрении машинного обучения в процессы нашей жизни.

Список используемых источников

1. Аль-Нами Б. А., Дубоусова Е. В. Актуальные проблемы обеспечения безопасности информационных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 124–128.

2. Аль-Нами Б. А., Кочнев Т. В. Особенности систем управления и информационных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 159–163.

3. Голик А. В. Цифровая экономика в современном мире // Молодой ученый. 2019. № 45 (283). С. 280–281.

4. Шваб Клаус Четвертая промышленная революция. М.: Эксмо, 2022. 208 с.

5. Столбова М. И., Бренделева Е. А. Цифровая экономика // Научная библиотека. 2020. 387 с.

6. Аль-Нами Б. А., Борисов С. К. Анализ оптимизаторов глубокого обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С.72–76.

7. Аль-Нами Б. А., Бурков А. Д., Слепцов А. К. Современные информационные технологии и безопасность информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании: XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 79–84.

Статья представлена научным руководителем, кандидатом технических наук, ассистентом кафедры ИКД Аль-Нами Б. А.

UDC 004.75
SCSTI 50.41.25**RABBITMQ: THE PRINCIPLE OF OPERATION
AND THE APPLICATION IN MULTI-MODULE SOFTWARE****A. An'shakov, T. Galieva**

Bonch-Bruевич Saint-Petersburg State University of Telecommunications

The article discusses the basic principle of RabbitMQ message broker. The examples of practical application of RabbitMQ as a means of communication of various software and services are presented. The algorithm of using application level protocols to transfer messages between system components is described. The article is devoted to software developers and application architects.

RabbitMQ, AMQP, frame types, communication, workflow automation

In today's microservice applications, RabbitMQ message broker is a software tool for interoperability, communication between various software or services using the AMQP (Advanced Message Queuing Protocol) protocol.

The usage of the message broker such as RabbitMQ is a great solution for SOA (Service-Oriented Architecture). And nowadays it is the most widely used open source message broker (for example, T-Mobile, Runtastic, Mozilla, VMware, AT&T and others) [1].

The application can be easily deployed either locally or in a cloud solution. There is the support for multiple messaging protocols and for data streaming. RabbitMQ can be developed in distributed or federated configurations to meet scalability and high availability. It is also supported in multiple operating systems and provides a wide range of developer tools for different programming environments.

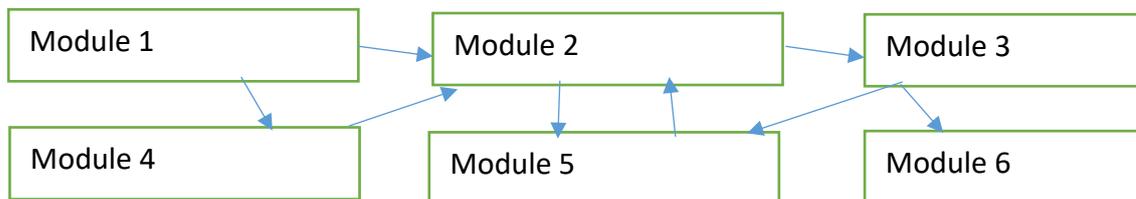
For understanding what RabbitMQ is and how RabbitMQ works, it needs to discuss the basic principle of operation.

First of all, RabbitMQ performs one main function – communication of applications and services, it works with message queue (broker) in applications, services, etc [2, p. 18].

For example, there is one system, which works using a set of modules. Each module is independent; it has a clear distributed role in each of the modules. The algorithm is conditioned by the fact that at the end of the primary module, one or another module must start. To automate workflows, they (modules) must communicate, exchange messages at the application level to understand who (developers) and when to finish their work. And in this case, RabbitMQ helps.

Another good example can be given in the form of the work of the post office. RabbitMQ would be a post office, correspondence and delivery courier at the same time. Only instead of paper letters, there would be binary values.

The example of software operation is shown below (pic. 1).



Pic. 1. The example of software operation.

The information from modules is transferred and processed according to certain algorithms, business model, task, etc.

This solution has its advantages, but there are also disadvantages. One of the brightest examples is that when changing a task, business model or algorithm in any of the modules, the changes can completely paralyze the work of the whole software or service, that's why there is no flexible scalability.

Besides, microservice architectures are also well known, communication between modules or services is organized by means of HTTP request inside.

If one of the modules or services will be rebooted, will not be able to respond to the request, for example during a Dos attack, the whole service or any part of it will be inoperable. This is one obvious example where a message broker needs to be implemented.

There is another example when different modules or services can be run on different programming environments. That's why for implementing services you can use best practices, involving different development teams with different programming environments, using the cross-functionality of RabbitMQ.

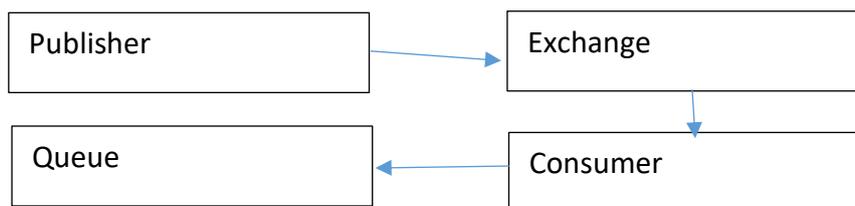
In the case of the presence of a message broker in the system, indicators of system maturity reveal. After that, the functionality of systems increases, the need for tasks grows but the usual algorithms sometimes become insufficient.

As mentioned earlier, the work of RabbitMQ is similar to the post office.

In this case, the post office would be act as a PO Box where messages from other modules of the system arrive. In turn, the other modules would know where to go for the messages (task) they are waiting for.

The basic principle of operation of RabbitMQ is based on the AMQP (Advanced Message Queueing Protocol) protocol. It is an open source application layer protocol for message passing between system components. The mission idea is to exchange messages between individual subsystems (or independent applications) through an AMQP broker which performs routing, possibly guarantees delivery, distributes data streams, and subscribes to the right types of messages.

The AMQP broker operation on which RabbitMQ is based is shown below (pic. 2) [3].



Pic 2. The AMQP broker operation.

RabbitMQ has an extension to the AMQP protocol – exchange to exchange binding, through which two exchangers can be linked to each other in order to set up more sophisticated message routing [4, p. 73].

Besides, the AMQP-broker has proved itself very well when using this protocol in RPC (Remote Procedure Call). For example, Module 1 is a kind of web interface for data input, and Modules 2 and 3 are the main and auxiliary algorithm, executed in C# and Java respectively, which start working together by means of RPC. But RPC itself works by means of RabbitMQ.

It proves the practical example below.

At the beginning of communication people begin with a greeting, in the case of AMQP, the protocol header is such greeting. With the server receiving such a request from the client (Module 2, from Module 1), inside RabbitMQ it starts the greeting with the `Connection.Start` command, and the client responds with an RPC message `Connection.StartOk`. This command would collectively represent a “frame”. The `Connection.Start` command consists of two parts AMQP class and method. The AMQP Connection class and method `Start` is the `Connection.Start` RPC request.

An AMQP frame consists of three parts, which are called the frame header when they are combined. The very first field is the only byte indicating the type of this frame, and the second field specifies the channel number for which the frame is intended. The third field carries the size in bytes of the payload of this frame. This frame header and the final byte marker create a “frame”.

An AMQP frame can be categorized into five frame types: protocol header frame, method frame, content header frame, body frame, and heartbeat frame.

Each frame type has some distinctive purpose, but some frames are used much more frequently than others. For example, the protocol header frame is used only once, when connecting to RabbitMQ; the method frame carries a specific RPC request or response that is sent or received from RabbitMQ; the content header frame contains the size and properties of some message; the body frames actually make up the messages; the heartbeat frame is sent to and from RabbitMQ as a check to ensure that both sides of the connection are available and working properly.

It is worth noting that besides the AMQP protocol, RabbitMQ can work with protocols MQTT and STOMP [2, p. 177].

The MQTT (MQ Telemetry Transport) protocol is a lightweight messaging protocol that is used for mobile applications, and supports RabbitMQ via a plug-in. Developed as a subscription-based publishing protocol, MQTT was originally invented in 1999 by Andy Stanford-Clark of IBM and Arien Nipper of Eurotech. MQTT was designed for messaging on resource-constrained devices and in low-bandwidth environments, without conceding reliability limitations to messaging. Although it does not have the same functional characteristics as AMQP, the explosive growth of mobile applications has led to the growing popularity of MQTT in recent years.

Originally named TMPP, the STOMP (Streaming Text Oriented Message Protocol) protocol was first described in 2005 by Brian McCallister. Modeled after HTTP, STOMP adopts an easy-to-read text-based protocol. Originally implemented in Apache ActiveMQ and designed with simplicity in mind, STOMP is now supported in multiple broker implementations and has client libraries for most programming languages. The STOMP 1.2 specification was released in 2012 and is supported by RabbitMQ in conjunction with its previous two versions. Support for STOMP is provided by some kind of plug-in that is distributed as part of the central RabbitMQ package.

It is worth discussing the example of practical application of RabbitMQ as a means of communication of various software and services.

If you have some data publishing service, the general architectural principle is to maintain a client application that generates an order as a file with input data.

On one of the servers (Server 1) the script was programmed on the executive files, which in turn would run through the task scheduler on the server on a schedule, every day at 9.00 p.m. In the initial data processing, input data from the user are involved, which were set earlier to the time in the schedule. After processing the data would be sent back to the next server (Server 2). On this server the mechanism of further processing was implemented in the same way as on Server 1, by schedule. Everything works until the moment when the system needs to be scaled up or the processing of the input data stream takes longer than the scheduled processing of Server 2. It turns out that the data has not yet been processed on Server 1, but Server 2 should have already been working.

To make the example above work more stable it is necessary to implement the AMQP protocol. It is no longer necessary to guess any time for the start of the processing task, it is enough to teach the servers to communicate with each other through the flow, and the indispensable assistant should be RabbitMQ.

The client creates the task and the client application sends a message to the broker that the task has arrived. Broker in turn sends a message to Server 1 that the task has started, at the current moment of time, the process has started. When Server 1 finishes processing the data, it also sends a message to the broker that it has finished and informs Server 2 through the broker that it should start the next data processing. At the finish line Server 2 sends a message to the broker that

everything is ready, the broker sends this information to the client, the cycle is over.

The shown above examples of practical application of RabbitMQ and the AMQP protocol demonstrates that this technology can significantly increase the flexibility and fault tolerance of information systems in various areas. With the use of RabbitMQ, the prospects of the developed software can significantly increase.

Because of key features of RabbitMQ such as the open source code, the ability to integrate across different programming environments, minor server requirements, security (secured client connections by authentication with a client certificate), the practical application for programming languages (Java, Ruby, Python, PHP, JavaScript and C#), it is possible to integrate RabbitMQ with various modules created in a various development environment.

References

1. RabbitMQ is the most widely deployed open source message broker. // The official website of RabbitMQ. 2024. URL: <https://www.rabbitmq.com> (accessed: 26.01.2024)
2. Gavin M. RabbitMQ in Depth // Manning Publications. 2018. P. 264. ISBN 978-1617291005.
3. AMQP // The official website of Wikipedia. 2024. URL: <https://ru.wikipedia.org/wiki/AMQP> (accessed: 26.01.2024)
4. Rindin A. *Sovremennye standarty informazionnogo vzaimodeistviya sistem: ucheb. posobie.* Voronezh: Voronezhskij gosudarstvennij tekhnicheskij universitet, 2021. 144 p. ISBN 978-5-7731-0943-3.

Статья представлена доцентом кафедры ИНиРЯ СПбГУТ, кандидатом филологических наук, доцентом Е. А. Гориковой.

ANNOTATIONS

INFORMATION SYSTEMS AND TECHNOLOGIES

Absattarov G., Abylhasenov M., Burlakov A., Shakirbekov D. Centralized Data Classifier as a Tool for Providing Regulatory and Reference Information for Applied Information Systems. – PP. 5–9.

The article discusses the issues of constructing and maintaining a centralized data classifier as a tool for centralized provision of regulatory and reference information for applied information systems. The use of technology on an existing automated control system will reduce the cost of technical operation through the use of potential, centralized maintenance of regulatory and reference information of information systems.

Key words: centralized classifier, information systems, operational data.

Averyanov A., Dolgov E. Development of a Software Package for Automated Analysis of the Security of Information Telecommunication Networks. – PP. 10–15.

In today's world, information protection is becoming more and more relevant. With the development of digital technologies, the number of threats related to the violation of confidentiality, integrity and availability of data is increasing. Particular attention is paid to the protection of information systems of public institutions, as they are objects of increased interest for attackers who can cause serious damage to national security. The article discusses the relevance of creating a software package for comprehensive analysis of network infrastructure security, identifying possible vulnerabilities and developing recommendations for their elimination, thus increasing the overall level of IS.

Key words: penetration testing, security analysis, information security.

Avramenko V., Chichkov E. Software Package for Experimental Evaluation of Neural Networks Efficiency. – PP. 16–19.

The method of experimental estimation of efficiency of variants of realisation of various architectures of neural networks on the basis of the software complex providing identical initial data and conditions for testing of the estimated neural networks is offered. The structure and description of the software complex operation, neural networks efficiency indicators are presented.

Key words: neural network, software system, indicator, evaluation, efficiency, accuracy, resource intensity, efficiency.

Agafonov N., Vozgrin G., Volynkin P. Development of Software for Collecting Information About Objects on a Limited Area by a Mobile Robot ROBO-PICA. – PP. 20–24.

The software for the ROBO-PICA robotic platform is presented, which allows a mobile robot to scan a site of limited dimensions for the detection of 5x5 cm objects on it. The robot moves along a given contrasting trajectory line. When an object is detected using a distance sensor, the robot signals this with an audible signal, drives around an obstacle and stores the location of the detected object in memory. After the surface scanning is completed, the robot re-runs the distance, but in the absence of objects. In the places of the former location of objects, the robot makes it clear by an audible signal that an object was previously in this place.

Key words: mobile robots, area scanning algorithms, solving hardware problems.

Agenosov D., Baisarin B., Pogodin N., Svechnikov D. Security Risk Ranking Penetration Test Management Software. – PP. 25–27.

This article discusses proposals for building a penetration test software tool based on ranking security threats. The software tool allows you to obtain data for scanning, collect information from tested hosts, find vulnerabilities and generate exploits, and generate reports. The developed proposals ensure the receipt of objective data based on the results of security studies of the facility.

Key words: security threats, vulnerability scanning, penetration testing software.

Al-Nami B., Babayeva E. Research and Comparison of Photodetectors. – PP. 28–31.

In 2024, photographers are still hotly debating the advantages of Lightroom over Photoshop. Each platform provides powerful editing features and tools, but it is important to understand their differences in order to make an informed decision. In this article, we will compare Adobe Photoshop and Lightroom, talk about the differences and similarities of the software.

Key words: quality, reliability, control of processes and products, radiophotonics, photodetector, radiophoton transmission line, Adobe Photoshop, Adobe lightroom.

Al-Nami B., Beliaeva N. UI-design of a Flower Delivery Mobile App. – PP. 32–36.

This article aims to study the use of flower delivery mobile applications, analyze the visual and functional representation of the design for such an application, as well as to assess its analogues.

Key words: UI-design, graphical user interface, mobile application, development tools, interface, design, mobile applications, implementation, design.

Al-Nami B., Bokov I. The Role of Neural Networks in the Development of Machine Translation. – PP. 37–40.

The main goal of the following article is an introduction to the principles of operation of neural networks during machine translation of text. In addition, the article provides the world history of machine translation, its current problems and development prospects, as well as general information regarding the principles of operation of neural networks.

Key words: neural networks, automation, machine translation, natural language, artificial intelligence, machine translation technologies.

Al-Nami B., Pigareva J. User Interface Development Website of the Logistics Company. – PP. 41–44.

This scientific article is devoted to the development of the user interface of the logistics company's website to solve the existing problem of the disparate storage of branded products and documents. The article discusses the process of creating a specialized section on a web platform designed for convenient employee access to current versions of document templates, presentations, logos and other branded materials.

Key words: website, interface, carousel, identity, design, user, flat design, user interface, visual interface design, user experience, interface design, site interfaces.

Al-Nami B., Selina V. Encryption and Decryption of Information. – PP. 45–49.

This article discusses the problem of information leakage and falsification. The purpose of the work is to study cryptography and identify a method for protecting transmitted information. During the work, the need to protect information was identified. As a result, the “encoder” program was written, with the help of which information is encrypted and then decrypted in order to prevent the possibility of reading and forging it.

Key words: encryption, decryption, information protection, information environment, symmetric encryption, program, cryptography, cryptographic keys, shared private key, authentication.

Al-Nami B., Simkin K. Exploring the Difference in Using Functional and Object-Oriented Programming in Python Language. – PP. 50–52.

At the beginning of the article, we will understand the definitions of these. In the modern IT industry, there are a huge number of different programming languages, they mainly use two types of programming: object-oriented and functional. This article will examine the use of these types of programming in the Python language, as one of the simplest and most popular in the industry.

Key words: Python, programming language, web development, Python libraries, language syntax, object-oriented programming.

Al-Nami B., Tuzhikova M. Fundamentals of Modern Containerization. – PP. 53–57.

With the development of information technology and software development, the growth in the number of programs and their volume, a need arose for some tool that would allow programs to be quickly and easily deployed on various devices and operating systems. We need an assistant who would simplify the process of creating an environment in which all the application's dependencies will be taken into account, and in which it can run without problems, which, of course, will make life much easier for programmers.

Key words: containerization, development, data, applications, management, resource, monitoring, indicators.

Al-Nami B., Tsyganova D. Choice of Program for Graduates of the Bachelor Program in the Profession of Design Engineering. Guide to Using Georecounter. – PP. 58–63.

Many graduates of a bachelor's degree program are faced with the challenge of learning new programs that can make their jobs in engineering and design easier. This article will help them become familiar with the program for future design engineers and demonstrate its functionality, and we will also look at an example of its work on one of the most popular computer-aided design and drawing systems - Automated Computer Aided Drafting and Design - design using computer technology.

Key words: design, Automated Computer Aided Drafting and Design, AutoCAD, engineer, drafting.

Apostolevskiy D., Klimov A. Confidentiality of Personal Information on the Internet. – PP. 64–67.

The Internet has become an integral part of our lives. It gives us access to information, helps us in study and work, and allows us to communicate with friends and family. However, in addition to its many benefits, the digital landscape poses inherent risks to personal safety and security. This article will discuss the types of Internet dangers and methods to combat them.

Key words: information security, personal data protection, legal regulation, safe Internet, cyberbullying, grooming, social networks.

Artamonov N., Vasiliev N., Vitkevich N., Kustov A. Overview of Smart Home Sensor Analyses. – PP. 68–72.

This article describes the architecture model of the Internet of Things, as well as a comprehensive comparison of various smart home systems, such as Google, Yandex, Xiaomi and Apple technologies, with an emphasis on their functionality, usability, integration with other devices, as well as aspects of data security and privacy. Through an analysis of the main characteristics and features of each system, the article allows readers to gain a complete understanding of the capabilities and limitations of various smart home systems, helping them make informed choices when planning or upgrading their home automation.

Key words: machine learning, smart home, automation technologies, information processing, device integration, functionality of smart home systems.

Artamonov N., Lipatnikov V., Melekhov K. Method for Network Control of Information and Telecommunication Network Security. – PP. 73–78.

This article examines the issue of developing a structure for network control tools and choosing neural network technology for building network security control tools. Various types of neural networks are considered and the most suitable neural network for network control is selected. The research results presented in the article may be useful for specialists in the field of information security and network technologies.

Key words: network control tools (NSC), information and telecommunication network (ITCN), neural networks.

Akhramenko A., Kuznetsova O. Software Application for Visualization of Plein Air Venues. – PP. 79–83.

Plein-air painting events demonstrate the growing interest among the population in Russia. Wide access to education and the development of creative communities create a favorable environment for the development of interest in the open air. Visualization of possible places for holding plein airs on the map provides the widest opportunities for everyone to capture places in the open air.

Key words: geoinformation software, software application, visualization, plein air, plein air venues.

Balakirev D. Generation of Facial Expression Animation for a Three-Dimensional Model Using Vocal Data. – PP. 84–87.

This work is devoted to the generation of facial expression animation for a three-dimensional model based on vocal data. The idea of facial expression animation is not new, but it requires hardware to track facial features. This work is devoted to the generation of facial expressions

using a software method involving artificial neural networks, which makes it cheaper and easier to create it. This can be used in the movie industry, the video game industry, as well as during virtual conferences and streaming using virtual avatars.

Key words: animation, 3D, modeling, three-dimensional model, neural network, generation, synthesis, facial expressions, avatar, video game industry, movie industry, simulation.

Balyberdin S., Bondarenko I., Zharanova A. Formation of a Telegram Bot Model for Searching for Musicians and Creating Collaborations. – PP. 88–93.

An innovative approach to organizing musical collaborations using a Telegram bot is considered. An analysis of existing services for searching for musicians has been carried out, and their shortcomings have been identified. The basic algorithms for data search and filtering are presented. The algorithm and method of calculating the similarity metric for issuing recommendations to the user are described. A model of an information system for searching for musicians and creating collaborations is proposed. The range of technological solutions for future development is given.

Key words: recommendation algorithms, similarity metric, recommendation system, Telegram bot.

Beckel L., Nikolaev A. Organization of Computer and Computer Network Security in a Secondary Educational Institution. – PP. 94–98.

Due to the rise in cybercrimes, schools need to ensure the security of computers and computer networks. First, we divide the school network into two networks, a network for teachers and a network for students. It is also necessary that anti-virus software be installed on computers. Some computers should have restricted access.

Key words: computer, computer network, security, secondary educational institution, attack.

Belous K., Gorbach A., Matyukhina V. Automated Telecommunication Equipment Control System – PP. 99–103.

Software products for monitoring network telecommunications equipment are designed for operational monitoring of processes occurring in networks, which allows you to quickly identify and eliminate failures, as well as monitor and neutralize emergency situations with minimal costs. Existing software products do not always make it possible to satisfy the needs of a specific user, and therefore the task of creating an automated system of this class is an urgent task.

Key words: computer network, equipment, database, control.

Belous K., Demidov A. Software for Visualizing Omron PLC Control Commands – PP. 104–107.

An overview of modern Omron PLC programming tools is presented. It is shown that existing software does not allow us to fully analyze the process of transmitting control commands to actuators, since they require their physical presence, which is not always possible. The Omron PLC and its role in automatic control are considered. A prototype of software written in the high-level language C# is presented, which allows one to analyze the structure of control commands, as well as their impact on virtual automation objects.

Key words: SCADA, PLC, visualization, software.

Besedin M., Zadboev V., Polishchuk V. Analysis of the Operating Principles of DNS Servers and DDoS Attacks. – PP. 108–112.

The article focuses on the relationship between DNS, which is a critical infrastructure of the Internet, providing transformations necessary for routing network traffic, as well as DDoS attacks, which pose a serious threat to the stability of network infrastructure through distributed denial of service methods.

Key words: DNS, DDoS, principles of operation, methods of attack, methods of influence.

Besedin M., Zadboev V., Sadovnikov V. Analysis of the Capabilities of the High-Level Python Programming Language for Automating Network Configuration and Monitoring Data Transmission. – PP. 113–116.

Problem statement: currently, there is an increasing need to automate various processes occurring in data transmission networks, including in situations where it is necessary to automate the configuration of a large number of network devices. The purpose of this article is to consider the question of the optimal choice of a tool for automating the processes of interaction between network devices. Results: the paper describes the main tools, highlights their disadvantages and advantages, and provides examples of the use of these tools in specific situations.

Key words: programming, networks, information security, automation.

Bikbulatov V., Meshkov A., Tkachev D. User identification using RFID tags. – PP. 117–121.

Unique identification technology using radio waves and the use of an RFID tag, which contains a microchip with a special identifier recorded and an antenna for receiving and transmitting a signal to special readers. An RFID tag is placed on a specific item to identify in real time of a person, animal or any product. Thus, let's look at the concept of RFID tag technology, operating principle, application advantages and disadvantages.

Key words: radio frequency identification, RFID tags, ISO standards.

Birikh E., Bulova M., Kazantsev A., Minyaev A. Development of a Software Module for Automating the Determination of the Level of Security Information Systems of Personal Data. – PP. 122–127.

This article presents the development of a software module written in Python, which allows you to automate the process of generating information security requirements in personal data information systems in accordance with the requirements of the Federal Service for Technical and Export Control of Russia.

Key words: information protection; data security; information security; security level, automated system, security threat, personal data information system, informatization object.

Bovshik P., Litvinov V. Automation of the Decision-Making Process in the Tasks of Configuring Software and Hardware Complexes for Storing and Processing Information. – PP. 128–132.

In the modern world, where almost every enterprise is struggling to reduce the downtime of work activities and the corresponding economic costs due to the human factor, the issue of automation of a particular process arises. To solve this issue, decision support systems are already being used. The paper discusses the concept of decision making in order to automate the work process of system administrators. As a result of scientific research, the basic concept of decision-making in problems of configuring software and hardware systems for storing and processing information is presented.

Key words: decision support system, configuration of software and hardware systems, information storage, information processing.

Boyko A., Kuzin P., Kuzina E., Potapov I., Usov N. Application of the Mathematical Model of the Light Path For Spectral Resource Management in Optical Transport Networks. . – PP. 133–137.

The paper provides a rigorous definition of light path. The concept of a light path is extended and clarified by combining the route of passage and the assigned spectrum of an optical signal. The set of acceptable light paths is proposed to be formed on the basis of the ratio of optical signal power to noise power in the light path bandwidth for a particular type of signal. A number of optimality criteria for solving the problems of search and distribution of light paths is presented. A mathematical model of the light path is developed, which allows to increase the efficiency of spectral resource management in optical transport networks. On the basis of the proposed model it is possible to solve the subproblems of search for light path routes taking into account the requirements for non-intersectivity of spectra, contiguity of elementary frequency intervals of each light path, continuity of the spectrum along the entire route.

Key words: optical transport network, lightpaths, transmission quality, spectrum allocation.

Bolshebratskiy K., Dobrythin M. Analysis of the Procedure of the Interaction of Software Funds Established at the Mail Serverage of the Electronic Account System. – PP. 138–143.

The article provides an analysis of the interaction of software installed on the mail servers of the e-mail system. The study is aimed at identifying and analyzing the sequence of actions and interaction of software components operating on mail servers. The results can be used to increase the efficiency of mail systems by ensuring their security by analyzing the possibility of interaction between programs and their vulnerabilities.

Key words: Email, interprocess interaction, server.

Borganova L., Sabinin O. The Research of Migration Methods of Programs in PL/SQL from Oracle DBMS to PL/pgSQL in PostgreSQL DBMS. – PP. 144–148.

In this article, the relevance of the transition to open database management systems is justified and the issue of migration between Oracle and PostgreSQL is considered. An overview of modern solutions for converting the code of software components written in the PL/SQL procedural language used in Oracle to PL/pgSQL used in PostgreSQL is conducted, and the tasks of the preparatory stage of migration are analyzed. As a result, the algorithm of program migration between the two systems is described and the processes of converting functions, procedures, triggers and packages are considered.

Key words: database management system, relational database, Oracle, PostgreSQL, migration of software components, migration of PL/SQL, PL/pgSQL.

Boyashova E., Melnikov M., Sheremet D. Using Visual Aids as a Tool to Ensure Understanding of the Data Presented Using Infographics. – PP. 149–152.

The work touches upon aspects related to distortions in the perception of information, as well as the objectivity of visualization. The factors influencing the effectiveness of the perception of the presented information, as well as the extraction of only those data that are useful from the information flow, are considered. At the same time, the data should be transformed into consistent conclusions that contribute to productive communication. In addition, the paper pays

attention to the mistakes made in the design of infographics, as well as offers recommendations for its creation.

Key words: infographics, visual aids, information perception, communication, information, data, data representation.

Bykov D., Klimov A., Romashkin K. Analysis of Cryptographic Data Encryption Algorithms. – PP. 153–156.

The article analyzes asymmetric data encryption algorithms (Rivest-Shamir-Adleman, Digital Signature Algorithm, ElGamal algorithm and Elliptic Curve Digital Signature Algorithm). The assessment was carried out taking into account the level of security, speed of encryption and decryption, as well as ease of implementation. In addition, the key sizes of each algorithm and their corresponding analysis are discussed. The most preferred were Elliptic Curve Digital Signature Algorithm and Rivest-Shamir-Adleman.

Key words: cryptography, encryption, asymmetric methods, decryption, algorithms.

Vaganov A. Marchakov A. The Device for Protection the Electronic Equipment of the Automated Control System Based on Modern Programmable Chips. – PP. 157–162.

The article considers the device for protection the electronic equipment of ACS from the negative effects of instability of supply voltage, various pulse interference, as well as incorrect modes of its activation and operation. The relevance of the development of such a class of devices is substantiated, and the main advantages and disadvantages of similar systems and methods of automated control system protection based on modern programmable chips are considered. A block diagram of the protection system is presented and the choice of a modern element base for its implementation based on programmable discrete integrated circuits is justified. The choice of a mathematical apparatus for calculating individual blocks of the system has been made. The results of the simulation are presented.

Key words: protective device, pulse interference, microcontroller, power supply, AFR, block diagram.

Verkhova G., Kozlova E. Architecture of Software and Algorithmic Support for Processing and Visualization of Information Presented in GeoJSON Format. – PP. 163–166.

The results of developing a software architecture for performing overlay operations on objects presented in the GeoJSON format and visualizing the results are presented. As a result of the research, many basic overlay operations have been identified and algorithms that implement these operations have been identified. The application has a service-oriented architecture. The business logic is implemented as a microservice, and the visualization system is implemented as a microfrontend. A distinctive feature of the proposed architecture is the ability to deeply integrate the software into any geoinformation applications with a microservice architecture.

Key words: overlay operations, vector and raster models, microservice architecture, methods for performing overlay operations, GeoJSON.

Verkhova G., Letuchy V. Current State and Prospects for the Development of Digital Twins of Spatially Distributed Cyber-Physical Production Systems. – PP. 167–169.

The results of research in the field of formation of spatially distributed cyber-physical production systems based on digital twins are presented. The key differences between digital twins of spatially distributed objects and traditional digital twins of production equipment, which do

not take into account geoinformation aspects, are analyzed. Possible scenarios for the development of digital twins of spatially distributed cyber-physical production systems and their role in the formation of a unified geoinformation cyber environment are considered.

Key words: digital double, structure, analysis, logical and mathematical description, cyber-physical system, system.

Verkhova G., Permiakov A. Methods for Forming Allowable Zones for Location of Technical Objects on a Digital Terrain Model. – PP. 170–173.

The task of optimizing the placement of technical objects on the terrain using a search algorithm requires a formalized definition of permissible placement zones. These zones are determined by the type and parameters of the terrain, the presence of necessary infrastructure, and engineering communications. Modern geoinformation systems allow solving placement problems interactively, but utilizing search algorithms for these purposes in such systems is challenging because most of them lack advanced tools to automate this process. The article presents the results of research on methods for forming permissible placement zones of technical objects on digital terrain models and their implementation in modern geoinformation systems, as well as proposes an approach to forming such zones.

Key words: placement zones, GIS, technical object, digital terrain model, optimization of spatial object placement.

Verkhova G., Popov I. Software and Algorithmic Support for Managing Spatial Relationships Between Geographic Objects Based on Temporal Graphs. – PP. 174–178.

When solving a wide class of problems using geographic information technologies, it is necessary to take into account topological relationships between spatially distributed objects, however, in modern geographic information systems, support for topological modeling is implemented at a level that is insufficient for the current state of development of information technologies. The article presents the results of the development of software and algorithmic support for managing spatial relationships between geographic objects based on temporal graphs. The software under consideration implements basic operations on temporal graphs. This type of software can be used in advanced geographic information systems based on a knowledge base.

Key words: temporal graphs, geographic information systems, topological relationships.

Verkhova G., Suetin A. Method of Information Interaction in Interoperable Cyber Environments. – PP. 179–183.

A method for implementing information interaction within a single cyber environment formed from local interoperable cyber environments is proposed. The proposed method is distinguished by the organization of information interaction using three types of agents. Models for the formation of agents for the implementation of information interaction between local cyber environments are presented. Examples of possible implementation of the agent approach at the level of database synchronization are considered.

Key words: cyber environment, virtual organization, virtual enterprise, interoperable cyber environment.

Vladimirova E., Kryukova E. The Use of Modern Information Technologies in the Process of Training Engineering Specialists in Telecommunications Universities. – PP. 184–189.

The article talks about the rapid development, active implementation and use of modern information technologies in the process of training engineering specialists. This makes it possible to make electronic educational resources more accessible to a wide audience of users, and helps to increase the intensity and efficiency of the educational process.

Key words: electronic information educational environment of the university, electronic library, content, information technology, distance learning, availability of electronic educational resources, students, teaching staff.

Vnukov I., Filippov F. Deep Learning Tools for News Texts Classification in Intelligent Recommender Systems. – PP. 190–194.

The current state and prospects of development of intelligent recommender systems are described. Integration of deep learning models into intelligent recommender systems is actualized. Various architectures of deep learning models, including full-link feed-forward neural networks, one-dimensional convolutional neural networks, recurrent neural networks, as well as Transformer architecture, are studied in the context of their application to the classification of Russian-language news texts. A comparative analysis taking into account various hyperparameters aimed at optimizing the accuracy and performance of the models has been carried out.

Key words: artificial neural networks, deep learning, intelligent recommender systems, text classification.

Vovik A. Complex Mathematical Model of Information Security Management Process in IoT Systems. – PP. 195–201.

Solving the problem of information security management in IoT systems today is the most important condition for ensuring information security and maintaining the required level of information security in information systems. At the same time, the possibilities of information security management are limited by the absence of common numerical metrics of the main components of the process. To ensure the possibility of obtaining numerical estimation, the author developed a complex mathematical model of the process of information security management in IoT systems, combining methods of fuzzy modelling, structuring methods and methods of expert estimation.

Key words: Information security management, mathematical modelling, numerical assessment of information security, Internet of Things system.

Voloshinov D., Urvantsev G., Sharipova K. Expanding the Training Dataset Using Synthetic Data in Image Generation Models Finetuning. – PP. 202–206.

The paper researches potential of expanding the training dataset with synthetic data in image generation models finetuning. The methods of synthetic data generation are described and the efficiency of their use is studied. The analysis of experimental results is given, practical approaches to their integration are proposed, and prospects for further research in the image generation models finetuning are suggested.

Key words: modern technologies, neural networks, machine learning, image generation, Stable Diffusion, graphic content, finetuning algorithms, LoRA, ethnic diversity.

Volynkin P. Algorithmic and Software Solutions for Forecasting Areas of Flooding. – PP. 207–210.

In the era of activation of both natural and man-made crises, the task of forecasting areas of flooding is becoming particularly relevant. In this regard, the task of machine modeling of the flooding process is set, taking into account many factors. The article discusses algorithmic and software solutions for forecasting areas of flooding, taking into account the terrain features.

Key words: flooding, relief, modeling, forecasting.

Volynkin P., Gilmanova M., Analysis of Changes in Video Container Parameters after Embedding a Video Messages. – PP. 210–214.

In the era of active development of information technology, the transmission and viewing of data in video format is becoming one of the most common types of traffic. This makes them a convenient option to use as a container for stegocommunication. It is impossible to completely hide the presence of an embedded message, but it is possible to minimize its visibility. This is achieved by minimizing file size changes. The Masker 7.5 program was used to automate the implementation of the stegocommunication in the video container, and the results of the implementation for various file formats are also presented.

Key words: steganography, video, container, *.avi, *.mov, *.mpg.

Volynkin P., Kirsanova V. Comparative Analysis and Selection of Microcontrollers for the Implementation of Automatic Altitude Control Software for UAVs. – PP. 214–218.

The paper "Comparative analysis and selection of microcontrollers for the implementation of automatic altitude control software for UAVs" is a study of different types of microcontrollers, focusing on the selection of the optimal one for the development of automatic altitude control software for unmanned aerial vehicles (UAVs). The paper analyzes several types of microcontrollers including their specifications, performance and power consumption. The comparative analysis revealed the main advantages and disadvantages of each type of microcontroller in the context of automatic UAV flight altitude control. Based on the data obtained, a reasonable choice of the microcontroller that best meets the requirements for the development of automatic altitude control software is made.

Key words: microcontroller, comparison, programming, UAV.

Volynkin P., Tumanov I. Design of a System for Automated Loading of Tiles. – PP. 219–222.

The article is devoted to the design of a system of automated loading of tiles intended for updating electronic maps. The development is emphasized on the creation of a convenient mechanism for updating tiles, which is essential for ensuring the relevance and accuracy of geospatial data. The study also provides a comparative analysis of existing similar systems, identifying their strengths and weaknesses. The advantages of the developed system over other solutions are described, providing a rationale for selecting specific solutions.

Key words: automated loading of tiles, electronic maps, geographical data.

Volynkin P., Chinyaev V. The Algorithm for Predicting the Oil Spill Zone. – PP. 223–225.

This research aims to develop an algorithm for constructing oil contamination zones on the ground based on a theoretical approach. The algorithm takes into account various factors such as terrain topography, hydrological conditions, and oil spill characteristics to accurately predict the spreading of oil and identify areas at risk of contamination. The proposed algorithm

has the potential to improve response strategies for oil spills and enhance environmental monitoring and disaster management efforts.

Key words: Oil contamination, Algorithm, Theoretical approach.

Volynkin P., Shumilova A. Algorithm for Constructing Visibility Zones for Landscapes with Complex Terrain. – PP. 225–230.

The construction of visibility zones for landscapes with complex terrain is necessary for various geographic information systems, urban planning, environmental monitoring and other areas. The algorithms reviewed in this work take into account different types of source data. Each of the algorithms has its own advantages and disadvantages. Depending on these factors and the expected result, the necessary method for constructing visibility zones is selected. As a result of the work of some algorithms, the resulting visibility zones are presented.

Key words: visibility area, visibility area construction, floating horizon algorithm, Z-buffer algorithm, triangulation, double iteration.

Gaibaliev E., Filippov F. Development of a System for Searching Music by Rhythm. – PP. 231–234.

The relevance of the development and development of a system for searching music by rhythm is presented. The functional requirements for a search music system are highlighted. The range of technologies for system development has been determined. A method for automatically detecting and extracting rhythmic structure in a musical composition is described. An algorithm for its implementation and application is proposed. The choice of the type of neural network for implementing music search by rhythm is justified. The principle of training a neural network to solve the problem is considered.

Key words: information system development, music recognition by rhythm, music search.

Gvozdkov I., Likar A., Povedaiko M. Dark Cool is an Alternative Hacking Tool. – PP. 235–238.

The constant expansion of the list of software for the pentest greatly simplifies the life of attackers. There are no guarantees that the specified software will be used only for good purposes, as a result, there is a need for constant monitoring of this kind of software and familiarization with it.

Key words: protection; access to information; countering hacking of information systems.

Gorbachev P., Kopylov S., Tabunshchikova M. An Approach to Marking Electronic Documents Displayed on a Monitor Screen by Applying an Invisible Marker. – PP. 239–242.

High speed of information processing, convenient storage and management of data, the ability to model and analyze, multitasking of modern computers - all this determines the rapid development and spread of computer technology, automation of work with data. But in addition to all the advantages of using information technology, there is also a main disadvantage in the form of data leakage. To protect against this, various methods and means are being developed. This article presents an approach to screen marking the image displayed on the monitor screen in order to prevent data leakage caused by photographing the screen or taking a screenshot and then sending the generated image outside the controlled perimeter.

Key words: information leakage, marking of the image displayed on the monitor screen.

Gromov V. Forgotten and Unappreciated Programming Languages in Educational Process as Basis for Programming in Educational Process. – PP. 243–247.

The paper discusses the methodology of teaching students using virtual machine systems in the performance of academic tasks in the discipline "Architecture of Information Systems" at the St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruевич. The given methodology is based on the long-term experience of formation and operation of the Federal information system of the State Automobile Inspectorate from 1996 to 2013. It analyses the prospects of forming the skills of creating information systems for students in the conditions of modern development of computer technology.

Key words: Virtual machine systems, software systems, operating systems.

Gromov V. Student Presence Accounting Programme as Basis for Changing Behavioural Algorithms in Information Systems. – PP. 248–252.

The report examines the program for recording the presence of students in classes as a basis for changing the behavioral algorithms of teachers and students during lectures, practical and laboratory classes. The prospects for introducing a trial operation of a program for recording the presence of students for modern information systems in the conditions of import substitution and a shortage of information capacity are analyzed.

Key words: Virtual machine systems, software systems, operating systems.

Gruzdev A., Krakhmalev D., Pavlovich A. Development of the Architecture and Structure of Data Storage Using Fuzzy Dates of Historical Artifacts. – PP. 253–257.

In the world of architecture and history, there is an important task – the search and identification of artifacts, taking into account different levels of accuracy of the dates of their creation. The article provides an analysis of the choice of architecture for the implementation of a software component that allows solving the task. The concept of "pure architecture" and its components are considered. The variants of database management systems and storage structures are analyzed based on a clear and fuzzy dating format in the system. The influence of the selected solutions on the scalability and efficiency of the system is described.

Key words: fuzzy logic, clean architecture, database, membership function, system scalability, relational and non-relational storage.

Gubin A., Litvinov V., Mikhailova E., Filippov F. Assessment of Students' Training Level Based on Test Results, Taking Into Account their Psychophysiological State. – PP. 258–262.

The paper analyses aspects of assessing the level of students' training using testing, taking into account both the quality of test tasks and psychophysiological factors affecting students' abilities. Mathematical models are considered and a methodology of assessment formation is proposed, taking into account both the complexity of tasks and physiological parameters of students. The presented method allows for a more accurate assessment of students' level of training and can be used to optimise the prediction of student's grade during testing.

Key words: training level assessment, mathematical models of testing, Rasch model, Birnbaum model, psychophysiological factors.

Gubin A., Litvinov V., Filippov F. Simulation model of the Process of Atmospheric Air Pollution for Monitoring the Ecological Situation. – PP. 262–267.

A method is proposed for monitoring the environmental situation in the urban environment by using a simulation model of the process of air pollution, which takes into account a number of factors that have a negative impact on the environment. A mathematical formalization of the model of the process of atmospheric air pollution has been carried out. To create a simulation model, the AnyLogic modeling environment was used, which supports system dynamics methods. A number of experiments were carried out varying the parameters of the input data, which made it possible to make predictions about the factors that have the greatest impact on the environmental situation in the city.

Key words: simulation modeling, system dynamics, environmental monitoring, AnyLogic.

Gubin A., Litvinov V., Filippov F. Gradient Learning Methods of Parametrized Quantum Circuits. – PP. 268–273.

Training models based on quantum circuits using gradient methods are researched. The features of using analytical gradients to optimize the parameters of a variational scheme are considered. The influence of model sensitivity on the choice of metric when calculating gradients is shown. A comparison is made of a simple stochastic approximation of simultaneous perturbations with a natural gradient based on quantum Fisher information. The costs of implementing various approaches are estimated depending on the number of model parameters and the learning rate.

Key words: machine learning, gradients, parameterized quantum circuits, parameter optimization.

Dorofeev I., Lyubimov A. Modeling of a Flexible Production Module Based on a Colored Petri Net. – PP. 274–279.

The article discusses a flexible production module, including a storage device, an industrial robot and technological machine tools. The flexible production module is controlled from a local control system. The control system, in general, may include a numerical control system for technological equipment and an industrial robot control system. Modeling by the module is performed using a colored Petri net, which takes into account the flexibility of processing products with different technological characteristics within a single technological process. The developed model of a colored Petri net allows us to describe the structure of the control program of a flexible production module.

Key words: flexible production module, local control system, colored Petri net.

Evseev D., Lyubimov A., Chebykin N. Application of Web Technologies in Distributed Control and Management Systems of Technological Objects. – PP. 280–284.

The paper considers approaches and solutions for the development of distributed control and management systems for technological processes and objects based on SCADA systems and technologies of the industrial Internet of Things. The use of user applications using mobile telecommunications and web browsers based on web-oriented SCADA systems, as well as the full-duplex WebSocket protocol for managing technological processes and objects in real time are shown as promising areas for organizing remote access in control and management systems.

Key words: distributed control and management system, web technologies, WebSocket protocol, WebScada system.

Zharanova A., Kotlova M., Nerman K. Modeling a Task Planner for Parents and Children with a Reward System. – PP. 285–290.

The development of a task planner for parents and children with a reward system is updated. On the basis of the analysis of existing services the requirements to the developed information system are allocated. The model of the information system of the task scheduler for parents and children with reward system is formed, the key elements of the model are described. The main functional capabilities of the system are presented in the use case diagram. The life cycle of the task including the processes of execution, checking and scoring is described. An algorithm for recommending tasks based on the child's completed tasks is proposed.

Key words: digital platform, modeling, child motivation, financial education, parenting, time management, schedule organization.

Zharanova A., Slezak G. Development of an Algorithm for Automated Construction of Local Computer Networks Models for Procedural Virtual Spaces Generation System. – PP. 291–296.

The urgency of creation and application of the algorithm of automated construction of local area network models for systems of procedural generation of virtual spaces is substantiated. The requirements to the data structure of the algorithm for compatibility with the final information system are described. The structure of the algorithm and its data is formed and described. The linguistic and software were selected taking into account the purposes of using the designed algorithm. The realization of the algorithm using the selected software is performed. Possibilities of extension of the algorithm and its adaptation for different end information systems are presented.

Key words: local networks, procedural generation, simulation, game engine, algorithm, simulator.

Zhenihov E., Pekarskaya O. Intelligent Information Systems: Main Characteristics, Application and Prospects of Development in Knowledge Management. – PP. 297–303.

The article is devoted to the description of intelligent information systems, their characteristics, classification, application, and role in knowledge management. The methodology of data mining using intelligent information systems is presented. It was noted that today in our country it is especially important to create the necessary conditions for the development and implementation of artificial intelligence technologies, primarily in order to improve the quality of life of the population, strengthen national security, develop various sectors of the economy, health, culture, and education.

Key words: intelligent information systems, data mining, knowledge management, operational analytical data processing, logical and mathematical system.

Zadboev V., Lipatnikov V., Nefedov V. A Way to Improve the Integrity of Files of Information Resources of the Data Transmission Network under Attack Conditions. – PP. 304–307.

Modern computer technologies, which are constantly progressing in their development, make various tasks in the field of cybersecurity relevant. Developing the most effective way to protect files is currently becoming one of the important tasks of most developers.

Key words: executable files, information attachment, integrity assurance, data transmission network.

Zadboev V., Rogovoy N., Shevchenko A. Analysis of the Capabilities of Domestic Tools Used to Monitor Information Security of Data Transmission Networks. – PP. 308–313.

The article is devoted to the study of technologies and tools developed in Russia, designed to ensure information security in data networks. The work analyzes existing monitoring tools, identifying their main characteristics, advantages and disadvantages. Particular attention is paid to their applicability in the context of protection against modern threats and attacks such as cyberattacks and data leaks.

Key words: Information security, data networks, monitoring, SIEM systems, incidents.

Zolotov O., Matiukhina T., Olefirenko M., Sotenko S. Correction of Systems of Automatic Control and Modelling. – PP. 314–317.

In the theory of linear automatic control systems, the method of synthesis of correcting devices on logarithmic frequency responses became widespread, however when modeling more convenient is a work with transfer functions of a system. Transition to transfer functions allows to apply more flexibly different methods of optimization of structure of the projected system. Article is devoted to justification, development and combination of these approaches in a uniform technique.

Key words: systems of automatic control, frequency characteristics, transfer functions of system.

Zolotov O., Matyukhina T., Rakovskii O. On the Role of Artificial Intelligence in Decision-Making Systems, in Relation to the Management of Structures with Feedback. – PP. 318–321.

Classical automatic feedback control systems can be applied in many fields. At the same time, they can be combined with the use of artificial intelligence. However, the place of artificial intelligence in feedback systems has not yet been determined. We can consider this issue using the example of decision-making in the medical field, where there is a large amount of verbal information, and fuzzy decision boundaries lead to the use of fuzzy logic mechanisms.

Key words: Treatment methods, management theory, feedback principle, neural network, expert system.

Izmaylov N., Iskulov E., Kurdubova V. The Study of the Stability Of Solutions of Linear Systems Based on Operational Calculus. – PP. 322–325.

This paper examines such applications of the theory of functions of a complex variable as operational calculus and stability theory. Operational calculus is a powerful tool for analyzing and designing control systems, and stability theory allows you to assess the stability of dynamic systems and predict their behavior in various conditions. The use of operational calculus methods has made it possible to solve problems related to the study of the stability of solutions of linear differential equations. For some well-known analytical stability criteria, console applications have been written in the C language.

Key words: Operational calculus, stability theory, C++.

Ilyina I., Klimov A., Shelekhov V. Using Technology to Fight with Fake News. – PP. 326–329.

In the modern world, the spread of fake news has become a serious problem, undermining trust in the media, people and even states, distorting public discourse and even influencing elections and other important public and political activities. Recognizing the need to address this prob-

lem, technological innovations are increasingly being used to combat the spread of disinformation. This article examines various technological solutions and their potential to mitigate the impact of fake news in a digital society.

Key words: Fake, Mass information, blockchain, AI, artificial intelligence, data, news.

Ilna O., Kupchinenko O., Skoropad A. About Mandatory Access Control. – PP. 330–334.

The implementation of the mandatory access control model in new versions of special purpose operating system Astra Linux SE is considered. The use of special attributes of mandatory access control - labels are analyzed. For the main directories in operating systems of special purpose Astra Linux SE, examples of settings for mandatory attributes, levels and categories are presented.

Key words: operating system of a special purpose, information security, access rights, mandatory access control model, level, category, labels.

Ilna O., Kupchinenko O., Skoropad A. Network Protected File System. – PP. 335–339.

The composition of a network protected file system, its main tasks and basic capabilities, as well as the presentation and tasks of a protected file server and a client of a network protected file system, features of configuring a file server and access to a shared network resource are considered. The analysis of the capabilities of a secure file server is carried out and its advantages over other file servers are formulated.

Key words: network protected file system, shared network resources, file storage, network resource mounting, secure file server.

Ilna O., Kupchinenko O., Skoropad A. Web Applications in a Secured Operating System. – PP. 340–344.

An analysis of the differences of web in operating systems of special purpose Astra Linux SE was carried out. The composition and application of a secure complex of hypertext data processing programs are considered. A comparison of protection and user identification mechanisms has been carried out. Methods for improving the performance of web applications are presented.

Key words: operating system of a special purpose, web application, web server, mandatory access control, authentication, Kerberos protocol.

Ismailov D., Litvinov V. Increasing the Efficiency of Warehouse Management Systems (WMS) by Optimizing Goods Placement. – PP. 345–349.

The scientific article examines strategies for optimizing time and placing goods in a warehouse in conditions of labor shortage. Using neural network analysis data and a simulation model, an innovative approach is proposed aimed at increasing the efficiency of warehouse logistics and reducing labor costs, taking into account the balance between placement by product groups and ABC analysis. The authors foresee practical testing of the developed methods in warehouses, with an emphasis on taking into account the cost of moving goods.

Key words: WMS, Warehouse Management System, warehouse management system, warehouse logistics.

Kalinyuk A., Konstantinov S. Comparison of SQL and NoSQL Databases. – PP. 350–356.
Modern software is often faced with the task of processing terabytes and even petabytes of data. Distributed computing is widely used to solve this problem, which imposes new requirements on the DBMS: scalability and the ability to process transactions in a distributed manner. In distributed systems based on a relational data storage model, performing transactions and pooling operations involving a large number of cluster nodes is difficult and inefficient. This has led to the growing popularity of non-relational databases, which allow for greater flexibility, better scalability and high fault tolerance. Such databases are called NoSQL.

Key words: SQL, NoSQL, DB, DBMS.

Kovalev I., Nogin S., Pantyukhin O., Pashchenko V. General Approach to Determining Computer Network Monitoring Nodes. – PP. 357–360.
Maintaining the functionality of computer networks remains an urgent problem. One of the ways to solve this problem is to monitor various network parameters. The choice of appropriate parameters and places for their monitoring are largely determined by the purposes of monitoring.

Key words: computer networks, monitoring, monitoring node, monitoring parameters, selection of monitoring node.

Kovalev R., Saltanov A. The Problem of Using Control Systems Document-Oriented Databases. – PP. 361–364.
The paper considers the problem of the choice and application of document-oriented database management systems. This problem is a cause-and-effect relationship in the formulation of the task of developing software and algorithmic software for managing document-oriented databases used at various stages of the product lifecycle. The popularization of non-relational databases requires an in-depth study of their qualitative properties, advantages and disadvantages in the management of document-oriented databases intended for use in related fields of enterprise activity, or in the production of dual-use products.

Key words: database management system, document-oriented databases, relational databases, non-relational databases

Kozinov E., Lukyanov V., Khomutovsky S., Petrova T. Comparison of Domestic Software for Creation of Game Content with Foreign Analogues. – PP. 365–368.
In the article, the authors consider the functionality of game engines of foreign and domestic production. The article presents a comparison of the main characteristics of the most commonly used game engines in the modern GameDev industry. The authors focus on the need to develop domestic software for creating game content, since at this stage there is a lag behind foreign software in terms of functionality and ease of development. The authors conclude that despite the high threshold for entry into the domestic game engine Unigine, it has wide development functionality in the field of augmented and virtual reality, but it also requires development in other areas.

Key words: Game engine GameDev, Unreal Engine, Unity, Unigine.

Kolmakov A., Litvinov V. Development of a Prototype of a Software Module for Implementing Realistic Behavior of Virtual Agents in Unreal Engine 5 Using the Environmental Query System (EQS). – PP. 369–371.
Technologies for implementing the intelligent behavior of virtual agents in the built-in tools of Unreal Engine 5 have been investigated. The main five components have been identified: the

agent controller, the behavior tree, the senses, the environment query system (EQS) and animation editing. These technologies are used to solve the avoiding obstacles problem by agents with different values of EQS input parameters - with greater agent behavior accuracy, the load on the computing resource gradually increases, which leads to low FPS values. This suggests that solving the problem of increasing realism by increasing the number of points and decreasing the distance between environment query system (EQS) points leads to subtle results and unnecessary performance losses.

Key words: Virtual agent, spatial query, FPS, obstacle avoidance task.

Komashinskiy T., Chikalov N. Clusterization of Http-Requests Using the Method of Self-Organizing Kohonen Networks. – PP. 372–378.

The article presents an approach to solving the problem of searching for targeted computer attacks at the application level, based on self-organizing Kohonen neural networks. The purpose of the study is to increase the efficiency of detecting anomalies and attacks in web traffic. This article examined the detection of SQL injections by clustering the Kohonen network of incoming HTTP traffic requests.

Key words: Kohonen networks, HTTP request clustering, self-organizing networks

Komashinskiy T., Chikalov N. Model for Monitoring the Behavior of Corporate Web Users. – PP. 379–381.

It is known that one of the main causes of danger in web applications is the generation of anomalous traffic, non-profile traffic, changes in the behavior profile of a web application or web user, untrusted frameworks and modules that are “overloaded” with unnecessary functionality, etc. All this creates an unnecessary load that makes access to the web resource difficult. This circumstance is one of those events that sooner or later corporate web applications that are not adapted to different types of load may encounter. Taking this into account, to determine the behavior profile of a web application and a web user, a structural model of a virtualized web application monitoring function is proposed.

Key words: Virtualized network functions, web application monitoring, monitoring model.

Komashinskiy T., Chikalov N. Proposals for Forming a Web Application Monitoring System Based on Virtualized Network Functions. – PP. 382–384.

The growth of web applications has made monitoring web resources a major challenge. The presence of a large number of libraries and frameworks increases the number of potential vulnerabilities in the final web application.

Modern Web Application Monitoring is a synthetic monitoring solution that continuously checks the response time, content, overall performance of web applications, security. In this paper, the authors propose a structural model of a virtualized web application monitoring function.

Key words: Virtualized network functions, web application monitoring.

Kopylov S., Mihajlova E. About Some Aspects of Malware Static Signs. – PP. 384–389.

Malicious software remains the most significant threat to the information security of user’s confidential information and personal data. A significant increase in the volume of transmitted and processed information has shown an increased number of cases of embedding and subsequent spread of malicious code into data types containing protected information. This feature makes the task of identifying the feature space characterizing malicious software embedded in various file formats a relevant research area. The work provides an the static signs overview

of malicious software, presents their description and provides the distinctive features inherent in files containing embedded malicious code.

Key words: malware, static signs.

Kopylov S., Polehin A. Functional Model of Embedding Malicious Software Containing Anti-Analysis Tools Into PDF Files. – PP. 390–394.

Ensuring information security of information systems is one of the most relevant areas of cybersecurity policy implementation. The rapid growth in the number of information security violation incidents makes the task of improving security measures a relevant research area. To solve this problem, it is necessary to evaluate not only existing security measures and their inherent shortcomings, but also the implementing computer attacks means. The paper presents a functional model for introducing malicious software containing anti-analysis tools into PDF files. The developed model takes into account the features of the malicious code embedding into the structural components of PDF files and the obfuscating transformations usage used to protect embedded malicious code from static analysis methods.

Key words: malware, PDF files, obfuscation.

Kopylov S., Capkov N. Detecting Malware in PDF Files Using Viewer Code Coverage Analysis. – PP. 395–399.

Recent years have been marked by a significant increase in the share of electronic document management in information interaction various areas. Electronic documents are an integral part of the work of many organizations, simplifying the information exchange processes and data management. At the same time, with the growing use of electronic documents, there is an increase in the number of information security violations associated with the malicious software embedding. The most common type of data containing malware is the PDF format. Due to the popularity of this format, there has been a significant increase in information security violations. To reduce the number of incidents of information security violations when working with PDF documents, it is necessary to develop new or improve existing means of detecting malicious code. A proposed detection approach could be one based on dynamic analysis of PDF document viewers. The paper describes an approach to detecting malicious software by analyzing the code coverage of a PDF document viewer.

Key words: malware detection, fuzz testing.

Kopytova E., Mavrichev V., Petrov D. Fillipov F. Ethical Issues in Artificial Intelligence. – PP. 399–402.

The development and application of artificial intelligence brings with it many ethical issues that require attention and discussion. One such challenge is the use of autonomous decision-making systems. How much can we trust artificial intelligence to make decisions? Which of these decisions could have fatal consequences for individuals or society as a whole? How to avoid the fate of James Cameron's universe? Rules, ethical principles and restrictions are the only way to ensure the safety and reliability of such systems. The article will examine issues related to the development and application of artificial intelligence, including autonomous decision-making systems, data security and privacy, as well as inequality and possible social consequences.

Key words: artificial intelligence, ethical principles, ethical regulation of artificial intelligence, copyright, license agreement.

Korovkina E., Litvinov V. Analysis of Vulnerabilities in Maritime Information Systems. – PP. 402–405.

The study provides an assessment and analysis of the primary ship-specific technologies susceptible to cyber-attacks. This research holds significance in light of the integral role maritime transportation plays in contemporary society. The precision of vessel instrumentation is paramount, as any compromise in operational systems could lead to catastrophic consequences. Thus, it is imperative to identify, anticipate, and mitigate potential threats to information security within maritime environments. Key ship systems susceptible to vulnerabilities are examined, including Bridge Navigation Systems, Cargo Systems, Propulsion and Energy Management Systems, Onboard Access Control Systems, Passenger Service Systems, Public Networks, Crew Welfare Systems, and Radio Communication and Telecommunication Systems.

Key words: pertinent to this study include cybersecurity, maritime transport, cyber-attacks, ship security, and technical safeguarding measures.

Kosenkova A., Nesterov S. The Assessment the Effect of Changing the Size of a Write-Ahead Log Segment on Database Performance in PostgreSQL. – PP. 406–410.

The paper describes the effect of changing the size of the Write-Ahead Log segment (`wal_segment_size`) on the performance of the PostgreSQL database. The Write-Ahead Log plays an important role in maintaining data consistency when a server fails. On disk, the log is stored as a sequence of files, also called segments. Configuring log parameters can help to increase database performance.

Key words: databases, PostgreSQL, Write-Ahead Log.

Kosov P., Labkovskaya R. Data Visualization in R Programming Language. – PP. 411–415.

Data visualization is an extremely valuable skill as well as a powerful tool for studying patterns, trends and relationships in data sets. Visualization is a key step in the use of Open Data, as it provides a better understanding of the problem area, extracts and transfers the basic knowledge from the data, and guides future analysis using more sophisticated methods. In order to create objective, visual and understandable visualization graphs, certain basic principles need to be taken into account, as the process can be complex. This article is devoted to the consideration of the key principles of data visualization in R programming language.

Key words: data visualization, data analysis, ChatGPT, open data, R.

Kosov P., Labkovskaya R. ChatGPT for Data Analysis. – PP. 416–421.

The article is devoted to an innovative approach to Data Analysis with ChatGPT in R language. The paper discusses various features of ChatGPT that will help to optimize data analysis processes, including data sets, statistical summary generation, visualization and Shiny interactive applications. Special attention is paid to interaction with ChatGPT through queries in R language for automation and improvement of data analysis processes.

Key words: data analysis, chatbot, ChatGPT, R, artificial intelligence, data visualization.

Krasavtseva K., Rakovsky O. Research and Analysis of the Potential for Automation of Microclimate Monitoring. – PP. 422–426.

The main aspects of the development of microclimate monitoring technologies are considered and analysed. The range of applications for such technologies and the prospects for automation

are defined. A review of the technical tools used for monitoring microclimates is conducted. The features of microclimates as an automation target are identified.

Key words: microclimate, monitoring, microclimate monitoring, analysis, instrument, sensor.

Krivko D., Markin D. Automation of Penetration Testing Based on the Results of Ranking Information about Vulnerabilities. – PP. 427–431.

The article presents the results of the development of a penetration testing automation tool, taking into account the results of ranking information about vulnerabilities. A description of the interaction of the structural elements of the automation tool with scanning tools, vulnerability registries and information about the presence of exploits is presented.

Key words: penetration testing, vulnerabilities, exploit, scanning.

Krivolapov D., Pavlovich A. The Choice of Technology and Software for Visual Quality Control Processes of Assembly Operations. – PP. 432–436.

The ways to reduce the complexity and ensure the efficiency and simplicity of the learning process for assembly operations for engineers in the field of telecommunications due to modern technologies of virtual/augmented and mixed reality based on general application tools are considered. The procedures for analyzing and selecting software tools for modeling informative models, as well as procedures for selecting and analyzing technology for their detailed display, are investigated. The results of the application of the integration option of the selected software tools are presented.

Key words: telecommunications, augmented reality, virtual reality, automation.

Krylova E.R. Organization of Automatic Management of Temporary Labor Collectives (Team-Works) within the Framework of a Virtual Enterprise Using a Rating System. – PP. 437–440.

The article deals with the problem of optimized formation of temporary labor collectives (team-works) based on virtual enterprises, and also addresses the issue of developing a rating system or an electronic reputation system within companies, and suggests a way to use the web application interface to automatically calculate the rating of a participant in the cyber environment from a legal (corporate) entity.

Key words: cyber environment, virtual enterprises, electronic reputation, smart manufacturing, temporary labor collectives, team-works, rating system.

Kuznetsova O., Kulikov D., Trubchaninov K. GIS Service for the Delivery of Micro-Greenery in the Murmansk Region. – PP. 441–445.

Recently, microgreens have gained great popularity and now it is becoming easier to purchase fresh greens. Despite the growing interest, the issue of delivering micro-greenery still remains unresolved. The way out of this situation may be the use of geoinformation systems.

Key words: geoinformation support, GIS service, micro-greenery, micro-greenery delivery.

Kuznetsova O., Popova V. Mobile Application for Visualization of Iconic Personal Sites. – PP. 446–450.

Geoinformation systems and mobile technologies have become firmly embedded in the lives of most people – their personal sphere is no exception. Visualization of iconic places on the map

using a mobile application provides the widest possibilities for constructing and preserving personal history.

Key words: geoinformation support, mobile application, visualization, personal iconic sites, personal history construction.

Kuznetsova O., Yavdoshchuk V. Geoinformation Application for the Promotion of IT Directions of Higher Education. – PP. 451–454.

The goal of any university is to provide 100% enrollment of students who meet the requirements of the university in terms of knowledge and desire to obtain relevant specialties. To achieve this, it is necessary to contact the applicant in advance, and not at the time of submitting documents, and / or only providing information about the specialties being studied. Geoinformation technologies will help to significantly facilitate interaction with potential applicants.

Key words: geoinformation support, geoinformation application, IT directions, promotion of IT directions.

Labkovskaya R., Tarasov V. A study of the Approach to the Intellectualization of Corporate Information Infrastructure Management. – PP. 455–457.

A modern organization, even a small one, cannot be imagined without a developed and diverse information infrastructure that requires operational management, maintenance and modernization. The efficiency of the organization's work and, ultimately, its profit, reputation, etc. depend on the speed and accuracy of decision-making in managing the components of a corporate information system. It is necessary to form an approach to the organization of such management - the choice of optimization criteria, means and mechanisms for its implementation.

Key words: corporate information infrastructure, software-configurable network, traffic classification, machine learning, neural networks.

Lapko A. The Study Results of Transaction Behavior at Various Isolation Levels in PostgreSQL DBMS. – PP. 458–463.

The article is devoted to the transaction behavior study at various isolation levels in the PostgreSQL DBMS. The anomalies possible in the database during parallel execution of transactions are given. Data snapshots, the behavior of SQL statements and the causes of anomalies at various levels of transaction isolation in the PostgreSQL DBMS are described in detail. Sets of SQL statements that in parallel running can lead to an access error and rollback of the last committed transaction at various isolation levels are presented.

Key words: database, parallel execution of transactions, PostgreSQL DBMS, transaction isolation level, data snapshot, SQL statement, commit and rollback of a transaction.

Lebedev D., Shiyan A. Comparative Analysis of Level Editors in Realistic UAV Simulators. – PP. 464–466.

This article provides a comparative analysis of level editors in UAV simulators. The comparison took into account the functionality for creating landscapes, the ability to customize the scenario, change weather, edit physics systems, display object hierarchy. The level editors of the simulators Liftoff, AI Drone Simulator, Velocidrone and The Drone Racing League Simulator were reviewed.

Key words: UAV, simulator, level editor, scenario editor.

Lipatnikov V., Parfirov V. A Decision Support Method for Managing A Communication Network Based on Neural Network Technology. – PP. 467–472.

A method is proposed in which a neural network, depending on the availability of resources, determines sets of actions that are evaluated for compliance with the result of their application with the specified criteria with maximum efficiency. The developed method can be used in decision support systems in the interests of ensuring the sustainable functioning of communication networks, as well as other complex organizational and technical systems operating under destructive influences.

Key words: communication network, neural network, criterion, management efficiency, management actions, decision support system, management decision, resource.

Litvinov V., El Zabayar Shevchenko N. Algorithm for Reducing Inhomogeneous Discrete Time Values of Finite Markov Chains to a Homogeneous Form. – PP. 473–477.

The problem of bringing non-uniform discrete time values in finite Markov chains to their homogeneous form has been updated. The situations in which it is necessary to apply this algorithm are described. The main stages of the algorithm formation are revealed. Software has been developed for simulation of the algorithm. Experimental studies and comparative analysis of the results of a finite Markov chain using the developed algorithm were carried out to confirm its computational correctness. The practical significance of using the developed algorithm in modeling probabilistic processes based on finite Markov chains is revealed.

Key words: finite Markov chains, discrete time, time profile, quality indicators, heterogeneity.

Lyubimov A., Lyubimov C. On the Issue of Solving the Traveling Salesman Problem In Automation and Control Systems. – PP. 478–482.

The paper shows the features of solving the applied problems of a traveling salesman by heuristic methods and algorithms in a travel form. A method of layered decomposition of an undirected weighted graph is proposed to search for a Hamiltonian cycle of minimum weight using invariant structures and a procedure for tightening edges.

Key words: the traveling salesman problem, the Hamiltonian cycle of minimum weight, heuristic methods of combinatorial optimization, invariant structures, layered graph decomposition.

Maksimova S., Musaeva T. Analysis of Current Problems in Creating Graphical User Interfaces. – PP. 483–487.

The article discusses the problems of developing graphical interfaces for websites, mobile applications and information systems that are relevant today. The problems of the complexity of providing the cognitive properties of one interface for different categories of users, the imperfection of scientific knowledge about the human brain, the availability of eye-tracking technology, and interface adaptation are considered. Conclusions are drawn about possible ways to solve the identified problems, and directions in which research is needed are identified.

Key words: user interface, graphical interface, usability, cognitive interface, adaptive interface.

Mannanov A., Shiyan P. Modern Aspects of Cyber Security and Data Protection. – PP. 488–492.

This scientific article discusses key issues in the field of cybersecurity and methods of data protection in the modern information society. The article examines modern challenges and

threats faced by organizations and individuals, and proposes methods and strategies for ensuring information security.

Key words: cybersecurity, cybersecurity system protection, information protection, information environment, symmetric encryption, program, data protection.

Matveev A., Naidenov O., Paramonov A. Overview of Vulnerabilities and Security Trends in the Internet of Things. – PP. 493–496.

This article highlights the integration of Internet of Things (IoT) devices into various business domains, which has brought unprecedented convenience and efficiency, but has also led to a myriad of security challenges. The diverse range of security vulnerabilities inherent in IoT ecosystems is examined. Factors such as weak authentication, legacy asset vulnerabilities, inconsistent security standards, and gaps between mobile networks and the cloud are explored. Famous incidents such as the Mirai botnet and the Target credit card data leak are also examined in detail. In addition, the paper describes a range of potential solutions, from strengthening physical defences to implementing strong encryption protocols and using network firewalls. The purpose of this study is to provide a comprehensive understanding of IoT security issues and suggest viable strategies to address them.

Key words: internet of things (iot), information security, security threat, iot vulnerabilities.

Matveev P., Filippov F. Development of Service for Charitable Foundations Supporting Using Ethereum Smart-Contracts. – PP. 497–500.

The relevance of developing a service to support charitable foundations using smart contracts in the Ethereum blockchain network is presented. The structure of the service for supporting charitable foundations is described. A technology stack has been defined for the development of service subsystems. An algorithm for automated fundraising on a smart contract and their transfer to the blockchain wallet of a charitable organization upon completion of fundraising is described. The development of a service interface using the Metamask blockchain wallet is described.

Key words: charity, blockchain, smart contract, development of an automated system.

Musaeva T., Ramzaev K. Mobility Module Based on Stuart Platform. – PP. 501–505.

In a dynamically developing world, a large number of products and equipment appear, the study and use of which requires special highly qualified competencies of employees. Some of them belong to sources of increased danger or are included in the list of dangerous devices for their intended purpose and functionality, which imposes special requirements for their use and training. In this regard, there is a need for a new approach using modern tools and technologies used in teaching.

The article analyzes the existing types of mobility devices based on the Stewart platform, and examines their control systems. The conclusions made will allow us to develop a high-quality and flexible control system for a domestic simulator. The expected results of the development are to improve the user experience and expand the scope of application.

Key words: Gough-Stewart platform, mobility module, six degrees of freedom, control system, simulator control tool.

Musaeva T., Titov P. Analysis of Problems and Peculiarities of Personalization of Online Education. – PP. 506–511.

The article deals with the application of the method of personalized choice of educational course in online format taking into account individual needs of a person.

The research is conducted, the Russian market and popular platforms of online education, offered tools, current trends and promising directions of development are analyzed. The main problems and proposals for their solution have been identified.

Also, the main individual and cognitive characteristics of a person are investigated to determine their influence on the effectiveness of the learning result. Based on the conclusions drawn, a method of selecting personalized online courses taking into account individual characteristics of students is proposed.

Key words: online education, course selection, individual characteristics, personalization of education, course aggregators.

Novikov E. Group Control Problem, its Analysis and Solving Methods. – PP. 512–516.

The problem of controlling group (swarm) of agents is examined. In order to describe field of the problem, problem conditions are systematized, widespread analysis methods and solving approaches are examined. Specifically, the taxonomy for classifying different problem settings is provided, solutions analysis methods are described, group behavior approaches are provided.

Key words: Group control problem, swarm control, swarm robotics, multi-agent robotic system, multi-agent system.

Paskenova A. DLP System as an Incident Investigation Tool. – PP. 517–520.

Today, due to the increase in the number of cases of information leakage and violation of its integrity by employees, the topic of protection against threats in the field of information security is becoming very relevant. In addition, most enterprises and companies are moving into the category of the military-industrial complex (MIC), which makes this topic even more relevant. In addition, in order to form a high-quality regulatory framework, it is necessary to thoroughly and qualitatively form judicial practice in the field of information protection. In solving all these tasks, DLP systems are used, which, in turn, perform the role and functions of protecting information from threats, an incident investigation tool, as well as the formation of typical incidents to enable further investigation and the formation of a modified legal framework.

Key words: DLP-systems, investigation of information incidents, analysis and prospects for their development.

Pestov I., Smurov I., Fedorov P., Fedorova E. Analysis of Methods for Detecting Anomalies and Attacks in Cloud Infrastructures. – PP. 521–526.

Cloud infrastructures are becoming more popular and more important for various companies and organizations. However, with the increasing use of the cloud, the number of potential security threats, such as anomalies and attacks on information systems, also increases.

Analyzing methods for detecting anomalies and attacks in cloud infrastructures is critical to ensuring the security of data and resources in the cloud. In this article, we will look at various approaches to detecting anomalies and attacks in the cloud, including the use of statistical methods, machine learning, behavioral analysis, log analysis, and signature analysis.

Key words: Cloud infrastructures, security threats, attacks, anomalies.

Prokofev P. Multidimensional Models of Geographical Objects. – PP. 527–530.

The general structure of georelational databases is considered. Multi-aspect models of geographical objects are presented, allowing one to describe natural and anthropogenic objects within a single multi-aspect environment. The results of this work can be used to implement software that allows solving problems of geographic information modeling, analysis, planning and management of spatially distributed objects within a geographic region.

Key words: GIS, cartography, geographical objects, databases, multi-aspect models.

Pshenichnikova D., Sabinin O. Translation of Relational Algebra Operations into SQL Commands Taking into Account Restrictions for Operations. – PP. 531–535.

This article discusses the possibility of translating relational algebra operations into SQL commands. The eight operations of relational algebra and their limitations are reviewed. A method is proposed for translating relational algebra operations into SQL. An algorithm for checking the constraint: coincidence of relationship patterns is considered.

Key words: relational algebra operations, SQL language, DBMS_SQL package.

Rakovsky O., Chuharev I. Development of a System for Analyzing Student Performance. – PP. 536–538.

The article discusses the importance of performance analysis for organizing successful student learning. There are many factors to consider that may influence student performance. For example, such factors are admission scores, form of education, class attendance, and exam results. The main goal of such analysis is to improve the quality of training and control over the progress of the educational process.

Key words: analysis, educational process, students, assessment, factors

Rakovsky O., Chuhareva E. Identification of Consumer Preferences in Order to Improve Marketing Activities. – PP. 539–541.

Analysis of consumer preferences is an important tool for improving marketing activities. It allows you to identify the most popular goods and services, determine the target audience, adapt products to consumer needs and improve the quality of service. The results of the analysis help companies develop effective marketing strategies and improve customer satisfaction.

Key words: Marketing activities, target audience, needs.

Romadova P. The Algorithm of Personalized Recommendations of Leisure Places for Tourists. – PP. 542–545.

This article describes an algorithm for recommending places of interest to tourists. To create a list of suitable places to visit, the user's preferences are considered. This is done by filtering based on content, checked by the similarity of the vectors of the description of places. The result of the algorithm is a ranked list from the most to the least suitable places for the user in accordance with his preferences.

Key words: Content-based filtering, recommendation systems, algorithm, tourism.

Ruban E, Smorodin G, Shanenko D. Analysis of the Development of CRM Systems. – PP. 546–550.

An analysis of the possibilities and prospects for the development of CRM systems in the information ecosystem of the corporation is carried out. The main advantages and disadvantages of

CRM systems are noted, taking into account the opinions of leading analysts of information systems and trends in the development of corporations. The structure of the CRM system and solutions based on artificial intelligence, which allow you to significantly optimize the behavior of the CRM system, are shown in detail.

Key words: CRM systems, Customer Relationship Management, Cloud Technology, Business Processes.

Soloviev A., Sorokin N., Tikhonov S. Application of Artificial Intelligence in Software Engineering. – PP. 551–554.

In the context of technological progress and the spread of artificial intelligence (AI), the impact of AI on software engineering is considered. It is emphasized that automation of various stages of the life cycle of a software product thanks to AI significantly reduces code development time. Emphasizes the role of machine learning in data analysis, performance optimization, and creating models to predict trends. In addition, successful examples of the use of AI in various fields such as healthcare, finance and technical support are discussed. Specific projects such as GitHub Copilot and Tesla Autopilot. Finally, it is emphasized that flexibility and adaptation of programmers to the capabilities of AI are becoming key competencies in an era of rapid technological development.

Key words: artificial intelligence, software engineering, chatbots, information technology.

Spiridonov D., Fedorchenko E. Modeling attacks based on Microsoft Kubernetes Threat Matrix. – PP. 555–557.

Today, the use of Kubernetes in the field of information technology has become widespread. This platform allows you to deploy and configure cloud infrastructure. The effect of attack detection based on the Microsoft Kubernetes Threat Matrix is at work. Attack modeling allows you to assess the vulnerability of the Kubernetes system to known attacks, as well as determine a set of defenses and minimize the damage from possible attacks.

Key words: Microsoft Kubernetes Threat Matrix, Kubernetes, Docker, Attack modeling, bas.

Strelets C., Shabanov A. The Cryptocurrencies and Blockchain: Responsibility and Potential in Digitizing Government Administration. – PP. 558–562.

The main goal of this article is to research how cryptocurrencies and blockchain could bring value for the government and help with providing public services. It explores the advantages of cryptocurrencies, including improved transparency and cost reduction, as well as the benefits of blockchain technologies, such as data reliability and enhanced identification systems. It examines the challenges that could be faced in the process of integration of these technologies into the public sector.

Key words: Digitization, government administration, blockchain, distributed ledger technologies, cryptocurrencies, digital currencies, electronic document management, electronic voting.

Trofimenkov A. Verification of Anomalies at Processing of Panoramic Images. – PP. 563–565. *Synthesis of the panoramic images generated from video shots, the pilotless flying machines received from the chamber, shows that there are distortions during algorithm work of connection initial pictures in a panorama. Procedure of an establishment of reliability of the found out anomalies can be considered as their verification.*

Key words: anomalies; fuzzy sets; detection; panoramic images; filtration, verification.

Fedorova M., Yugai O. Automated System for Accounting for Radio Electronics Element Base. – PP. 566–570.

Recently, thanks to the active development of IT technologies, the field of digital accounting and control in various areas of human activity is rapidly developing. A high degree of automation allows you to reduce working time, which serves as a significant incentive to increase labor productivity, as well as avoid a number of human errors, and as a result, maximize profits and minimize labor costs. The article discusses a specially developed web application, the functionality of which allows you to keep track of the manufacturer's availability of components for the production of radio-electronic devices.

Key words: digital accounting, automation, labor productivity, labor costs, web application.

Fedorova M., Yakovlev D. Automation System for Goods Accounting and Cargo Transportation Management. – PP. 571–576.

Recently, by digitalization, the transport logistics industry is moving away from the usual paper work and active human participation in the process of transportation management and warehouse accounting. Automated systems include specialized software and hardware to optimize distribution processes within an organization. The implementation of data systems allows you to improve communication between different departments, reduce time for operations, effectively save material resources and evaluate the effectiveness of employees. The article discusses the provided and developed software that provides functional two subsystems - transport management and warehouse accounting, as well as console interaction between them.

Key words: automation, cargo transportation, integrations, monitoring, REST.

Khamzina O. The Problem of the Relevance of Search Results in Electronic Library Resources. – PP. 577–580.

As the volume of scientific publications grows in electronic form, it becomes increasingly difficult to effectively search for up-to-date information. This article explores the problems of multi-criteria searching in scientific electronic library resources, considering the publication date as the most important criterion. The article analyzes the influence of a multi-criteria approach on the effectiveness of search results, identifies the main problems and proposes ways to solve them.

Key words: search engines, search engine analysis, multi-criteria search.

Chupakhin I., Shiyan P. Where Will Machine Learning Have the Biggest Impact? – PP. 581–586.

This article will provide a comparative analysis of the use of machine learning in various areas of our lives. Statistics on the use of machine learning based on the development of technology and the power of computing systems will be considered.

Key words: machine learning, artificial intelligence, natural language, computer system, artificial neural networks.

Аньшаков А. Е., Галиева Т. Р. RabbitMQ: принцип работы и применение в многомодульных ПО. – С. 587–591.

В статье рассматривается основной принцип работы брокера сообщений RabbitMQ. Представлены примеры практического применения RabbitMQ как средства коммуникации различных ПО и сервисов. Описывается алгоритм использования протоколов прикладного уровня для передачи сообщений между компонентами системы. Статья предназначена для разработчиков ПО и архитекторов приложений.

Ключевые слова: RabbitMQ, AMQP, типы кадров, коммуникация, автоматизация рабочих процессов.

ANNOTATIONS

INFORMATION SYSTEMS AND TECHNOLOGIES

Absattarov G., Abylhasenov M., Burlakov A., Shakirbekov D. Centralized Data Classifier as a Tool for Providing Regulatory and Reference Information for Applied Information Systems. – PP. 5–9.

The article discusses the issues of constructing and maintaining a centralized data classifier as a tool for centralized provision of regulatory and reference information for applied information systems. The use of technology on an existing automated control system will reduce the cost of technical operation through the use of potential, centralized maintenance of regulatory and reference information of information systems.

Key words: centralized classifier, information systems, operational data.

Averyanov A., Dolgov E. Development of a Software Package for Automated Analysis of the Security of Information Telecommunication Networks. – PP. 10–15.

In today's world, information protection is becoming more and more relevant. With the development of digital technologies, the number of threats related to the violation of confidentiality, integrity and availability of data is increasing. Particular attention is paid to the protection of information systems of public institutions, as they are objects of increased interest for attackers who can cause serious damage to national security. The article discusses the relevance of creating a software package for comprehensive analysis of network infrastructure security, identifying possible vulnerabilities and developing recommendations for their elimination, thus increasing the overall level of IS.

Key words: penetration testing, security analysis, information security.

Avramenko V., Chichkov E. Software Package for Experimental Evaluation of Neural Networks Efficiency. – PP. 16–19.

The method of experimental estimation of efficiency of variants of realisation of various architectures of neural networks on the basis of the software complex providing identical initial data and conditions for testing of the estimated neural networks is offered. The structure and description of the software complex operation, neural networks efficiency indicators are presented.

Key words: neural network, software system, indicator, evaluation, efficiency, accuracy, resource intensity, efficiency.

Agafonov N., Vozgrin G., Volynkin P. Development of Software for Collecting Information About Objects on a Limited Area by a Mobile Robot ROBO-PICA. – PP. 20–24.

The software for the ROBO-PICA robotic platform is presented, which allows a mobile robot to scan a site of limited dimensions for the detection of 5x5 cm objects on it. The robot moves along a given contrasting trajectory line. When an object is detected using a distance sensor, the robot signals this with an audible signal, drives around an obstacle and stores the location of the detected object in memory. After the surface scanning is completed, the robot re-runs the distance, but in the absence of objects. In the places of the former location of objects, the robot makes it clear by an audible signal that an object was previously in this place.

Key words: mobile robots, area scanning algorithms, solving hardware problems.

Agenosov D., Baisarin B., Pogodin N., Svechnikov D. Security Risk Ranking Penetration Test Management Software. – PP. 25–27.

This article discusses proposals for building a penetration test software tool based on ranking security threats. The software tool allows you to obtain data for scanning, collect information from tested hosts, find vulnerabilities and generate exploits, and generate reports. The developed proposals ensure the receipt of objective data based on the results of security studies of the facility.

Key words: security threats, vulnerability scanning, penetration testing software.

Al-Nami B., Babayeva E. Research and Comparison of Photodetectors. – PP. 28–31.

In 2024, photographers are still hotly debating the advantages of Lightroom over Photoshop. Each platform provides powerful editing features and tools, but it is important to understand their differences in order to make an informed decision. In this article, we will compare Adobe Photoshop and Lightroom, talk about the differences and similarities of the software.

Key words: quality, reliability, control of processes and products, radiophotonics, photodetector, radiophoton transmission line, Adobe Photoshop, Adobe lightroom.

Al-Nami B., Beliaeva N. UI-design of a Flower Delivery Mobile App. – PP. 32–36.

This article aims to study the use of flower delivery mobile applications, analyze the visual and functional representation of the design for such an application, as well as to assess its analogues.

Key words: UI-design, graphical user interface, mobile application, development tools, interface, design, mobile applications, implementation, design.

Al-Nami B., Bokov I. The Role of Neural Networks in the Development of Machine Translation. – PP. 37–40.

The main goal of the following article is an introduction to the principles of operation of neural networks during machine translation of text. In addition, the article provides the world history of machine translation, its current problems and development prospects, as well as general information regarding the principles of operation of neural networks.

Key words: neural networks, automation, machine translation, natural language, artificial intelligence, machine translation technologies.

Al-Nami B., Pigareva J. User Interface Development Website of the Logistics Company. – PP. 41–44.

This scientific article is devoted to the development of the user interface of the logistics company's website to solve the existing problem of the disparate storage of branded products and documents. The article discusses the process of creating a specialized section on a web platform designed for convenient employee access to current versions of document templates, presentations, logos and other branded materials.

Key words: website, interface, carousel, identity, design, user, flat design, user interface, visual interface design, user experience, interface design, site interfaces.

Al-Nami B., Selina V. Encryption and Decryption of Information. – PP. 45–49.

This article discusses the problem of information leakage and falsification. The purpose of the work is to study cryptography and identify a method for protecting transmitted information. During the work, the need to protect information was identified. As a result, the “encoder” program was written, with the help of which information is encrypted and then decrypted in order to prevent the possibility of reading and forging it.

Key words: encryption, decryption, information protection, information environment, symmetric encryption, program, cryptography, cryptographic keys, shared private key, authentication.

Al-Nami B., Simkin K. Exploring the Difference in Using Functional and Object-Oriented Programming in Python Language. – PP. 50–52.

At the beginning of the article, we will understand the definitions of these. In the modern IT industry, there are a huge number of different programming languages, they mainly use two types of programming: object-oriented and functional. This article will examine the use of these types of programming in the Python language, as one of the simplest and most popular in the industry.

Key words: Python, programming language, web development, Python libraries, language syntax, object-oriented programming.

Al-Nami B., Tuzhikova M. Fundamentals of Modern Containerization. – PP. 53–57.

With the development of information technology and software development, the growth in the number of programs and their volume, a need arose for some tool that would allow programs to be quickly and easily deployed on various devices and operating systems. We need an assistant who would simplify the process of creating an environment in which all the application's dependencies will be taken into account, and in which it can run without problems, which, of course, will make life much easier for programmers.

Key words: containerization, development, data, applications, management, resource, monitoring, indicators.

Al-Nami B., Tsyganova D. Choice of Program for Graduates of the Bachelor Program in the Profession of Design Engineering. Guide to Using Georecounter. – PP. 58–63.

Many graduates of a bachelor's degree program are faced with the challenge of learning new programs that can make their jobs in engineering and design easier. This article will help them become familiar with the program for future design engineers and demonstrate its functionality, and we will also look at an example of its work on one of the most popular computer-aided design and drawing systems - Automated Computer Aided Drafting and Design - design using computer technology.

Key words: design, Automated Computer Aided Drafting and Design, AutoCAD, engineer, drafting.

Apostolevskiy D., Klimov A. Confidentiality of Personal Information on the Internet. – PP. 64–67.

The Internet has become an integral part of our lives. It gives us access to information, helps us in study and work, and allows us to communicate with friends and family. However, in addition to its many benefits, the digital landscape poses inherent risks to personal safety and security. This article will discuss the types of Internet dangers and methods to combat them.

Key words: information security, personal data protection, legal regulation, safe Internet, cyberbullying, grooming, social networks.

Artamonov N., Vasiliev N., Vitkevich N., Kustov A. Overview of Smart Home Sensor Analyses. – PP. 68–72.

This article describes the architecture model of the Internet of Things, as well as a comprehensive comparison of various smart home systems, such as Google, Yandex, Xiaomi and Apple technologies, with an emphasis on their functionality, usability, integration with other devices, as well as aspects of data security and privacy. Through an analysis of the main characteristics and features of each system, the article allows readers to gain a complete understanding of the capabilities and limitations of various smart home systems, helping them make informed choices when planning or upgrading their home automation.

Key words: machine learning, smart home, automation technologies, information processing, device integration, functionality of smart home systems.

Artamonov N., Lipatnikov V., Melekhov K. Method for Network Control of Information and Telecommunication Network Security. – PP. 73–78.

This article examines the issue of developing a structure for network control tools and choosing neural network technology for building network security control tools. Various types of neural networks are considered and the most suitable neural network for network control is selected. The research results presented in the article may be useful for specialists in the field of information security and network technologies.

Key words: network control tools (NSC), information and telecommunication network (ITCN), neural networks.

Akhramenko A., Kuznetsova O. Software Application for Visualization of Plein Air Venues. – PP. 79–83.

Plein-air painting events demonstrate the growing interest among the population in Russia. Wide access to education and the development of creative communities create a favorable environment for the development of interest in the open air. Visualization of possible places for holding plein airs on the map provides the widest opportunities for everyone to capture places in the open air.

Key words: geoinformation software, software application, visualization, plein air, plein air venues.

Balakirev D. Generation of Facial Expression Animation for a Three-Dimensional Model Using Vocal Data. – PP. 84–87.

This work is devoted to the generation of facial expression animation for a three-dimensional model based on vocal data. The idea of facial expression animation is not new, but it requires hardware to track facial features. This work is devoted to the generation of facial expressions

using a software method involving artificial neural networks, which makes it cheaper and easier to create it. This can be used in the movie industry, the video game industry, as well as during virtual conferences and streaming using virtual avatars.

Key words: animation, 3D, modeling, three-dimensional model, neural network, generation, synthesis, facial expressions, avatar, video game industry, movie industry, simulation.

Balyberdin S., Bondarenko I., Zharanova A. Formation of a Telegram Bot Model for Searching for Musicians and Creating Collaborations. – PP. 88–93.

An innovative approach to organizing musical collaborations using a Telegram bot is considered. An analysis of existing services for searching for musicians has been carried out, and their shortcomings have been identified. The basic algorithms for data search and filtering are presented. The algorithm and method of calculating the similarity metric for issuing recommendations to the user are described. A model of an information system for searching for musicians and creating collaborations is proposed. The range of technological solutions for future development is given.

Key words: recommendation algorithms, similarity metric, recommendation system, Telegram bot.

Beckel L., Nikolaev A. Organization of Computer and Computer Network Security in a Secondary Educational Institution. – PP. 94–98.

Due to the rise in cybercrimes, schools need to ensure the security of computers and computer networks. First, we divide the school network into two networks, a network for teachers and a network for students. It is also necessary that anti-virus software be installed on computers. Some computers should have restricted access.

Key words: computer, computer network, security, secondary educational institution, attack.

Belous K., Gorbach A., Matyukhina V. Automated Telecommunication Equipment Control System – PP. 99–103.

Software products for monitoring network telecommunications equipment are designed for operational monitoring of processes occurring in networks, which allows you to quickly identify and eliminate failures, as well as monitor and neutralize emergency situations with minimal costs. Existing software products do not always make it possible to satisfy the needs of a specific user, and therefore the task of creating an automated system of this class is an urgent task.

Key words: computer network, equipment, database, control.

Belous K., Demidov A. Software for Visualizing Omron PLC Control Commands – PP. 104–107.

An overview of modern Omron PLC programming tools is presented. It is shown that existing software does not allow us to fully analyze the process of transmitting control commands to actuators, since they require their physical presence, which is not always possible. The Omron PLC and its role in automatic control are considered. A prototype of software written in the high-level language C# is presented, which allows one to analyze the structure of control commands, as well as their impact on virtual automation objects.

Key words: SCADA, PLC, visualization, software.

Besedin M., Zadboev V., Polishchuk V. Analysis of the Operating Principles of DNS Servers and DDoS Attacks. – PP. 108–112.

The article focuses on the relationship between DNS, which is a critical infrastructure of the Internet, providing transformations necessary for routing network traffic, as well as DDoS attacks, which pose a serious threat to the stability of network infrastructure through distributed denial of service methods.

Key words: DNS, DDoS, principles of operation, methods of attack, methods of influence.

Besedin M., Zadboev V., Sadovnikov V. Analysis of the Capabilities of the High-Level Python Programming Language for Automating Network Configuration and Monitoring Data Transmission. – PP. 113–116.

Problem statement: currently, there is an increasing need to automate various processes occurring in data transmission networks, including in situations where it is necessary to automate the configuration of a large number of network devices. The purpose of this article is to consider the question of the optimal choice of a tool for automating the processes of interaction between network devices. Results: the paper describes the main tools, highlights their disadvantages and advantages, and provides examples of the use of these tools in specific situations.

Key words: programming, networks, information security, automation.

Bikbulatov V., Meshkov A., Tkachev D. User identification using RFID tags. – PP. 117–121.

Unique identification technology using radio waves and the use of an RFID tag, which contains a microchip with a special identifier recorded and an antenna for receiving and transmitting a signal to special readers. An RFID tag is placed on a specific item to identify in real time of a person, animal or any product. Thus, let's look at the concept of RFID tag technology, operating principle, application advantages and disadvantages.

Key words: radio frequency identification, RFID tags, ISO standards.

Birikh E., Bulova M., Kazantsev A., Minyaev A. Development of a Software Module for Automating the Determination of the Level of Security Information Systems of Personal Data. – PP. 122–127.

This article presents the development of a software module written in Python, which allows you to automate the process of generating information security requirements in personal data information systems in accordance with the requirements of the Federal Service for Technical and Export Control of Russia.

Key words: information protection; data security; information security; security level, automated system, security threat, personal data information system, informatization object.

Bovshik P., Litvinov V. Automation of the Decision-Making Process in the Tasks of Configuring Software and Hardware Complexes for Storing and Processing Information. – PP. 128–132.

In the modern world, where almost every enterprise is struggling to reduce the downtime of work activities and the corresponding economic costs due to the human factor, the issue of automation of a particular process arises. To solve this issue, decision support systems are already being used. The paper discusses the concept of decision making in order to automate the work process of system administrators. As a result of scientific research, the basic concept of decision-making in problems of configuring software and hardware systems for storing and processing information is presented.

Key words: decision support system, configuration of software and hardware systems, information storage, information processing.

Boyko A., Kuzin P., Kuzina E., Potapov I., Usov N. Application of the Mathematical Model of the Light Path For Spectral Resource Management in Optical Transport Networks. . – PP. 133–137.

The paper provides a rigorous definition of light path. The concept of a light path is extended and clarified by combining the route of passage and the assigned spectrum of an optical signal. The set of acceptable light paths is proposed to be formed on the basis of the ratio of optical signal power to noise power in the light path bandwidth for a particular type of signal. A number of optimality criteria for solving the problems of search and distribution of light paths is presented. A mathematical model of the light path is developed, which allows to increase the efficiency of spectral resource management in optical transport networks. On the basis of the proposed model it is possible to solve the subproblems of search for light path routes taking into account the requirements for non-intersectivity of spectra, contiguity of elementary frequency intervals of each light path, continuity of the spectrum along the entire route.

Key words: optical transport network, lightpaths, transmission quality, spectrum allocation.

Bolshebratskiy K., Dobrythin M. Analysis of the Procedure of the Interaction of Software Funds Established at the Mail Serverage of the Electronic Account System. – PP. 138–143.

The article provides an analysis of the interaction of software installed on the mail servers of the e-mail system. The study is aimed at identifying and analyzing the sequence of actions and interaction of software components operating on mail servers. The results can be used to increase the efficiency of mail systems by ensuring their security by analyzing the possibility of interaction between programs and their vulnerabilities.

Key words: Email, interprocess interaction, server.

Borganova L., Sabinin O. The Research of Migration Methods of Programs in PL/SQL from Oracle DBMS to PL/pgSQL in PostgreSQL DBMS. – PP. 144–148.

In this article, the relevance of the transition to open database management systems is justified and the issue of migration between Oracle and PostgreSQL is considered. An overview of modern solutions for converting the code of software components written in the PL/SQL procedural language used in Oracle to PL/pgSQL used in PostgreSQL is conducted, and the tasks of the preparatory stage of migration are analyzed. As a result, the algorithm of program migration between the two systems is described and the processes of converting functions, procedures, triggers and packages are considered.

Key words: database management system, relational database, Oracle, PostgreSQL, migration of software components, migration of PL/SQL, PL/pgSQL.

Boyashova E., Melnikov M., Sheremet D. Using Visual Aids as a Tool to Ensure Understanding of the Data Presented Using Infographics. – PP. 149–152.

The work touches upon aspects related to distortions in the perception of information, as well as the objectivity of visualization. The factors influencing the effectiveness of the perception of the presented information, as well as the extraction of only those data that are useful from the information flow, are considered. At the same time, the data should be transformed into consistent conclusions that contribute to productive communication. In addition, the paper pays

attention to the mistakes made in the design of infographics, as well as offers recommendations for its creation.

Key words: infographics, visual aids, information perception, communication, information, data, data representation.

Bykov D., Klimov A., Romashkin K. Analysis of Cryptographic Data Encryption Algorithms. – PP. 153–156.

The article analyzes asymmetric data encryption algorithms (Rivest-Shamir-Adleman, Digital Signature Algorithm, ElGamal algorithm and Elliptic Curve Digital Signature Algorithm). The assessment was carried out taking into account the level of security, speed of encryption and decryption, as well as ease of implementation. In addition, the key sizes of each algorithm and their corresponding analysis are discussed. The most preferred were Elliptic Curve Digital Signature Algorithm and Rivest-Shamir-Adleman.

Key words: cryptography, encryption, asymmetric methods, decryption, algorithms.

Vaganov A. Marchakov A. The Device for Protection the Electronic Equipment of the Automated Control System Based on Modern Programmable Chips. – PP. 157–162.

The article considers the device for protection the electronic equipment of ACS from the negative effects of instability of supply voltage, various pulse interference, as well as incorrect modes of its activation and operation. The relevance of the development of such a class of devices is substantiated, and the main advantages and disadvantages of similar systems and methods of automated control system protection based on modern programmable chips are considered. A block diagram of the protection system is presented and the choice of a modern element base for its implementation based on programmable discrete integrated circuits is justified. The choice of a mathematical apparatus for calculating individual blocks of the system has been made. The results of the simulation are presented.

Key words: protective device, pulse interference, microcontroller, power supply, AFR, block diagram.

Verkhova G., Kozlova E. Architecture of Software and Algorithmic Support for Processing and Visualization of Information Presented in GeoJSON Format. – PP. 163–166.

The results of developing a software architecture for performing overlay operations on objects presented in the GeoJSON format and visualizing the results are presented. As a result of the research, many basic overlay operations have been identified and algorithms that implement these operations have been identified. The application has a service-oriented architecture. The business logic is implemented as a microservice, and the visualization system is implemented as a microfrontend. A distinctive feature of the proposed architecture is the ability to deeply integrate the software into any geoinformation applications with a microservice architecture.

Key words: overlay operations, vector and raster models, microservice architecture, methods for performing overlay operations, GeoJSON.

Verkhova G., Letuchy V. Current State and Prospects for the Development of Digital Twins of Spatially Distributed Cyber-Physical Production Systems. – PP. 167–169.

The results of research in the field of formation of spatially distributed cyber-physical production systems based on digital twins are presented. The key differences between digital twins of spatially distributed objects and traditional digital twins of production equipment, which do

not take into account geoinformation aspects, are analyzed. Possible scenarios for the development of digital twins of spatially distributed cyber-physical production systems and their role in the formation of a unified geoinformation cyber environment are considered.

Key words: digital double, structure, analysis, logical and mathematical description, cyber-physical system, system.

Verkhova G., Permiakov A. Methods for Forming Allowable Zones for Location of Technical Objects on a Digital Terrain Model. – PP. 170–173.

The task of optimizing the placement of technical objects on the terrain using a search algorithm requires a formalized definition of permissible placement zones. These zones are determined by the type and parameters of the terrain, the presence of necessary infrastructure, and engineering communications. Modern geoinformation systems allow solving placement problems interactively, but utilizing search algorithms for these purposes in such systems is challenging because most of them lack advanced tools to automate this process. The article presents the results of research on methods for forming permissible placement zones of technical objects on digital terrain models and their implementation in modern geoinformation systems, as well as proposes an approach to forming such zones.

Key words: placement zones, GIS, technical object, digital terrain model, optimization of spatial object placement.

Verkhova G., Popov I. Software and Algorithmic Support for Managing Spatial Relationships Between Geographic Objects Based on Temporal Graphs. – PP. 174–178.

When solving a wide class of problems using geographic information technologies, it is necessary to take into account topological relationships between spatially distributed objects, however, in modern geographic information systems, support for topological modeling is implemented at a level that is insufficient for the current state of development of information technologies. The article presents the results of the development of software and algorithmic support for managing spatial relationships between geographic objects based on temporal graphs. The software under consideration implements basic operations on temporal graphs. This type of software can be used in advanced geographic information systems based on a knowledge base.

Key words: temporal graphs, geographic information systems, topological relationships.

Verkhova G., Suetin A. Method of Information Interaction in Interoperable Cyber Environments. – PP. 179–183.

A method for implementing information interaction within a single cyber environment formed from local interoperable cyber environments is proposed. The proposed method is distinguished by the organization of information interaction using three types of agents. Models for the formation of agents for the implementation of information interaction between local cyber environments are presented. Examples of possible implementation of the agent approach at the level of database synchronization are considered.

Key words: cyber environment, virtual organization, virtual enterprise, interoperable cyber environment.

Vladimirova E., Kryukova E. The Use of Modern Information Technologies in the Process of Training Engineering Specialists in Telecommunications Universities. – PP. 184–189.

The article talks about the rapid development, active implementation and use of modern information technologies in the process of training engineering specialists. This makes it possible to make electronic educational resources more accessible to a wide audience of users, and helps to increase the intensity and efficiency of the educational process.

Key words: electronic information educational environment of the university, electronic library, content, information technology, distance learning, availability of electronic educational resources, students, teaching staff.

Vnukov I., Filippov F. Deep Learning Tools for News Texts Classification in Intelligent Recommender Systems. – PP. 190–194.

The current state and prospects of development of intelligent recommender systems are described. Integration of deep learning models into intelligent recommender systems is actualized. Various architectures of deep learning models, including full-link feed-forward neural networks, one-dimensional convolutional neural networks, recurrent neural networks, as well as Transformer architecture, are studied in the context of their application to the classification of Russian-language news texts. A comparative analysis taking into account various hyperparameters aimed at optimizing the accuracy and performance of the models has been carried out.

Key words: artificial neural networks, deep learning, intelligent recommender systems, text classification.

Vovik A. Complex Mathematical Model of Information Security Management Process in IoT Systems. – PP. 195–201.

Solving the problem of information security management in IoT systems today is the most important condition for ensuring information security and maintaining the required level of information security in information systems. At the same time, the possibilities of information security management are limited by the absence of common numerical metrics of the main components of the process. To ensure the possibility of obtaining numerical estimation, the author developed a complex mathematical model of the process of information security management in IoT systems, combining methods of fuzzy modelling, structuring methods and methods of expert estimation.

Key words: Information security management, mathematical modelling, numerical assessment of information security, Internet of Things system.

Voloshinov D., Urvantsev G., Sharipova K. Expanding the Training Dataset Using Synthetic Data in Image Generation Models Finetuning. – PP. 202–206.

The paper researches potential of expanding the training dataset with synthetic data in image generation models finetuning. The methods of synthetic data generation are described and the efficiency of their use is studied. The analysis of experimental results is given, practical approaches to their integration are proposed, and prospects for further research in the image generation models finetuning are suggested.

Key words: modern technologies, neural networks, machine learning, image generation, Stable Diffusion, graphic content, finetuning algorithms, LoRA, ethnic diversity.

Volynkin P. Algorithmic and Software Solutions for Forecasting Areas of Flooding. – PP. 207–210.

In the era of activation of both natural and man-made crises, the task of forecasting areas of flooding is becoming particularly relevant. In this regard, the task of machine modeling of the flooding process is set, taking into account many factors. The article discusses algorithmic and software solutions for forecasting areas of flooding, taking into account the terrain features.

Key words: flooding, relief, modeling, forecasting.

Volynkin P., Gilmanova M., Analysis of Changes in Video Container Parameters after Embedding a Video Messages. – PP. 210–214.

In the era of active development of information technology, the transmission and viewing of data in video format is becoming one of the most common types of traffic. This makes them a convenient option to use as a container for stegocommunication. It is impossible to completely hide the presence of an embedded message, but it is possible to minimize its visibility. This is achieved by minimizing file size changes. The Masker 7.5 program was used to automate the implementation of the stegocommunication in the video container, and the results of the implementation for various file formats are also presented.

Key words: steganography, video, container, *.avi, *.mov, *.mpg.

Volynkin P., Kirsanova V. Comparative Analysis and Selection of Microcontrollers for the Implementation of Automatic Altitude Control Software for UAVs. – PP. 214–218.

The paper "Comparative analysis and selection of microcontrollers for the implementation of automatic altitude control software for UAVs" is a study of different types of microcontrollers, focusing on the selection of the optimal one for the development of automatic altitude control software for unmanned aerial vehicles (UAVs). The paper analyzes several types of microcontrollers including their specifications, performance and power consumption. The comparative analysis revealed the main advantages and disadvantages of each type of microcontroller in the context of automatic UAV flight altitude control. Based on the data obtained, a reasonable choice of the microcontroller that best meets the requirements for the development of automatic altitude control software is made.

Key words: microcontroller, comparison, programming, UAV.

Volynkin P., Tumanov I. Design of a System for Automated Loading of Tiles. – PP. 219–222.

The article is devoted to the design of a system of automated loading of tiles intended for updating electronic maps. The development is emphasized on the creation of a convenient mechanism for updating tiles, which is essential for ensuring the relevance and accuracy of geospatial data. The study also provides a comparative analysis of existing similar systems, identifying their strengths and weaknesses. The advantages of the developed system over other solutions are described, providing a rationale for selecting specific solutions.

Key words: automated loading of tiles, electronic maps, geographical data.

Volynkin P., Chinyaev V. The Algorithm for Predicting the Oil Spill Zone. – PP. 223–225.

This research aims to develop an algorithm for constructing oil contamination zones on the ground based on a theoretical approach. The algorithm takes into account various factors such as terrain topography, hydrological conditions, and oil spill characteristics to accurately predict the spreading of oil and identify areas at risk of contamination. The proposed algorithm

has the potential to improve response strategies for oil spills and enhance environmental monitoring and disaster management efforts.

Key words: Oil contamination, Algorithm, Theoretical approach.

Volynkin P., Shumilova A. Algorithm for Constructing Visibility Zones for Landscapes with Complex Terrain. – PP. 225–230.

The construction of visibility zones for landscapes with complex terrain is necessary for various geographic information systems, urban planning, environmental monitoring and other areas. The algorithms reviewed in this work take into account different types of source data. Each of the algorithms has its own advantages and disadvantages. Depending on these factors and the expected result, the necessary method for constructing visibility zones is selected. As a result of the work of some algorithms, the resulting visibility zones are presented.

Key words: visibility area, visibility area construction, floating horizon algorithm, Z-buffer algorithm, triangulation, double iteration.

Gaibaliev E., Filippov F. Development of a System for Searching Music by Rhythm. – PP. 231–234.

The relevance of the development and development of a system for searching music by rhythm is presented. The functional requirements for a search music system are highlighted. The range of technologies for system development has been determined. A method for automatically detecting and extracting rhythmic structure in a musical composition is described. An algorithm for its implementation and application is proposed. The choice of the type of neural network for implementing music search by rhythm is justified. The principle of training a neural network to solve the problem is considered.

Key words: information system development, music recognition by rhythm, music search.

Gvozdkov I., Likar A., Povedaiko M. Dark Cool is an Alternative Hacking Tool. – PP. 235–238.

The constant expansion of the list of software for the pentest greatly simplifies the life of attackers. There are no guarantees that the specified software will be used only for good purposes, as a result, there is a need for constant monitoring of this kind of software and familiarization with it.

Key words: protection; access to information; countering hacking of information systems.

Gorbachev P., Kopylov S., Tabunshchikova M. An Approach to Marking Electronic Documents Displayed on a Monitor Screen by Applying an Invisible Marker. – PP. 239–242.

High speed of information processing, convenient storage and management of data, the ability to model and analyze, multitasking of modern computers - all this determines the rapid development and spread of computer technology, automation of work with data. But in addition to all the advantages of using information technology, there is also a main disadvantage in the form of data leakage. To protect against this, various methods and means are being developed. This article presents an approach to screen marking the image displayed on the monitor screen in order to prevent data leakage caused by photographing the screen or taking a screenshot and then sending the generated image outside the controlled perimeter.

Key words: information leakage, marking of the image displayed on the monitor screen.

Gromov V. Forgotten and Unappreciated Programming Languages in Educational Process as Basis for Programming in Educational Process. – PP. 243–247.

The paper discusses the methodology of teaching students using virtual machine systems in the performance of academic tasks in the discipline "Architecture of Information Systems" at the St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruевич. The given methodology is based on the long-term experience of formation and operation of the Federal information system of the State Automobile Inspectorate from 1996 to 2013. It analyses the prospects of forming the skills of creating information systems for students in the conditions of modern development of computer technology.

Key words: Virtual machine systems, software systems, operating systems.

Gromov V. Student Presence Accounting Programme as Basis for Changing Behavioural Algorithms in Information Systems. – PP. 248–252.

The report examines the program for recording the presence of students in classes as a basis for changing the behavioral algorithms of teachers and students during lectures, practical and laboratory classes. The prospects for introducing a trial operation of a program for recording the presence of students for modern information systems in the conditions of import substitution and a shortage of information capacity are analyzed.

Key words: Virtual machine systems, software systems, operating systems.

Gruzdev A., Krakhmalev D., Pavlovich A. Development of the Architecture and Structure of Data Storage Using Fuzzy Dates of Historical Artifacts. – PP. 253–257.

In the world of architecture and history, there is an important task – the search and identification of artifacts, taking into account different levels of accuracy of the dates of their creation. The article provides an analysis of the choice of architecture for the implementation of a software component that allows solving the task. The concept of "pure architecture" and its components are considered. The variants of database management systems and storage structures are analyzed based on a clear and fuzzy dating format in the system. The influence of the selected solutions on the scalability and efficiency of the system is described.

Key words: fuzzy logic, clean architecture, database, membership function, system scalability, relational and non-relational storage.

Gubin A., Litvinov V., Filippov F. Simulation model of the Process of Atmospheric Air Pollution for Monitoring the Ecological Situation. – PP. 258–262.

A method is proposed for monitoring the environmental situation in the urban environment by using a simulation model of the process of air pollution, which takes into account a number of factors that have a negative impact on the environment. A mathematical formalization of the model of the process of atmospheric air pollution has been carried out. To create a simulation model, the AnyLogic modeling environment was used, which supports system dynamics methods. A number of experiments were carried out varying the parameters of the input data, which made it possible to make predictions about the factors that have the greatest impact on the environmental situation in the city.

Key words: simulation modeling, system dynamics, environmental monitoring, AnyLogic.

Gubin A., Litvinov V., Filippov F. Gradient Learning Methods of Parametrized Quantum Circuits. – PP. 262–267.

Training models based on quantum circuits using gradient methods are researched. The features of using analytical gradients to optimize the parameters of a variational scheme are considered. The influence of model sensitivity on the choice of metric when calculating gradients is shown. A comparison is made of a simple stochastic approximation of simultaneous perturbations with a natural gradient based on quantum Fisher information. The costs of implementing various approaches are estimated depending on the number of model parameters and the learning rate.

Key words: machine learning, gradients, parameterized quantum circuits, parameter optimization.

Gubin A., Litvinov V., Mikhailova E., Filippov F. Assessment of Students' Training Level Based on Test Results, Taking Into Account their Psychophysiological State. – PP. 268–273.

The paper analyses aspects of assessing the level of students' training using testing, taking into account both the quality of test tasks and psychophysiological factors affecting students' abilities. Mathematical models are considered and a methodology of assessment formation is proposed, taking into account both the complexity of tasks and physiological parameters of students. The presented method allows for a more accurate assessment of students' level of training and can be used to optimise the prediction of student's grade during testing.

Key words: training level assessment, mathematical models of testing, Rasch model, Birnbaum model, psychophysiological factors.

Dorofeev I., Lyubimov A. Modeling of a Flexible Production Module Based on a Colored Petri Net. – PP. 274–279.

The article discusses a flexible production module, including a storage device, an industrial robot and technological machine tools. The flexible production module is controlled from a local control system. The control system, in general, may include a numerical control system for technological equipment and an industrial robot control system. Modeling by the module is performed using a colored Petri net, which takes into account the flexibility of processing products with different technological characteristics within a single technological process. The developed model of a colored Petri net allows us to describe the structure of the control program of a flexible production module.

Key words: flexible production module, local control system, colored Petri net.

Evseev D., Lyubimov A., Chebykin N. Application of Web Technologies in Distributed Control and Management Systems of Technological Objects. – PP. 280–284.

The paper considers approaches and solutions for the development of distributed control and management systems for technological processes and objects based on SCADA systems and technologies of the industrial Internet of Things. The use of user applications using mobile telecommunications and web browsers based on web-oriented SCADA systems, as well as the full-duplex WebSocket protocol for managing technological processes and objects in real time are shown as promising areas for organizing remote access in control and management systems.

Key words: distributed control and management system, web technologies, WebSocket protocol, WebScada system.

Zharanova A., Kotlova M., Nerman K. Modeling a Task Planner for Parents and Children with a Reward System. – PP. 285–290.

The development of a task planner for parents and children with a reward system is updated. On the basis of the analysis of existing services the requirements to the developed information system are allocated. The model of the information system of the task scheduler for parents and children with reward system is formed, the key elements of the model are described. The main functional capabilities of the system are presented in the use case diagram. The life cycle of the task including the processes of execution, checking and scoring is described. An algorithm for recommending tasks based on the child's completed tasks is proposed.

Key words: digital platform, modeling, child motivation, financial education, parenting, time management, schedule organization.

Zharanova A., Slezak G. Development of an Algorithm for Automated Construction of Local Computer Networks Models for Procedural Virtual Spaces Generation System. – PP. 291–296.

The urgency of creation and application of the algorithm of automated construction of local area network models for systems of procedural generation of virtual spaces is substantiated. The requirements to the data structure of the algorithm for compatibility with the final information system are described. The structure of the algorithm and its data is formed and described. The linguistic and software were selected taking into account the purposes of using the designed algorithm. The realization of the algorithm using the selected software is performed. Possibilities of extension of the algorithm and its adaptation for different end information systems are presented.

Key words: local networks, procedural generation, simulation, game engine, algorithm, simulator.

Zhenihov E., Pekarskaya O. Intelligent Information Systems: Main Characteristics, Application and Prospects of Development in Knowledge Management. – PP. 297–303.

The article is devoted to the description of intelligent information systems, their characteristics, classification, application, and role in knowledge management. The methodology of data mining using intelligent information systems is presented. It was noted that today in our country it is especially important to create the necessary conditions for the development and implementation of artificial intelligence technologies, primarily in order to improve the quality of life of the population, strengthen national security, develop various sectors of the economy, health, culture, and education.

Key words: intelligent information systems, data mining, knowledge management, operational analytical data processing, logical and mathematical system.

Zadboev V., Lipatnikov V., Nefedov V. A Way to Improve the Integrity of Files of Information Resources of the Data Transmission Network under Attack Conditions. – PP. 304–307.

Modern computer technologies, which are constantly progressing in their development, make various tasks in the field of cybersecurity relevant. Developing the most effective way to protect files is currently becoming one of the important tasks of most developers.

Key words: executable files, information attachment, integrity assurance, data transmission network.

Zadboev V., Rogovoy N., Shevchenko A. Analysis of the Capabilities of Domestic Tools Used to Monitor Information Security of Data Transmission Networks. – PP. 308–313.

The article is devoted to the study of technologies and tools developed in Russia, designed to ensure information security in data networks. The work analyzes existing monitoring tools, identifying their main characteristics, advantages and disadvantages. Particular attention is paid to their applicability in the context of protection against modern threats and attacks such as cyberattacks and data leaks.

Key words: Information security, data networks, monitoring, SIEM systems, incidents.

Zolotov O., Matiukhina T., Olefirenko M., Sotenko S. Correction of Systems of Automatic Control and Modelling. – PP. 314–317.

In the theory of linear automatic control systems, the method of synthesis of correcting devices on logarithmic frequency responses became widespread, however when modeling more convenient is a work with transfer functions of a system. Transition to transfer functions allows to apply more flexibly different methods of optimization of structure of the projected system. Article is devoted to justification, development and combination of these approaches in a uniform technique.

Key words: systems of automatic control, frequency characteristics, transfer functions of system.

Zolotov O., Matyukhina T., Rakovskii O. On the Role of Artificial Intelligence in Decision-Making Systems, in Relation to the Management of Structures with Feedback. – PP. 318–321.

Classical automatic feedback control systems can be applied in many fields. At the same time, they can be combined with the use of artificial intelligence. However, the place of artificial intelligence in feedback systems has not yet been determined. We can consider this issue using the example of decision-making in the medical field, where there is a large amount of verbal information, and fuzzy decision boundaries lead to the use of fuzzy logic mechanisms.

Key words: Treatment methods, management theory, feedback principle, neural network, expert system.

Izmaylov N., Iskulov E., Kurdubova V. The Study of the Stability Of Solutions of Linear Systems Based on Operational Calculus. – PP. 322–325.

This paper examines such applications of the theory of functions of a complex variable as operational calculus and stability theory. Operational calculus is a powerful tool for analyzing and designing control systems, and stability theory allows you to assess the stability of dynamic systems and predict their behavior in various conditions. The use of operational calculus methods has made it possible to solve problems related to the study of the stability of solutions of linear differential equations. For some well-known analytical stability criteria, console applications have been written in the C language.

Key words: Operational calculus, stability theory, C++.

Ilyina I., Klimov A., Shelekhov V. Using Technology to Fight with Fake News. – PP. 326–329.

In the modern world, the spread of fake news has become a serious problem, undermining trust in the media, people and even states, distorting public discourse and even influencing elections and other important public and political activities. Recognizing the need to address this prob-

lem, technological innovations are increasingly being used to combat the spread of disinformation. This article examines various technological solutions and their potential to mitigate the impact of fake news in a digital society.

Key words: Fake, Mass information, blockchain, AI, artificial intelligence, data, news.

Ilna O., Kupchinenko O., Skoropad A. About Mandatory Access Control. – PP. 330–334.

The implementation of the mandatory access control model in new versions of special purpose operating system Astra Linux SE is considered. The use of special attributes of mandatory access control - labels are analyzed. For the main directories in operating systems of special purpose Astra Linux SE, examples of settings for mandatory attributes, levels and categories are presented.

Key words: operating system of a special purpose, information security, access rights, mandatory access control model, level, category, labels.

Ilna O., Kupchinenko O., Skoropad A. Network Protected File System. – PP. 335–339.

The composition of a network protected file system, its main tasks and basic capabilities, as well as the presentation and tasks of a protected file server and a client of a network protected file system, features of configuring a file server and access to a shared network resource are considered. The analysis of the capabilities of a secure file server is carried out and its advantages over other file servers are formulated.

Key words: network protected file system, shared network resources, file storage, network resource mounting, secure file server.

Ilna O., Kupchinenko O., Skoropad A. Web Applications in a Secured Operating System. – PP. 340–344.

An analysis of the differences of web in operating systems of special purpose Astra Linux SE was carried out. The composition and application of a secure complex of hypertext data processing programs are considered. A comparison of protection and user identification mechanisms has been carried out. Methods for improving the performance of web applications are presented.

Key words: operating system of a special purpose, web application, web server, mandatory access control, authentication, Kerberos protocol.

Ismailov D., Litvinov V. Increasing the Efficiency of Warehouse Management Systems (WMS) by Optimizing Goods Placement. – PP. 345–349.

The scientific article examines strategies for optimizing time and placing goods in a warehouse in conditions of labor shortage. Using neural network analysis data and a simulation model, an innovative approach is proposed aimed at increasing the efficiency of warehouse logistics and reducing labor costs, taking into account the balance between placement by product groups and ABC analysis. The authors foresee practical testing of the developed methods in warehouses, with an emphasis on taking into account the cost of moving goods.

Key words: WMS, Warehouse Management System, warehouse management system, warehouse logistics.

Kalinyuk A., Konstantinov S. Comparison of SQL and NoSQL Databases. – PP. 350–356.
Modern software is often faced with the task of processing terabytes and even petabytes of data. Distributed computing is widely used to solve this problem, which imposes new requirements on the DBMS: scalability and the ability to process transactions in a distributed manner. In distributed systems based on a relational data storage model, performing transactions and pooling operations involving a large number of cluster nodes is difficult and inefficient. This has led to the growing popularity of non-relational databases, which allow for greater flexibility, better scalability and high fault tolerance. Such databases are called NoSQL.

Key words: SQL, NoSQL, DB, DBMS.

Kovalev I., Nogin S., Pantyukhin O., Pashchenko V. General Approach to Determining Computer Network Monitoring Nodes. – PP. 357–360.
Maintaining the functionality of computer networks remains an urgent problem. One of the ways to solve this problem is to monitor various network parameters. The choice of appropriate parameters and places for their monitoring are largely determined by the purposes of monitoring.

Key words: computer networks, monitoring, monitoring node, monitoring parameters, selection of monitoring node.

Kovalev R., Saltanov A. The Problem of Using Control Systems Document-Oriented Databases. – PP. 361–364.
The paper considers the problem of the choice and application of document-oriented database management systems. This problem is a cause-and-effect relationship in the formulation of the task of developing software and algorithmic software for managing document-oriented databases used at various stages of the product lifecycle. The popularization of non-relational databases requires an in-depth study of their qualitative properties, advantages and disadvantages in the management of document-oriented databases intended for use in related fields of enterprise activity, or in the production of dual-use products.

Key words: database management system, document-oriented databases, relational databases, non-relational databases

Kozinov E., Lukyanov V., Khomutovsky S., Petrova T. Comparison of Domestic Software for Creation of Game Content with Foreign Analogues. – PP. 365–368.
In the article, the authors consider the functionality of game engines of foreign and domestic production. The article presents a comparison of the main characteristics of the most commonly used game engines in the modern GameDev industry. The authors focus on the need to develop domestic software for creating game content, since at this stage there is a lag behind foreign software in terms of functionality and ease of development. The authors conclude that despite the high threshold for entry into the domestic game engine Unigine, it has wide development functionality in the field of augmented and virtual reality, but it also requires development in other areas.

Key words: Game engine GameDev, Unreal Engine, Unity, Unigine.

Kolmakov A., Litvinov V. Development of a Prototype of a Software Module for Implementing Realistic Behavior of Virtual Agents in Unreal Engine 5 Using the Environmental Query System (EQS). – PP. 369–371.
Technologies for implementing the intelligent behavior of virtual agents in the built-in tools of Unreal Engine 5 have been investigated. The main five components have been identified: the

agent controller, the behavior tree, the senses, the environment query system (EQS) and animation editing. These technologies are used to solve the avoiding obstacles problem by agents with different values of EQS input parameters - with greater agent behavior accuracy, the load on the computing resource gradually increases, which leads to low FPS values. This suggests that solving the problem of increasing realism by increasing the number of points and decreasing the distance between environment query system (EQS) points leads to subtle results and unnecessary performance losses.

Key words: Virtual agent, spatial query, FPS, obstacle avoidance task.

Komashinskiy T., Chikalov N. Model for Monitoring the Behavior of Corporate Web Users. – PP. 372–378.

It is known that one of the main causes of danger in web applications is the generation of anomalous traffic, non-profile traffic, changes in the behavior profile of a web application or web user, untrusted frameworks and modules that are “overloaded” with unnecessary functionality, etc. All this creates an unnecessary load that makes access to the web resource difficult. This circumstance is one of those events that sooner or later corporate web applications that are not adapted to different types of load may encounter. Taking this into account, to determine the behavior profile of a web application and a web user, a structural model of a virtualized web application monitoring function is proposed.

Key words: Virtualized network functions, web application monitoring, monitoring model.

Komashinskiy T., Chikalov N. Proposals for Forming a Web Application Monitoring System Based on Virtualized Network Functions. – PP. 379–381.

The growth of web applications has made monitoring web resources a major challenge. The presence of a large number of libraries and frameworks increases the number of potential vulnerabilities in the final web application.

Modern Web Application Monitoring is a synthetic monitoring solution that continuously checks the response time, content, overall performance of web applications, security. In this paper, the authors propose a structural model of a virtualized web application monitoring function.

Key words: Virtualized network functions, web application monitoring.

Komashinskiy T., Chikalov N. Clusterization of Http-Requests Using the Method of Self-Organizing Kohonen Networks. – PP. 382–384.

The article presents an approach to solving the problem of searching for targeted computer attacks at the application level, based on self-organizing Kohonen neural networks. The purpose of the study is to increase the efficiency of detecting anomalies and attacks in web traffic. This article examined the detection of SQL injections by clustering the Kohonen network of incoming HTTP traffic requests.

Key words: Kohonen networks, HTTP request clustering, self-organizing networks

Kopylov S., Mihajlova E. About Some Aspects of Malware Static Signs. – PP. 384–389.

Malicious software remains the most significant threat to the information security of user's confidential information and personal data. A significant increase in the volume of transmitted and processed information has shown an increased number of cases of embedding and subsequent spread of malicious code into data types containing protected information. This feature makes the task of identifying the feature space characterizing malicious software embedded in various file formats a relevant research area. The work provides an the static signs overview

of malicious software, presents their description and provides the distinctive features inherent in files containing embedded malicious code.

Key words: malware, static signs.

Kopylov S., Polehin A. Functional Model of Embedding Malicious Software Containing Anti-Analysis Tools Into PDF Files. – PP. 390–394.

Ensuring information security of information systems is one of the most relevant areas of cybersecurity policy implementation. The rapid growth in the number of information security violation incidents makes the task of improving security measures a relevant research area. To solve this problem, it is necessary to evaluate not only existing security measures and their inherent shortcomings, but also the implementing computer attacks means. The paper presents a functional model for introducing malicious software containing anti-analysis tools into PDF files. The developed model takes into account the features of the malicious code embedding into the structural components of PDF files and the obfuscating transformations usage used to protect embedded malicious code from static analysis methods.

Key words: malware, PDF files, obfuscation.

Kopylov S., Capkov N. Detecting Malware in PDF Files Using Viewer Code Coverage Analysis. – PP. 395–399.

Recent years have been marked by a significant increase in the share of electronic document management in information interaction various areas. Electronic documents are an integral part of the work of many organizations, simplifying the information exchange processes and data management. At the same time, with the growing use of electronic documents, there is an increase in the number of information security violations associated with the malicious software embedding. The most common type of data containing malware is the PDF format. Due to the popularity of this format, there has been a significant increase in information security violations. To reduce the number of incidents of information security violations when working with PDF documents, it is necessary to develop new or improve existing means of detecting malicious code. A proposed detection approach could be one based on dynamic analysis of PDF document viewers. The paper describes an approach to detecting malicious software by analyzing the code coverage of a PDF document viewer.

Key words: malware detection, fuzz testing.

Kopytova E., Mavrichev V., Petrov D. Fillipov F. Ethical Issues in Artificial Intelligence. – PP. 399–402.

The development and application of artificial intelligence brings with it many ethical issues that require attention and discussion. One such challenge is the use of autonomous decision-making systems. How much can we trust artificial intelligence to make decisions? Which of these decisions could have fatal consequences for individuals or society as a whole? How to avoid the fate of James Cameron's universe? Rules, ethical principles and restrictions are the only way to ensure the safety and reliability of such systems. The article will examine issues related to the development and application of artificial intelligence, including autonomous decision-making systems, data security and privacy, as well as inequality and possible social consequences.

Key words: artificial intelligence, ethical principles, ethical regulation of artificial intelligence, copyright, license agreement.

Korovkina E., Litvinov V. Analysis of Vulnerabilities in Maritime Information Systems. – PP. 402–405.

The study provides an assessment and analysis of the primary ship-specific technologies susceptible to cyber-attacks. This research holds significance in light of the integral role maritime transportation plays in contemporary society. The precision of vessel instrumentation is paramount, as any compromise in operational systems could lead to catastrophic consequences. Thus, it is imperative to identify, anticipate, and mitigate potential threats to information security within maritime environments. Key ship systems susceptible to vulnerabilities are examined, including Bridge Navigation Systems, Cargo Systems, Propulsion and Energy Management Systems, Onboard Access Control Systems, Passenger Service Systems, Public Networks, Crew Welfare Systems, and Radio Communication and Telecommunication Systems.

Key words: pertinent to this study include cybersecurity, maritime transport, cyber-attacks, ship security, and technical safeguarding measures.

Kosenkova A., Nesterov S. The Assessment the Effect of Changing the Size of a Write-Ahead Log Segment on Database Performance in PostgreSQL. – PP. 406–410.

The paper describes the effect of changing the size of the Write-Ahead Log segment (`wal_segment_size`) on the performance of the PostgreSQL database. The Write-Ahead Log plays an important role in maintaining data consistency when a server fails. On disk, the log is stored as a sequence of files, also called segments. Configuring log parameters can help to increase database performance.

Key words: databases, PostgreSQL, Write-Ahead Log.

Kosov P., Labkovskaya R. Data Visualization in R Programming Language. – PP. 411–415.

Data visualization is an extremely valuable skill as well as a powerful tool for studying patterns, trends and relationships in data sets. Visualization is a key step in the use of Open Data, as it provides a better understanding of the problem area, extracts and transfers the basic knowledge from the data, and guides future analysis using more sophisticated methods. In order to create objective, visual and understandable visualization graphs, certain basic principles need to be taken into account, as the process can be complex. This article is devoted to the consideration of the key principles of data visualization in R programming language.

Key words: data visualization, data analysis, ChatGPT, open data, R.

Kosov P., Labkovskaya R. ChatGPT for Data Analysis. – PP. 416–421.

The article is devoted to an innovative approach to Data Analysis with ChatGPT in R language. The paper discusses various features of ChatGPT that will help to optimize data analysis processes, including data sets, statistical summary generation, visualization and Shiny interactive applications. Special attention is paid to interaction with ChatGPT through queries in R language for automation and improvement of data analysis processes.

Key words: data analysis, chatbot, ChatGPT, R, artificial intelligence, data visualization.

Krasavtseva K., Rakovsky O. Research and Analysis of the Potential for Automation of Microclimate Monitoring. – PP. 422–426.

The main aspects of the development of microclimate monitoring technologies are considered and analysed. The range of applications for such technologies and the prospects for automation

are defined. A review of the technical tools used for monitoring microclimates is conducted. The features of microclimates as an automation target are identified.

Key words: microclimate, monitoring, microclimate monitoring, analysis, instrument, sensor.

Krivko D., Markin D. Automation of Penetration Testing Based on the Results of Ranking Information about Vulnerabilities. – PP. 427–431.

The article presents the results of the development of a penetration testing automation tool, taking into account the results of ranking information about vulnerabilities. A description of the interaction of the structural elements of the automation tool with scanning tools, vulnerability registries and information about the presence of exploits is presented.

Key words: penetration testing, vulnerabilities, exploit, scanning.

Krivolapov D., Pavlovich A. The Choice of Technology and Software for Visual Quality Control Processes of Assembly Operations. – PP. 432–436.

The ways to reduce the complexity and ensure the efficiency and simplicity of the learning process for assembly operations for engineers in the field of telecommunications due to modern technologies of virtual/augmented and mixed reality based on general application tools are considered. The procedures for analyzing and selecting software tools for modeling informative models, as well as procedures for selecting and analyzing technology for their detailed display, are investigated. The results of the application of the integration option of the selected software tools are presented.

Key words: telecommunications, augmented reality, virtual reality, automation.

Krylova E.R. Organization of Automatic Management of Temporary Labor Collectives (Team-Works) within the Framework of a Virtual Enterprise Using a Rating System. – PP. 437–440.

The article deals with the problem of optimized formation of temporary labor collectives (team-works) based on virtual enterprises, and also addresses the issue of developing a rating system or an electronic reputation system within companies, and suggests a way to use the web application interface to automatically calculate the rating of a participant in the cyber environment from a legal (corporate) entity.

Key words: cyber environment, virtual enterprises, electronic reputation, smart manufacturing, temporary labor collectives, team-works, rating system.

Kuznetsova O., Kulikov D., Trubchaninov K. GIS Service for the Delivery of Micro-Greenery in the Murmansk Region. – PP. 441–445.

Recently, microgreens have gained great popularity and now it is becoming easier to purchase fresh greens. Despite the growing interest, the issue of delivering micro-greenery still remains unresolved. The way out of this situation may be the use of geoinformation systems.

Key words: geoinformation support, GIS service, micro-greenery, micro-greenery delivery.

Kuznetsova O., Popova V. Mobile Application for Visualization of Iconic Personal Sites. – PP. 446–450.

Geoinformation systems and mobile technologies have become firmly embedded in the lives of most people – their personal sphere is no exception. Visualization of iconic places on the map

using a mobile application provides the widest possibilities for constructing and preserving personal history.

Key words: geoinformation support, mobile application, visualization, personal iconic sites, personal history construction.

Kuznetsova O., Yavdoshchuk V. Geoinformation Application for the Promotion of IT Directions of Higher Education. – PP. 451–454.

The goal of any university is to provide 100% enrollment of students who meet the requirements of the university in terms of knowledge and desire to obtain relevant specialties. To achieve this, it is necessary to contact the applicant in advance, and not at the time of submitting documents, and / or only providing information about the specialties being studied. Geoinformation technologies will help to significantly facilitate interaction with potential applicants.

Key words: geoinformation support, geoinformation application, IT directions, promotion of IT directions.

Labkovskaya R., Tarasov V. A study of the Approach to the Intellectualization of Corporate Information Infrastructure Management. – PP. 455–457.

A modern organization, even a small one, cannot be imagined without a developed and diverse information infrastructure that requires operational management, maintenance and modernization. The efficiency of the organization's work and, ultimately, its profit, reputation, etc. depend on the speed and accuracy of decision-making in managing the components of a corporate information system. It is necessary to form an approach to the organization of such management - the choice of optimization criteria, means and mechanisms for its implementation.

Key words: corporate information infrastructure, software-configurable network, traffic classification, machine learning, neural networks.

Lapko A. The Study Results of Transaction Behavior at Various Isolation Levels in PostgreSQL DBMS. – PP. 458–463.

The article is devoted to the transaction behavior study at various isolation levels in the PostgreSQL DBMS. The anomalies possible in the database during parallel execution of transactions are given. Data snapshots, the behavior of SQL statements and the causes of anomalies at various levels of transaction isolation in the PostgreSQL DBMS are described in detail. Sets of SQL statements that in parallel running can lead to an access error and rollback of the last committed transaction at various isolation levels are presented.

Key words: database, parallel execution of transactions, PostgreSQL DBMS, transaction isolation level, data snapshot, SQL statement, commit and rollback of a transaction.

Lebedev D., Shiyan A. Comparative Analysis of Level Editors in Realistic UAV Simulators. – PP. 464–466.

This article provides a comparative analysis of level editors in UAV simulators. The comparison took into account the functionality for creating landscapes, the ability to customize the scenario, change weather, edit physics systems, display object hierarchy. The level editors of the simulators Liftoff, AI Drone Simulator, Velocidrone and The Drone Racing League Simulator were reviewed.

Key words: UAV, simulator, level editor, scenario editor.

Lipatnikov V., Parfirov V. A Decision Support Method for Managing A Communication Network Based on Neural Network Technology. – PP. 467–472.

A method is proposed in which a neural network, depending on the availability of resources, determines sets of actions that are evaluated for compliance with the result of their application with the specified criteria with maximum efficiency. The developed method can be used in decision support systems in the interests of ensuring the sustainable functioning of communication networks, as well as other complex organizational and technical systems operating under destructive influences.

Key words: communication network, neural network, criterion, management efficiency, management actions, decision support system, management decision, resource.

Litvinov V., El Zabayar Shevchenko N. Algorithm for Reducing Inhomogeneous Discrete Time Values of Finite Markov Chains to a Homogeneous Form. – PP. 473–477.

The problem of bringing non-uniform discrete time values in finite Markov chains to their homogeneous form has been updated. The situations in which it is necessary to apply this algorithm are described. The main stages of the algorithm formation are revealed. Software has been developed for simulation of the algorithm. Experimental studies and comparative analysis of the results of a finite Markov chain using the developed algorithm were carried out to confirm its computational correctness. The practical significance of using the developed algorithm in modeling probabilistic processes based on finite Markov chains is revealed.

Key words: finite Markov chains, discrete time, time profile, quality indicators, heterogeneity.

Lyubimov A., Lyubimov C. On the Issue of Solving the Traveling Salesman Problem In Automation and Control Systems. – PP. 478–482.

The paper shows the features of solving the applied problems of a traveling salesman by heuristic methods and algorithms in a travel form. A method of layered decomposition of an undirected weighted graph is proposed to search for a Hamiltonian cycle of minimum weight using invariant structures and a procedure for tightening edges.

Key words: the traveling salesman problem, the Hamiltonian cycle of minimum weight, heuristic methods of combinatorial optimization, invariant structures, layered graph decomposition.

Maksimova S., Musaeva T. Analysis of Current Problems in Creating Graphical User Interfaces. – PP. 483–487.

The article discusses the problems of developing graphical interfaces for websites, mobile applications and information systems that are relevant today. The problems of the complexity of providing the cognitive properties of one interface for different categories of users, the imperfection of scientific knowledge about the human brain, the availability of eye-tracking technology, and interface adaptation are considered. Conclusions are drawn about possible ways to solve the identified problems, and directions in which research is needed are identified.

Key words: user interface, graphical interface, usability, cognitive interface, adaptive interface.

Mannanov A., Shiyan P. Modern Aspects of Cyber Security and Data Protection. – PP. 488–492.

This scientific article discusses key issues in the field of cybersecurity and methods of data protection in the modern information society. The article examines modern challenges and

threats faced by organizations and individuals, and proposes methods and strategies for ensuring information security.

Key words: cybersecurity, cybersecurity system protection, information protection, information environment, symmetric encryption, program, data protection.

Matveev A., Naidenov O., Paramonov A. Overview of Vulnerabilities and Security Trends in the Internet of Things. – PP. 493–496.

This article highlights the integration of Internet of Things (IoT) devices into various business domains, which has brought unprecedented convenience and efficiency, but has also led to a myriad of security challenges. The diverse range of security vulnerabilities inherent in IoT ecosystems is examined. Factors such as weak authentication, legacy asset vulnerabilities, inconsistent security standards, and gaps between mobile networks and the cloud are explored. Famous incidents such as the Mirai botnet and the Target credit card data leak are also examined in detail. In addition, the paper describes a range of potential solutions, from strengthening physical defences to implementing strong encryption protocols and using network firewalls. The purpose of this study is to provide a comprehensive understanding of IoT security issues and suggest viable strategies to address them.

Key words: internet of things (iot), information security, security threat, iot vulnerabilities.

Matveev P., Filippov F. Development of Service for Charitable Foundations Supporting Using Ethereum Smart-Contracts. – PP. 497–500.

The relevance of developing a service to support charitable foundations using smart contracts in the Ethereum blockchain network is presented. The structure of the service for supporting charitable foundations is described. A technology stack has been defined for the development of service subsystems. An algorithm for automated fundraising on a smart contract and their transfer to the blockchain wallet of a charitable organization upon completion of fundraising is described. The development of a service interface using the Metamask blockchain wallet is described.

Key words: charity, blockchain, smart contract, development of an automated system.

Musaeva T., Ramzaev K. Mobility Module Based on Stuart Platform. – PP. 501–505.

In a dynamically developing world, a large number of products and equipment appear, the study and use of which requires special highly qualified competencies of employees. Some of them belong to sources of increased danger or are included in the list of dangerous devices for their intended purpose and functionality, which imposes special requirements for their use and training. In this regard, there is a need for a new approach using modern tools and technologies used in teaching.

The article analyzes the existing types of mobility devices based on the Stewart platform, and examines their control systems. The conclusions made will allow us to develop a high-quality and flexible control system for a domestic simulator. The expected results of the development are to improve the user experience and expand the scope of application.

Key words: Gough-Stewart platform, mobility module, six degrees of freedom, control system, simulator control tool.

Musaeva T., Titov P. Analysis of Problems and Peculiarities of Personalization of Online Education. – PP. 506–511.

The article deals with the application of the method of personalized choice of educational course in online format taking into account individual needs of a person.

The research is conducted, the Russian market and popular platforms of online education, offered tools, current trends and promising directions of development are analyzed. The main problems and proposals for their solution have been identified.

Also, the main individual and cognitive characteristics of a person are investigated to determine their influence on the effectiveness of the learning result. Based on the conclusions drawn, a method of selecting personalized online courses taking into account individual characteristics of students is proposed.

Key words: online education, course selection, individual characteristics, personalization of education, course aggregators.

Novikov E. Group Control Problem, its Analysis and Solving Methods. – PP. 512–516.

The problem of controlling group (swarm) of agents is examined. In order to describe field of the problem, problem conditions are systematized, widespread analysis methods and solving approaches are examined. Specifically, the taxonomy for classifying different problem settings is provided, solutions analysis methods are described, group behavior approaches are provided.

Key words: Group control problem, swarm control, swarm robotics, multi-agent robotic system, multi-agent system.

Paskenova A. DLP System as an Incident Investigation Tool. – PP. 517–520.

Today, due to the increase in the number of cases of information leakage and violation of its integrity by employees, the topic of protection against threats in the field of information security is becoming very relevant. In addition, most enterprises and companies are moving into the category of the military-industrial complex (MIC), which makes this topic even more relevant. In addition, in order to form a high-quality regulatory framework, it is necessary to thoroughly and qualitatively form judicial practice in the field of information protection. In solving all these tasks, DLP systems are used, which, in turn, perform the role and functions of protecting information from threats, an incident investigation tool, as well as the formation of typical incidents to enable further investigation and the formation of a modified legal framework.

Key words: DLP-systems, investigation of information incidents, analysis and prospects for their development.

Pestov I., Smurov I., Fedorov P., Fedorova E. Analysis of Methods for Detecting Anomalies and Attacks in Cloud Infrastructures. – PP. 521–526.

Cloud infrastructures are becoming more popular and more important for various companies and organizations. However, with the increasing use of the cloud, the number of potential security threats, such as anomalies and attacks on information systems, also increases.

Analyzing methods for detecting anomalies and attacks in cloud infrastructures is critical to ensuring the security of data and resources in the cloud. In this article, we will look at various approaches to detecting anomalies and attacks in the cloud, including the use of statistical methods, machine learning, behavioral analysis, log analysis, and signature analysis.

Key words: Cloud infrastructures, security threats, attacks, anomalies.

Prokofev P. Multidimensional Models of Geographical Objects. – PP. 527–530.

The general structure of georelational databases is considered. Multi-aspect models of geographical objects are presented, allowing one to describe natural and anthropogenic objects within a single multi-aspect environment. The results of this work can be used to implement software that allows solving problems of geographic information modeling, analysis, planning and management of spatially distributed objects within a geographic region.

Key words: GIS, cartography, geographical objects, databases, multi-aspect models.

Pshenichnikova D., Sabinin O. Translation of Relational Algebra Operations into SQL Commands Taking into Account Restrictions for Operations. – PP. 531–535.

This article discusses the possibility of translating relational algebra operations into SQL commands. The eight operations of relational algebra and their limitations are reviewed. A method is proposed for translating relational algebra operations into SQL. An algorithm for checking the constraint: coincidence of relationship patterns is considered.

Key words: relational algebra operations, SQL language, DBMS_SQL package.

Rakovsky O., Chuharev I. Development of a System for Analyzing Student Performance. – PP. 536–538.

The article discusses the importance of performance analysis for organizing successful student learning. There are many factors to consider that may influence student performance. For example, such factors are admission scores, form of education, class attendance, and exam results. The main goal of such analysis is to improve the quality of training and control over the progress of the educational process.

Key words: analysis, educational process, students, assessment, factors

Rakovsky O., Chuhareva E. Identification of Consumer Preferences in Order to Improve Marketing Activities. – PP. 539–541.

Analysis of consumer preferences is an important tool for improving marketing activities. It allows you to identify the most popular goods and services, determine the target audience, adapt products to consumer needs and improve the quality of service. The results of the analysis help companies develop effective marketing strategies and improve customer satisfaction.

Key words: Marketing activities, target audience, needs.

Romadova P. The Algorithm of Personalized Recommendations of Leisure Places for Tourists. – PP. 542–545.

This article describes an algorithm for recommending places of interest to tourists. To create a list of suitable places to visit, the user's preferences are considered. This is done by filtering based on content, checked by the similarity of the vectors of the description of places. The result of the algorithm is a ranked list from the most to the least suitable places for the user in accordance with his preferences.

Key words: Content-based filtering, recommendation systems, algorithm, tourism.

Ruban E, Smorodin G, Shanenko D. Analysis of the Development of CRM Systems. – PP. 546–550.

An analysis of the possibilities and prospects for the development of CRM systems in the information ecosystem of the corporation is carried out. The main advantages and disadvantages of

CRM systems are noted, taking into account the opinions of leading analysts of information systems and trends in the development of corporations. The structure of the CRM system and solutions based on artificial intelligence, which allow you to significantly optimize the behavior of the CRM system, are shown in detail.

Key words: CRM systems, Customer Relationship Management, Cloud Technology, Business Processes.

Soloviev A., Sorokin N., Tikhonov S. Application of Artificial Intelligence in Software Engineering. – PP. 551–554.

In the context of technological progress and the spread of artificial intelligence (AI), the impact of AI on software engineering is considered. It is emphasized that automation of various stages of the life cycle of a software product thanks to AI significantly reduces code development time. Emphasizes the role of machine learning in data analysis, performance optimization, and creating models to predict trends. In addition, successful examples of the use of AI in various fields such as healthcare, finance and technical support are discussed. Specific projects such as GitHub Copilot and Tesla Autopilot. Finally, it is emphasized that flexibility and adaptation of programmers to the capabilities of AI are becoming key competencies in an era of rapid technological development.

Key words: artificial intelligence, software engineering, chatbots, information technology.

Spiridonov D., Fedorchenko E. Modeling attacks based on Microsoft Kubernetes Threat Matrix. – PP. 555–557.

Today, the use of Kubernetes in the field of information technology has become widespread. This platform allows you to deploy and configure cloud infrastructure. The effect of attack detection based on the Microsoft Kubernetes Threat Matrix is at work. Attack modeling allows you to assess the vulnerability of the Kubernetes system to known attacks, as well as determine a set of defenses and minimize the damage from possible attacks.

Key words: Microsoft Kubernetes Threat Matrix, Kubernetes, Docker, Attack modeling, bas.

Strelets C., Shabanov A. The Cryptocurrencies and Blockchain: Responsibility and Potential in Digitizing Government Administration. – PP. 558–562.

The main goal of this article is to research how cryptocurrencies and blockchain could bring value for the government and help with providing public services. It explores the advantages of cryptocurrencies, including improved transparency and cost reduction, as well as the benefits of blockchain technologies, such as data reliability and enhanced identification systems. It examines the challenges that could be faced in the process of integration of these technologies into the public sector.

Key words: Digitization, government administration, blockchain, distributed ledger technologies, cryptocurrencies, digital currencies, electronic document management, electronic voting.

Trofimenkov A. Verification of Anomalies at Processing of Panoramic Images. – PP. 563–565. *Synthesis of the panoramic images generated from video shots, the pilotless flying machines received from the chamber, shows that there are distortions during algorithm work of connection initial pictures in a panorama. Procedure of an establishment of reliability of the found out anomalies can be considered as their verification.*

Key words: anomalies; fuzzy sets; detection; panoramic images; filtration, verification.

Fedorova M., Yugai O. Automated System for Accounting for Radio Electronics Element Base. – PP. 566–570.

Recently, thanks to the active development of IT technologies, the field of digital accounting and control in various areas of human activity is rapidly developing. A high degree of automation allows you to reduce working time, which serves as a significant incentive to increase labor productivity, as well as avoid a number of human errors, and as a result, maximize profits and minimize labor costs. The article discusses a specially developed web application, the functionality of which allows you to keep track of the manufacturer's availability of components for the production of radio-electronic devices.

Key words: digital accounting, automation, labor productivity, labor costs, web application.

Fedorova M., Yakovlev D. Automation System for Goods Accounting and Cargo Transportation Management. – PP. 571–576.

Recently, by digitalization, the transport logistics industry is moving away from the usual paper work and active human participation in the process of transportation management and warehouse accounting. Automated systems include specialized software and hardware to optimize distribution processes within an organization. The implementation of data systems allows you to improve communication between different departments, reduce time for operations, effectively save material resources and evaluate the effectiveness of employees. The article discusses the provided and developed software that provides functional two subsystems - transport management and warehouse accounting, as well as console interaction between them.

Key words: automation, cargo transportation, integrations, monitoring, REST.

Khamzina O. The Problem of the Relevance of Search Results in Electronic Library Resources. – PP. 577–580.

As the volume of scientific publications grows in electronic form, it becomes increasingly difficult to effectively search for up-to-date information. This article explores the problems of multi-criteria searching in scientific electronic library resources, considering the publication date as the most important criterion. The article analyzes the influence of a multi-criteria approach on the effectiveness of search results, identifies the main problems and proposes ways to solve them.

Key words: search engines, search engine analysis, multi-criteria search.

Chupakhin I., Shiyan P. Where Will Machine Learning Have the Biggest Impact? – PP. 581–586.

This article will provide a comparative analysis of the use of machine learning in various areas of our lives. Statistics on the use of machine learning based on the development of technology and the power of computing systems will be considered.

Key words: machine learning, artificial intelligence, natural language, computer system, artificial neural networks.

Аньшаков А. Е., Галиева Т. Р. RabbitMQ: принцип работы и применение в многомодульных ПО. – С. 587–591.

В статье рассматривается основной принцип работы брокера сообщений RabbitMQ. Представлены примеры практического применения RabbitMQ как средства коммуникации различных ПО и сервисов. Описывается алгоритм использования протоколов прикладного уровня для передачи сообщений между компонентами системы. Статья предназначена для разработчиков ПО и архитекторов приложений.

Ключевые слова: RabbitMQ, AMQP, типы кадров, коммуникация, автоматизация рабочих процессов.

АВТОРЫ СТАТЕЙ

- АБСАТТАРОВ
Галымжан
Нурлыбекович слушатель Военной академии связи им.
Маршала Советского Союза С.М.
Буденного,
31aldabergenovyelnur4@yandex.ru
- АБЫЛХАСЕНОВ
Марат Даутович слушатель Военной академии связи им.
Маршала Советского Союза С.М.
Буденного, (812) 247-98-31
- АВЕРЬЯНОВ
Адэль Валерьевич сотрудник Академии Федеральной Службы
охраны России, г. Орёл,
adel.averyanov@bk.ru
- АЛЬ-НАМИ
Башер Али кандидат технических наук, старший
преподаватель, кафедры информатики и
компьютерного дизайна Санкт- Петер-
бургского государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, alnomibasheer@gmail.com
- АПОСТОЛЕВСКИЙ
Дмитрий Кириллович студент группы РБМ-21 Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича,
dimaapostolevskig@gmail.com
- АРТАМОНОВ
Никита Михайлович оператор роты научной Военной академии
связи им. С. М. Буденного,
nikiwfw@gmail.com
- АХРАМЕНКО
Антон Анатольевич студент группы ИСТ620о-1 Мурманского
арктического университета,
akhramenko_2002@mail.ru
- БАЛАКИРЕВ
Дмитрий Денисович аспирант кафедры информатики и
компьютерного дизайна Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, dimurator1@yandex.ru
- БАЛЫБЕРДИН
Сергей Денисович студент группы ИСТ-011 Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, balu20031@gmail.com

- БЕСЕДИН** Максим Дмитриевич младший научный сотрудник Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, pluxar@bk.ru
- БИКБУЛАТОВ** Владислав Радионович адъюнкт НИЦ Военной академии связи им. С.М. Буденного, aleks1998-2011@mail.ru
- БИРИХ** Эрнест Владимирович старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, be1982@mail.ru
- БОКОВ** Илья Григорьевич студент группы РТ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BokovPTS@mail.ru
- БОЛЬШЕБРАТСКИЙ** Кирилл Михайлович сотрудник Академии Федеральной Службы охраны России, kirillbolhov@mail.ru
- БОНДАРЕНКО** Игорь Борисович кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, igorlitmo@rambler.ru
- БУЛОВА** Марина Дмитриевна студент группы ИКБ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marina.bulova02020@gmail.com
- БУРЛАКОВ** Андрей Анатольевич кандидат военных наук, доцент, доцент кафедры Военной академии связи им. Маршала Советского Союза С.М. Буденного, p_oleg99@mail.ru
- ВАГАНОВ** Александр Валерьевич старший преподаватель кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut_ispiu@mail.ru
- ВАСИЛЬЕВ** Никита Алексеевич старший научный сотрудник научно-исследовательского центра Военной академии связи им. С. М. Буденного, vasn2020@mail.ru

- ВЕРХОВА доктор технических наук, профессор, зав. кафедрой интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina500@inbox.ru
Галина Викторовна
- ВИТКЕВИЧ научный сотрудник научно-исследовательского центра Военной академии связи им. С. М. Буденного, vasn2020@mail.ru
Наталья Львовна
- ВОЛОШИНОВ доктор технических наук, профессор, заведующий кафедрой ИКД Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voloshinov.dv@sut.ru
Денис Вячеславович
- ВОЛЫНКИН кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, pavelas@mail.ru
Павел Александрович
- ВОЛЫНКИН кандидат технических наук, доцент кафедры Интеллектуальных Систем Автоматизированного Управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavelas@mail.ru
Павел Александрович
- Громов Владислав кандидат технических наук, доцент кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov.vladislav.vitalevich@gmail.com
Витальевич
- ДОБРЫШИН кандидат технических наук, сотрудник Академии Федеральной Службы охраны России, dobrithin@ya.ru
Михаил Михайлович
- ДОЛГОВ кандидат технических наук, сотрудник Академии Федеральной Службы охраны России, г. Орёл, adel.averyanov@bk.ru
Евгений Петрович
- ДОРОФЕЕВ студент группы ИСТ-041 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, qwertylike@gmail.com
Иван Николаевич

- ЖАРАНОВА** ассистент кафедры информационных
Анастасия Олеговна управляющих систем Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, zharanovaan@gmail.com
- ЗАДБОЕВ** младший научны сотрудник Военной
Вадим Александрович орденов Жукова и Ленина Краснознаменной
академии связи имени Маршала Советского
Союза С. М. Буденного, zadboev89@mail.ru
- ЗОЛОТОВ** кандидат технических наук, профессор,
Олег Иванович доцент кафедры информационных
управляющих систем Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, ius@sut.ru
- ИЛЬИНА** кандидат географических наук, доцент,
Ольга Борисовна старший преподаватель кафедры
автоматизированных систем специального
назначения Военной академии связи имени
Маршала Советского Союза С.М.
Буденного, nastik94@yandex.ru
- КАЗАНЦЕВ** старший преподаватель Санкт-
Алексей Анатольевич Петербургского государственного универ-
ситета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, kazancev.aleksey@sut.ru
- КЛИМОВ** аспирант кафедры информатики и
Алексей компьютерного дизайна Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, kaa696@gmail.com
- КОЗИНОВ** оператор научной роты Военной академии
Егор Вячеславович связи им. С. М. Буденного,
vasn2020@mail.ru
- КОЗЛОВА** студент группы ИСТ-042 Санкт-
Екатерина Олеговна Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, galina500@inbox.ru
- КОЛМАКОВ** студент группы ИСТ-311м Санкт-
Антон Евгеньевич Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
a.e.kolmakov.docs@gmail.com

- КОМАШИНСКИЙ Тихон Владимирович аспирант, Акционерное общество «Научно-производственное предприятие «РАДАР ММС», г. Санкт-Петербург, tikhoma@ya.ru
- КОПЫЛОВ Сергей Александрович кандидат технических наук, сотрудник Федерального государственного казённого военного образовательного учреждения высшего образования «Академия Федеральной службы охраны Российской Федерации», gremlin.kop@mail.ru
- КОПЫТОВА Елена Вячеславовна студент группы ИСМ-21з Санкт-Петербургского государственного университета, el.kop16@gmail.com
- КОРОВКИНА Екатерина Викторовна магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mitchenkova0112@mail.ru
- КОСЕНКОВА Анна Алексеевна студентка группы 5130902/00202 Санкт-Петербургского политехнического университета Петра Великого, kosenkova2.aa@edu.spbstu.ru
- КОСОВ Павел Валерьевич старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosov_pavel@bk.ru
- КОТЛОВА Мария Владимировна старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkotlova@gmail.com
- КРАСАВЦЕВА Ксения Алексеевна студентка группы ИСТ-212м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasavtseva.ks@yandex.ru
- КРИВОЛАПОВ Даниил Антонович студент магистратуры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkrivola@ya.ru

- КРЫЛОВА Элеонора Ринатовна аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leonora.davletshina@mail.ru
- КУЗНЕЦОВА Ольга Борисовна кандидат экономических наук, доцент кафедры информационных технологий Мурманского арктического университета, kuznetsovaob@mstu.edu.ru
- КУЛИКОВ Денис Вадимович студент группы ИСТ620о-1 Мурманского арктического университета, kulikovdv@mauniver.ru
- КУПЧИНЕНКО Ольга Павловна преподаватель кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, k-olga102@yandex.ru
- КУСТОВ Александр Сергеевич старший оператор роты научной Военной академии связи им. С. М. Буденного, 4lexkustov@gmail.com
- ЛАБКОВСКАЯ Римма Яновна кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rimma.labkovskaya@gmail.com
- ЛАПКО Александр Николаевич кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, lan46@mail.ru
- ЛЕТУЧИЙ Василий Алексеевич аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, letuchiy.vasya@gmail.com
- ЛИПАТНИКОВ Валерий Алексеевич доктор технических наук, профессор, старший научный сотрудник Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

- ЛИТВИНОВ кандидат технических наук, доцент кафедры
Владислав Леонидович Информационных Управляющих Систем
(ИУС) Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vlad.litvinov61@gmail.com
- ЛУКЪЯНОВ доктор физико-математических наук,
Валерий Дмитриевич профессор кафедры сенсорики Санкт-
Петербургского национального
исследовательского университета
информационных технологий, механики и
оптики, vasn2020@mail.ru
- ЛЮБИМОВ кандидат технических наук, доцент кафедры
Александр Геннадьевич интеллектуальных систем автоматизации и
управления Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
a.g.lyubimov@yandex.ru
- МАВРИЧЕВ студент группы ИСМ-21з Санкт-
Вячеслав Петербургского государственного
Константинович университета, mavrichevsk@gmail.com
- МАННАНОВ студент группы ИКТР-22 Санкт-
Артём Александрович Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
falfef13372017@gmail.com
- МАРЧАКОВ студент группы ИСТ-041 Санкт-
Артём Сергеевич Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
artem.marchakov@bk.ru
- МАТВЕЕВ студент группы ИКТИ-35м Санкт-
Артём Сергеевич Петербургского государственного
университета телекоммуникаций им. проф.
М.А. Бонч-Бруевича,
artemmatveev2001@gmail.com
- МАТВЕЕВ студент группы ИСТ-013 Санкт-
Павел Вадимович Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
pamat2002@mail.ru

- МАТЮХИНА** Татьяна Владимировна кандидат технических наук, доцент, заместитель декана факультета радиотехнологий связи по учебной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tatjanavm@mail.ru
- МЕЛЕХОВ** Кирилл Витальевич адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, kirill_melehov@br.ru
- МЕШКОВ** Алексей Сергеевич оператор научной роты Военной академии связи им. С. М. Буденного, vasn2020@mail.ru
- МИНЯЕВ** Андрей Анатольевич кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev1.aa@sut.ru
- МИХАЙЛОВА** Екатерина Вадимовна сотрудник Федерального государственного казённого военного образовательного учреждения высшего образования «Академия Федеральной службы охраны Российской Федерации», s.kop@acdem.msk.rsnet.ru
- МУСАЕВА** Татьяна Вагиф кызы кандидат технических наук, доцент, доцент кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru
- НАЙДЕНОВ** Олег Андреевич студент группы М4105 Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, oleg.naydenovic@gmail.com
- НЕРМАН** Кристина Александровна студент группы ИСТ-012 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nerman.c@yandex.ru
- НЕСТЕРОВ** Сергей Александрович кандидат технических наук, доцент высшей школы Компьютерных технологий и информационных систем Санкт-Петербургского политехнического университета Петра Великого, nesterov@spbstu.ru

- НЕФЕДОВ старший оператор роты научной Военной
Виталий Владимирович академии связи им. Маршала Советского
Союза С. М. Буденного,
vit02.08.19992@mail.ru
- ПАВЛОВИЧ кандидат технических наук, доцент кафедры
Артур Александрович ИСАУ Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, fathertal@mail.ru
- ПАРАМОНОВ доктор технических наук, доцент, профессор
Александр Иванович кафедры СС и ПД систем Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, paramonov@sut.ru
- ПАРФИРОВ кандидат технических наук, докторант
Виталий Военной орденов Жукова и Ленина
Александрович Краснознаменной академии связи имени
Маршала Советского Союза
С.М. Буденного, vitaly.parfirov@yandex.ru
- ПЕСТОВ кандидат технических наук, Доцент кафедры
Игорь Евгеньевич защищенных систем связи Санкт-
Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича, ip@sut.ru
- ПЕТРОВ студент группы ИСМ-21з Санкт-
Дмитрий Валерьевич Петербургского государственного
университета, snowmandexter@gmail.com
- ПЕТРОВА научный сотрудник научно-
Татьяна Владимировна исследовательского центра Военной
академии связи им. Маршала Советского
Союза С. М. Буденного, vasn2020@mail.ru
- ПОЛЕХИН сотрудник Федерального государственного
Александр казённого военного образовательного
Александрович учреждения высшего образования
«Академия Федеральной службы охраны
Российской Федерации»,
s.kop@acdem.msk.rnet.ru
- ПОЛИЩУК младший научны сотрудник Военной
Владимир Романович орденов Жукова и Ленина Краснознаменной
академии связи имени Маршала Советского
Союза С. М. Буденного, waferfly@gmail.com

- ПОПОВА Валентина Юрьевна студент группы ИСТ620о-1 Мурманского арктического университета, popova.valyapopova2020@yandex.ru
- РАКОВСКИЙ Олег Владимирович кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rakovskyo@mail.ru
- РОГОВОЙ Николай Александрович старший оператор научного взвода научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, kolyanike32@gmail.com
- СЕЛИНА Валерия Васильевна студент группы ИКТ-38 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lerawarnins@mail.ru
- СКОРОПАД Александр Витальевич ведущий инженер Санкт-Петербургского филиала «ЛОНИИР», sav01236@yandex.ru
- СЛЕЗАК Герман Дмитриевич студент группы ИСТ-011 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slezakgerman@gmail.com
- СМУРОВ Илья Александрович студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ismurov@mail.ru
- ТАРАСОВ Владимир Анатольевич старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-liquidator@bk.ru
- ТИТОВ Павел Александрович студент 2 курса магистратуры группы ИСТ-231м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wowpointblog@gmail.com
- ТКАЧЕВ Дмитрий Федорович кандидат технических наук, начальник отдела НИЦ военной академии связи, aleks1998-2011@mail.ru

- ТРУБЧАНИНОВ Константин Андреевич студент группы ИСТ620о-1 Мурманского арктического университета, konstantintrubchaninov@yandex.ru
- ТУМАНОВ Иван Александрович студент группы ИСТ-051 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivan.tumanov.1999@mail.ru
- УРВАНЦЕВ Георгий Александрович студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minehaka@yandex.ru
- ФЕДОРОВ Павел Олегович аспирант группы 236А-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavel_lenin@mail.ru
- ФЕДОРОВА Екатерина Сергеевна студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ek.chukina@yandex.ru
- ФЁДОРОВА Мария Владимировна кандидат экономических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tale19quale@mail.ru
- ФИЛИППОВ Феликс Васильевич кандидат технических наук, старший научный сотрудник, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru
- ХОМУТОВСКИЙ Сергей Львович младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru
- ЧИКАЛОВ Никита Вячеславович старший инженер программист, Акционерное общество «Научно-исследовательский институт «Рубин», г. Санкт-Петербург, N.V.Chikalov@rubin-spb.ru

- ЧИНЯЕВ Вадим Андреевич студент группы ИСТ-042 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vadya.2002.2016@gmail.com
- ЧУХАРЕВА Екатерина Николаевна студентка группы ИСТ-311м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chuharevaen@yandex.ru
- ШАКЕРБЕКОВ Даурен Мухтарханович слушатель Военной академии связи им. Маршала Советского Союза С. М. Буденного, (812) 247-98-31
- ШАРИПОВА Камила Тимуровна студент группы ИКВТ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kalinamila03@yandex.ru
- ШЕВЧЕНКО Александр Александрович старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, кандидат технических наук, alex_pavel1991@mail.ru
- ШИЯН Павел Анатольевич старший преподаватель, кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shiyen.pa@sut.ru
- ШУМИЛОВА Анна Алексеевна студент группы ИСТ-042 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minsuchong55@gmail.com
- ЮГАЙ Олег Константинович студент группы ИСТ-141 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ugay03@gmail.com
- ЯВДОЩУК Валерия Владимировна студент группы ИСТ620о-1 Мурманского арктического университета, valeriyavd@gmail.com
- ЯКОВЛЕВ Данила Владимирович студент группы ИСТ-052 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dwhytt23@yandex.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

- Абсаттаров Г. Н. 5
Абылхасенов М. Д. 5
Аверьянов А. В. 10
Авраменко В. С. 16
Агафонов Н. Р. 20
Агеносов Д. А. 25
Аль-Нами Б. А. 28, 32, 37, 41, 45, 50, 53, 58
Апостолевский Д. К. 64
Артамонов Н. М. 68, 73
Ахраменко А. А. 79
Бабаева Э. Э. 28
Байсарин В. И. 25
Балакирев Д. Д. 84
Балыбердин С. Д. 88
Беккель Л. С. 94
Белоус К. В. 99, 104
Беляева Н. А. 32
Беседин М. Д. 108, 113
Бикбулатов В. Р. 117
Бирих Э. В. 122
Бовшик П. П. 128
Бойко А. П. 133
Боков И. Г. 37
Большебратский К. М. 138
Бондаренко И. Б. 88
Борганова Л. И. 144
Бояшова Е. П. 149
Булова М. Д. 122
Бурлаков А. А. 5
Быков Д. Б. 153
Ваганов А. В. 157
Васильев Н. А. 68
Верхова Г. В. 163
Верхова Г. В. 167, 170, 174, 179
Виткевич Н. Л. 68
Владимирова Е. С. 184
Внуков И. А. 190
Вовик А. Г. 195
Возгрин Г. В. 20
Волошинов Д. В. 202
Волынкин П. А. 20, 207, 210, 214, 219,
223, 225
Гайбалиев Э. Э. 231
Гвоздков И. В. 235
Гильманова М. К. 210
Горбач А. Ю. 99
Горбачев П. Н. 239
Громов В. В. 243, 248
Груздев А. А. 253
Губин А. Н. 258, 262, 268
Демидов А. А. 104
Добрынин М. М. 138
Долгов Е. П. 10
Дорофеев И. Н. 274
Евсеев Д. И. 280
Жаранова А. О. 88, 285, 291
Женихов Е. А. 297
Задбоев В. А. 108, 113, 304, 308
Золотов О. И. 314, 318
Измайлов Н. С. 322
Ильина И. В. 326
Ильина О. Б. 330, 335, 340
Искулов Е. Р. 322
Исмаилов Д. И. 345
Казанцев А. А. 122
Калинюк А. О. 350
Кирсанова В. Н. 214
Климов К. 64
Климов А. А. 153
Климов А. 326
Ковалев И. С. 357
Ковалёв Р. М. 361
Козинов Е. В. 365
Козлова Е. О. 163
Колмаков А. Е. 369
Комашинский Т. В. 372, 379, 382
Константинов С. А. 350
Копылов С. А. 239, 384, 390, 395

- Копытова Е. В. **399**
Коровкина Е. В. **402**
Косенкова А. А. **406**
Косов П. В. **411, 416**
Котлова М. В. **285**
Красавцева К. А. **422**
Крахмалев Д. С. **253**
Кривко Д. В. **427**
Криволапов Д. А. **432**
Крылова Э. Р. **437**
Крюкова Е. С. **184**
Кузин П. И. **133**
Кузина Е. И. **133**
Кузнецова О. Б. **79, 441, 446, 451**
Куликов Д. В. **441**
Купчиненко О. П. **330, 335, 340**
Курдубова В. В. **322**
Кустов А. С. **68**
Лабковская Р. Я. **411, 416, 455**
Лапко А. Н. **458**
Лебедев Д. В. **464**
Летучий В. А. **167**
Ликарь А. И. **235**
Липатников В. А. **73, 304, 467**
Литвинов В. Л. **128, 258, 262, 268, 345, 369, 402, 473**
Лукьянов В. Д. **365**
Любимов А. Г. **274, 280, 478**
Любимов С. А. **478**
Мавричев В. К. **399**
Максимова С. В. **483**
Маннанов А. А. **488**
Маркин Д. О. **427**
Марчаков А. С. **157**
Матвеев А. С. **493**
Матвеев П. В. **497**
Матюхина В. И. **99**
Матюхина Т. В. **314, 318**
Мелехов К. В. **73**
Мельников М. В. **149**
Мешков А. С. **117**
Миняев А. А. **122**
Михайлова Е. А. **258**
Михайлова Е. В. **384**
Мусаева Т. В. **483, 501, 506**
Найденов О. А. **493**
Нерман К. А. **285**
Нестеров С. А. **406**
Нефедов В. В. **304**
Николаев А. Д. **94**
Новиков Е. А. **512**
Ногин С. Б. **357**
Олефиренко М. Б. **314**
Павлович А. А. **253, 432**
Пантюхин О. И. **357**
Парамонов А. И. **493**
Парфиров В. А. **467**
Паскенова А. У. **517**
Пащенко В. В. **357**
Пекарская О. А. **297**
Пермяков А. А. **170**
Пестов И. Е. **521**
Петров Д. В. **399**
Петрова Т. В. **365**
Пигарева Ю. Р. **41**
Поведайко М. Д. **235**
Погодин Н. В. **25**
Полехин А. А. **390**
Полищук В. Р. **108**
Попов И. Ю. **174**
Попова В. Ю. **446**
Потапов И. А. **133**
Прокофьев П. А. **527**
Пшеничникова Д. Е. **531**
Раковский О. В. **318, 422, 536, 539**
Рамзаев К. К. **501**
Роговой Н. А. **308**
Ромадова П. О. **542**
Ромашкин К. А. **153**
Рубан Е. А. **546**
Сабинин О. Ю. **144, 531**
Садовников В. Е. **113**
Салтанов А. В. **361**
Свечников Д. А. **25**
Селина В. В. **45**
Симкин К. Е. **50**
Скоропад А. В. **330, 335, 340**
Слезак Г. Д. **291**
Сморозин Г. Н. **546**
Смуров И. А. **521**
Соловьев А. П. **551**
Сорокин Н. А. **551**
Сотенко С. М. **314**
Спиридонов Д. П. **555**
Стрелец К. М. **558**
Суетин А. Ю. **179**

- Табунщикова М. М. **239**
Тарасов В. А. **455**
Титов П. А. **506**
Тихонов С. С. **551**
Ткачев Д. Ф. **117**
Трофименков А. К. **563**
Трубчанинов К. А. **441**
Тужикова М. А. **53**
Туманов И. А. **219**
Урванцев Г. А. **202**
Усов Н. А. **133**
Федоров П. О. **521**
Федорова Е. С. **521**
Фёдорова М. В. **566, 571**
Федорченко Е. В. **555**
Филиппов Ф. В. **190, 231, 258, 262, 268,
399, 497**
Хамзина О. О. **577**
Хомутовский С. Л. **365**
Цапков Н. А. **395**
Цыганова Д. Д. **58**
Чебыкин Н. А. **280**
Чикалов Н. В. **372**
Чикалов Н. В. **379, 382**
Чиняев В. А. **223**
Чичков Е. С. **16**
Чупахин И. И. **581**
Чухарев И. А. **539**
Чухарева Е. Н. **536**
Шабанов А. П. **558**
Шакербеков Д. М. **5**
Шаненко Д. Е. **546**
Шарипова К. Т. **202**
Шевченко А. А. **308**
Шелехов В. П. **326**
Шеремет Д. Н. **149**
Шиян А. А. **464**



АПИНО
ІСАІТ

APINO.SUT.RU