

Международный журнал информационных технологий и энергоэффективности



Том 10 Номер 1(51)



2025



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	Пучков Г.Ю. К вопросу об использовании искусственного интеллекта для управления сетями профессиональной мобильной радиосвязи	5
	Puchkov G.Yu. On the issue of using artificial intelligence to manage professional mobile radio networks	
2.	Мадатов Д.А., Борисов В.В., Сивков В.С. Будущее технологии цифровых двойников	10
	Madatov D.A., Borisov V.V., Sivkov V.S. The future of digital twin technology	
3.	Сизов И.М., Сулимов А.Д. Использование LLDP в отечественных ОС на ядре LINUX	16
	Sizov I.M., Sulimov A.D. Using LLDP in domestic OS based on the LINUX kernel	
4.	Гультияев А.А. Методы обнаружения аномалий в потоковых данных высокой размерности	28
	Gulyaev A.A. Anomaly detection methods in high-dimensional streaming data	
5.	Храпов А.А. Использование ANTLR для анализа метрик холстеда в языках PYTHON и BML	36
	Khrapov A.A. Using ANTLR to analyze halsted metrics in PYTHON and BML languages	
6.	Иванова Н.А., Смоленцева Т.Е. Обзор банковского процесса по управлению проблемными проектами на платформе GREENDATA	42
	Ivanova N.A., Smolentseva T.E. Overview of the banking process for managing problematic projects on the GREEN DATA platform	
7.	Мадатов Д.А., Борисов В.В., Сивков В.С. Робототехника в медицине	45
	Madatov D.A., Borisov V.V., Sivkov V.S. Robotics in medicine	
8.	Ворожейкин Д.А. Введение адаптивного окна построения графика базовой нагрузки в расчетах по определению объема снижения электропотребления	52
	Vorozheikin D.A. Introducing of an adaptive window for building the base load schedule in calculations to determine the amount of power consumption reduction	
9.	Сергеев Д.Н. Выбор технологии асинхронной передачи данных в реальном времени при проектировании ВЕБ-мессенджеров	60
	Sergeev D.N. Selection of real-time asynchronous data communications technology in WEB messenger development	
10.	Дубиков Д.Э. Анализ пользовательских запросов на наличие сетевой атаки с использованием технологий больших данных	65

	Dubikov D.E. Analysis of user requests for the presence of network attack using big datatechnologies	
11.	Калиберда С.И. Применение PROCESS MINING для идентификации узких мест в бизнес-процессах	71
	Kaliberda S.I. Application of PROCESS MINING to identify bottle places in business processes	
12.	Бютнер С.И. Методы противодействия атаке типа «ПОДМЕНА МАРШРУТА» (BGP HIJACKING)	77
	Buetner S.I. Methods of countering a "ROUTE SUBSTITUTION" type attack (BGP HIJACKING)	
13.	Мухортов А.А., Усюкин Н.А. Модель программного интерфейса для использования в нейронном протезе конечности прямого подключения	81
	Mukhortov A.A., Usyukin N.A. A software interface model for use in a neural prosthetic limb of direct connection	
14.	Иванов Е.А., Амелютин Е.В. Разработка системы автоматической идентификации и классификации угроз безопасности в информационно-аналитической системе	97
	Ivanov E.A., Amelutin E.V. Development of a system for automatic identification and classification of security threats in an information and analytical system	
15.	Бютнер С.И. Построение сети для изоляции атакуемых сервисов: использование DMZ	108
	Buetner S.I. Building a network to isolate vulnerable services: using a DMZ	
16.	Буйтвидас А.В. Валидация структурированного контента и её роль в защите ВЕБ-приложений	112
	Buitvydas A.V. Validation of structured content and it's role in WEB application protection	
17.	Полежаева М.В., Кенжина Д.С., Аксёнова К.В., Сафонова Т.В., Мокряк А.В. Интеграция больших данных и геоинформационных систем для анализа городских экосистем	117
	Polezhaeva M.V., Kenzhina D.S., Aksenova K.V., Safonova T.V., Mokryak A.V. Integration of big data and geographic information systems for the analysis of natural ecosystems	
18.	Берников А.Д., Варфоломеева А.К., Швец П.А., Сафонова Т.В., Мокряк А.В. Как ИИ помощники меняют разработку	125
	Bernikov A.D., Varfolomeeva A.K., Shvets P.A., Safonova T.V., Mokryak A.V. How AI assistants are changing development	
19.	Полежаева М.В., Кенжина Д.С., Аксёнова К.В., Сафонова Т.В., Мокряк А.В. Применение блокчейн-технологий в управлении земельными ресурсами и кадастрами	132
	Polezhaeva M.V., Kenzhina D.S., Aksenova K.V., Safonova T.V., Mokryak A.V. Application of housing technologies in land management and cadastre	
20.	Спиридонова О.И. Аналитика данных: виды и её роль в здравоохранении	141

Spiridonova O.I. Data analytics: types and its role in healthcare		
21.	Уманский Д.М. Предсказание ошибок в производственном оборудовании используя машинное обучение	145
Umansky D.M. Predicting errors in production equipment using machine learning		
22.	Соловьев В.А., Канюков А.Р., Сапунов Д.М., Булыгин И.В. Технологии 3D-печати для изготовления печатных плат: методы, преимущества и недостатки	152
Solovyov V.A., Kanyukov A.R., Sapunov D.M., Bulygin I.V. Technologies of 3D-printing for manufacturing printed circuit boards: methods, advantages and disadvantages		
23.	Троян И.В. Защита от атак с использованием временных таблиц в базах данных	168
Troyan I.V. Protecting against attacks using temporary tables in databases		
24.	Троян И.В. Эффективные методы разбиения и изоляции метаданных для повышения безопасности	172
Troyan I.V. Effective methods for partitioning and isolating metadata to enhance security		
25.	Шмидт А.А. Исследование преимуществ использования защищенных локальных сетей передачи данных	176
Schmidt A.A. Exploring the benefits of using secure local data networks		
26.	Троян И.В. Минимизация временных файлов для предотвращения утечек данных из базы	181
Troyan I.V. Minimizing temporary files to prevent data leaks from databases		
ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ		
27.	Шульгинов П.А., Вахромов А.О., Чебаков С.А. Проблематика электропитания пассажирских вагонов	185
Shulginov P.A., Vakhromov A.O., Chebakov S.A. The problem of power supply for passenger cars		
28.	Кабиров А.Н., Мытник Д.И., Катренко А.И., Мархиль М.В. Увеличение коэффициента извлечения конденсата с помощью сайклинг-процесса на месторождениях Западной Сибири	192
Kabirov A.N., Mytnik D.I., Katrenko A.I., Markhil M.V. Increasing the condensate recovery coefficient using the cycling process in the fields of Western Siberia		
29.	Го Кэнань Изучение структуры циркония в зависимости от обработки	196
Guo Henan Studying the structure of zirconium depending on processing		
ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ		
30.	Ряпусов А.Р., Шпаньков А.В. Влияние математики на пожаротушение	203
Ryapusov A.R., Shpankov A.V. The impact of mathematics on firefighting		



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УПРАВЛЕНИЯ СЕТЯМИ ПРОФЕССИОНАЛЬНОЙ МОБИЛЬНОЙ РАДИОСВЯЗИ

Пучков Г.Ю.

ФКУ «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «СПЕЦИАЛЬНАЯ ТЕХНИКА И СВЯЗЬ» МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ, Москва, Россия, (111024, город Москва, ул. Пруд-Ключики, д.2), e-mail: pgu7@ya.ru

В статье рассматриваются вопросы использования полносвязных, рекуррентных и графовых нейросетей для обеспечения управления и безопасности сетей профессиональной мобильной радиосвязи, описываются возможности FCNN, MLP, RNN, GNN нейросетей по предсказанию уровней нагрузки на каналы радиосвязи, обеспечению сбора, обработки и проведения интеллектуального анализа данных о состоянии оборудования и восстановлению конфигурации сетей после возникновения аварийных ситуаций.

Ключевые слова: Нейросеть, искусственный интеллект, профессиональная мобильная радиосвязь, графовая модель, рекуррентная модель.

ON THE ISSUE OF USING ARTIFICIAL INTELLIGENCE TO MANAGE PROFESSIONAL MOBILE RADIO NETWORKS

Puchkov G.Yu.

FKU "RESEARCH AND PRODUCTION ASSOCIATION "SPECIAL EQUIPMENT AND COMMUNICATIONS" OF THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION, Moscow, Russia, (111024, Moscow, Prud-Klyuchiki str., 2), e-mail: pgu7@ya.ru

The article discusses the use of fully connected, recurrent and graph neural networks to ensure the management and security of professional mobile radio networks, describes the capabilities of FCNN, MLP, RNN, GNN neural networks to predict load levels on radio communication channels, to ensure the collection, processing and intelligent analysis of data on the condition of equipment and restore network configuration after emergencies.

Keywords: Neural network, artificial intelligence, professional mobile radio communication, graph model, recurrent model.

Современные сети профессиональной мобильной радиосвязи (далее – ПМР) являются важной частью инфраструктуры, обеспечивающей связь в интересах правоохранительных служб, подразделений, задействованных при проведении ликвидации последствий чрезвычайных ситуаций, предприятий транспорта и энергетики. В условиях увеличения объемов трафика, передаваемого по в сетям ПМР, и, как следствие, увеличения их масштабов и сложности, искусственный интеллект (ИИ) становится ключевым инструментом для повышения эффективности их управления и эксплуатации.

Современные сети ПМР таких стандартов (протоколов), как TETRA, DMR, APCO 25 представляют собой сложные системы с большим числом взаимосвязанных элементов, включая базовые станции, устройства пользователей, ретрансляторы и т.д.

Важное место в процессах управления сетями ПМР играют процедуры, обеспечивающие постоянный контроль критически важных параметров сети, устойчивость сети за счет прогнозирования будущих нагрузок и эффективного распределения ресурсов, быстрое выявление причин сбоев в работе сети и их оперативное устранение.

В этих условиях для оптимизации процессов управления в сетях ПМР представляется целесообразным использовать нейросети, позволяющие обрабатывать большие массивы информации при помощи технологий больших данных.

Источниками данных, необходимых для анализа состояния сети ПМР, являются сетевые устройства и клиентское оборудование (базовые станции, каналообразующая аппаратура, коммутаторы, криптомаршрутизаторы, оборудование, обеспечивающее информационную безопасность сети), абонентские радиостанции и другие устройства, генерирующие данные о состоянии сети, трафике, нагрузке и ошибках), лог-файлы и журналы событий (информация о событиях и действиях, происходящих в сети и на устройствах), пользовательские данные (информация о поведении пользователей, их активности и потреблении ресурсов).

Учитывая специфику сетей ПМР для оптимизации процессов их управления могут быть рекомендованы следующие типы нейросетей.

Полносвязные нейросети (Fully Connected Neural Networks, FCNN) или многослойные перцептроны (FCNN), являющиеся базовым типом искусственных нейронных сетей. Они состоят из нескольких слоев нейронов, где каждый нейрон в одном слое связан с каждым нейроном в следующем слое. Такая архитектура считается универсальной и позволяет решать широкий спектр задач анализа данных [1].

Применительно к ПМР данные нейросети могут быть использованы для предсказания уровня нагрузки на каналы радиосвязи, оптимального распределения ресурсов, адаптивной настройки мощности передатчиков базовых станций, динамического назначения номиналов радиочастот в зависимости от меняющейся электромагнитной обстановки.

Основными преимуществами полносвязных нейросетей является универсальность, простота архитектуры, хорошая производительность при ограниченном объеме данных, т. е. данные нейросети могут с успехом применяться в небольших по составу сетях ПМР.

Рекуррентные нейросети (Recurrent Neural Networks, RNN) представляют собой класс нейронных сетей, которые наиболее подходят для обработки последовательных данных, например, временных рядов. Их ключевая особенность — наличие внутренних циклов, позволяющих для принятия решений учитывать историю предыдущих состояний системы [2]. Способность RNN учитывать зависимости между событиями делает их весьма полезными для анализа и прогнозирования временных событий сети ПМР, что дает возможность с достаточной степенью точности прогнозировать распределение трафика по сегментам сети, вычислять вероятность возникновения перегрузок базовых станций и сетевых узлов и осуществлять адаптивное управление маршрутизацией пакетов данных в условиях быстро меняющейся нагрузки каналов связи.

Таким образом, основным преимуществом рекуррентных нейросетей является способность анализировать последовательные изменения состояния радиосети, что позволяет использовать их для прогнозирования возникновения различных аномальных явлений, приводящих к нарушению штатной работы сети ПМР. К недостаткам можно отнести трудность интерпретации результатов, полученных в результате анализа сложных нелинейных зависимостей. Это затрудняет их использование в критически важных

приложениях, где требуется объяснение принимаемых решений, например, в условиях активного вывода из строя оборудования сети путем преднамеренного внешнего воздействия.

Графовые нейронные сети (Graph Neural Networks, GNN) — это класс моделей машинного обучения, работающих с графовыми структурами данных. Они предназначены для обработки информации, представленной в виде узлов (вершин) и ребер графа, описывающих связи между ними. Узлы и ребра имеют свои весовые коэффициенты, отражающие текущее состояния процессов, происходящих в системе, моделируемой графом [3].

Основная идея GNN — это обмен информацией между узлами графа, осуществляющийся при помощи его ребер с целью обновления весовых коэффициентов узлов и ребер на основе информации, получаемой от соседних узлов. После обработки полученной информации узел обновляет значения своих весовых коэффициентов. В результате нескольких таких итераций создается глобальное представление о процессах, происходящих в системе, моделируемой графом, на основании чего осуществляется прогнозирование изменения весовых коэффициентов узлов и ребер в зависимости от тех или иных внешних воздействий на моделируемую систему.

Учитывая изложенное, представляется целесообразным использовать графовые нейронные сети для оптимизации процессов маршрутизации трафика в сетях ПМР. В данном случае в качестве узлов могут рассматриваться базовые станции, мобильные устройства, ретрансляторы, маршрутизаторы, в качестве ребер – соединяющие их каналы связи и радиоканалы.

Использование FCNN, MLP, RNN, GNN нейросетей для обеспечения автоматизации процессов управления в сетях ПМР, позволит:

- обеспечить сбор, обработку и интеллектуальный анализ данных о состоянии оборудования;
- по результатам анализа лог-файлов обнаруживать отклонения в работе оборудования и сети в целом;
- определять оптимальные сроки для проведения профилактического обслуживания;
- с учетом значений наработки на отказ оборудования прогнозировать вероятности выхода его из строя и формировать рекомендации по их замене до возникновения сбоев;
- используя данные о текущих версиях программного обеспечения, автоматически планировать и выполнять обновления программного обеспечения на сетевых устройствах;
- по результатам анализа статистических данных о различных состояниях сети, связанных с перегрузками на отдельных направлениях, выходом из строя телекоммуникационного оборудования, заранее создавать шаблоны конфигураций сети и оборудования, позволяющие оперативно менять маршруты трафика;
- в штатном режиме постоянно отслеживать все изменения конфигураций оборудования сети ПМР, сохраняя с определенной периодичностью их различные варианты, и при возникновении аномальной ситуации в работе сети оперативно осуществлять «откаты» к предыдущим конфигурациям. Это во многом облегчает работу администраторов сетей ПМР, так как обеспечивает оперативное и корректное внесение изменений в настройки большого количества устройств одновременно.

Автоматизация данного процесса при помощи нейросетевых технологий существенно снижает риск человеческой ошибки.

Использование FCNN, MLP, RNN нейросетей для обеспечения безопасности сетей ПМР имеет ряд преимуществ перед традиционными методами, а именно:

- на основе анализа исторических данных об инцидентах, возникавших ранее предсказывать возможность возникновения и тип атаки;
- за счет обучения нейросети на больших объемах данных позволяет обеспечить распознавания новых неизвестных ранее угроз;
- за счет использования методов биометрической аутентификации (распознавание лиц, отпечатков пальцев, радужной оболочки глаза и т. д.), повысить безопасность доступа к сетевым ресурсам;
- по результатам анализа необычного поведения пользователей предотвращать возникновение внутренних угроз и несанкционированного доступа к ресурсам сети;
- используя методы глубокого обучения, анализировать поведение программ в режиме реального времени, выявляя действия, направленные на осуществление несанкционированного доступа к данным или изменение системных файлов,
- при помощи эвристических методов анализа обнаруживать вредоносное программное обеспечение, не имеющее известных сигнатур.
- проводить анализ большого количества образцов программного обеспечения, классифицируя их как вредоносные или безопасные;
- выявлять отклонения в работе сети, характерные для DDoS-атак или попыток взлома системы безопасности;

Кроме того использование сверточных и рекуррентных нейросетей позволит обеспечить обнаружение подозрительных изменений в спектрах радиосигналов, которые, как правило, свидетельствуют о таких угрозах, как попытки глушения, перехвата или подмены радиосигнала

В заключении следует отметить, что современные технологии искусственного интеллекта при корректном их использовании могут сыграть важную роль в обеспечении надежной и эффективной эксплуатации сетей ПМР. Использование данных технологий позволяет существенно повысить уровень автоматизации процессов эксплуатации данных систем, снизить вероятность отказов, оптимизировать ресурсы.

Внедрение последних достижений в области искусственного интеллекта в процессы управления и эксплуатации сетей ПМР открывает новые горизонты для обеспечения их бесперебойной работы, больших объемов разнородного трафика, снижения расходов на процессы эксплуатации. В дальнейшем использование технологий искусственного интеллекта для автоматизации и оптимизации процессов управления в сетях ПМР будет только расширяться, предлагая всё более сложные и интегрированные решения, направленные на удовлетворение растущих требований к скорости, безопасности и масштабируемости.

Список литературы

1. I. Goodfellow, Y. Bengio, A. Courville. «Deep Learning». // MIT Press, 2016, 775 с. // ISBN-13: 978-0262035613.
2. Николенко С.И. «Рекуррентные нейронные сети». //Электронный ресурс: <https://logic.pdmi.ras.ru/~sergey/teaching/mlhse19/17-rnn.pdf>.

3. Бхарти Кхемани, Шрути Патил «Обзор графовых нейронных сетей: концепции, архитектуры, методы, проблемы, наборы данных, приложения и будущие направления», //В журнале «Журнал больших данных: 2024.

References

1. . I. Goodfellow, Y. Bengio, A. Courville. «Deep Learning». // MIT Press, 2016, 775 p. // ISBN-13: 978-0262035613.
 2. Nikolenko S.I. "Recurrent neural networks". //Electronic resource: <https://logic.pdmi.ras.ru/~sergey/teaching/mlhse19/17-rnn.pdf>.
 3. Bharti Khemani, Shruti Patil "Overview of graph neural networks: concepts, architectures, methods, problems, datasets, applications and future directions", //In the journal "Journal of Big Data: 2024.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942.2

БУДУЩЕЕ ТЕХНОЛОГИИ ЦИФРОВЫХ ДВОЙНИКОВ

¹ Мадатов Д.А., ² Борисов В.В., ³ Сивков В.С.

ФГБОУ ВО «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ», г. Самара, Россия (443010, г. Самара ул. Льва Толстого, 23), e-mail: ¹ dima.madatov.2015@mail.ru, ² v.borisov@psuti.ru, ³ v.sivkov@psuti.ru

Технология цифровых двойников развивается в быстром темпе, показывая как и огромные возможности, так и вероятные проблемы. В статье будут рассмотрены потенциальные направления развития технологии, ее возможное применение в различных отраслях и проблемы, с которыми она может столкнуться. Также будет затронута тема этических последствий и социального влияния данной технологии.

Ключевые слова: Цифровые двойники, искусственный интеллект, дополненная реальность, метавселенная, квантовые вычисления, облачные технологии.

THE FUTURE OF DIGITAL TWIN TECHNOLOGY

¹ Madatov D.A., ² Borisov V.V., ³ Sivkov V.S.

VOLGA REGION STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Samara, Russia (443010, Samara st. Lev Tolstoy, 23), e-mail: ¹ dima.madatov.2015@mail.ru, ² v.borisov@psuti.ru, ³ v.sivkov@psuti.ru

Digital twin technology is evolving at a rapid pace, showing both enormous opportunities and potential challenges. The article will discuss potential directions for the development of technology, its possible application in various industries, and the problems it may encounter. The ethical implications and social impact of this technology will also be addressed

Keywords: Digital twin, artificial intelligence, augmented reality, metaverse, quantum computing, cloud technologies.

Технология цифровых двойников быстро развивается из узкоспециализированных приложений в комплексный инструмент, влияющий на множество различных отраслей и аспектов жизни. Появление более мощных вычислительных ресурсов, развитие искусственного интеллекта и его распространение открывают невероятные перспективы для разработки и применения цифровых двойников. В этой работе рассматриваются основные тенденции и прогнозы развития этой технологии, анализируется ее потенциал для оптимизации производственных процессов, улучшения качества жизни и решения глобальных проблем.

Цифровые двойники представляют собой виртуальные копии физических объектов, процессов или систем. Эти копии создаются на основе данных из реального мира и используют моделирование для предсказаний поведения оригинала при различных условиях.

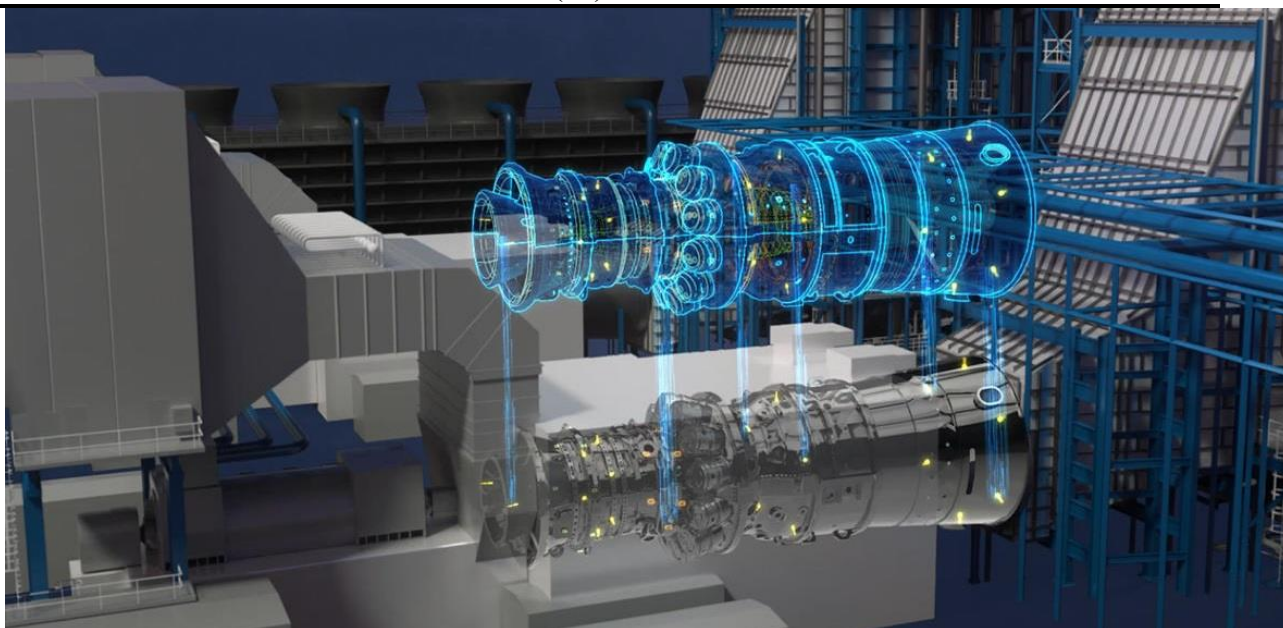


Рисунок 1 - Пример цифрового двойника

Источник: презентация с акселератора ПУТП 2024 на тему «Использование цифровых двойников для повышения эффективности основного оборудования ТЭС»

Потенциальные направления развития технологии цифровых двойников:

Несмотря на значительный прогресс, технологии цифровых двойников все еще имеют потенциал для развития. Рассмотрим некоторые варианты потенциального развития технологии цифровых двойников:

1. Искусственный интеллект и машинное обучение. Искусственный интеллект дает цифровым двойникам возможность учиться самостоятельно, анализировать большие объемы данных и прогнозировать поведение моделируемых систем на основе исторических данных и внешних факторов. Машинное обучение может повысить точность моделей, оптимизировать параметры и улучшить алгоритмы цифровых двойников, повышая эффективность управления и принятия решений. Благодаря этим технологиям цифровые двойники больше не являются статичными моделями, а становятся динамичными, саморазвивающимися системами, способными адаптироваться к меняющимся условиям и принимать решения в реальном времени, открывая новые перспективы оптимизации процессов во многих областях, от промышленности до медицины.

2. Дополненная реальность и метавселенные [1]. Дополненная реальность и метавселенные значительно расширяют возможности взаимодействия с цифровыми двойниками, делая их использование более интуитивным и эффективным. Интеграция цифровых двойников с технологиями виртуальной и дополненной реальности позволяет экспертам просматривать модели в трехмерном пространстве и взаимодействовать с ними, обеспечивая лучшее понимание того, как работают сложные системы, и позволяет получать виртуальные впечатления без физического вмешательства. Возможность применения цифрового двойника к реальному объекту в дополненной реальности открывает новые перспективы для профилактического обслуживания и удаленного управления оборудованием. Напротив, метавселенные создают виртуальные среды для сотрудничества с цифровыми двойниками, обеспечивая совместное моделирование и анализ данных, помогая ускорить

инновации и помочь более эффективно решать сложные проблемы. Таким образом, дополненная реальность и метавселенные выводят взаимодействие с цифровым двойником на принципиально новый уровень, предоставляя более мощные инструменты для моделирования, анализа и управления сложными системами.

3. Квантовые вычисления. Квантовые вычисления представляют собой революционный подход к обработке информации, который может фундаментально изменить развитие и перспективы технологии цифровых двойников. Способные решать сложные математические задачи гораздо быстрее и эффективнее, квантовые компьютеры позволят создавать цифровые двойники гораздо большей сложности и точности, моделируя систему с гораздо большим количеством переменных и взаимодействий, которые ранее были недоступны классическим компьютерным инструментам. Это открывает новые возможности для моделирования высокодинамичных процессов, таких как поток жидкости, поведение сложных молекулярных структур или реакция на экстремальные нагрузки. Кроме того, квантовые вычисления значительно сократят время, необходимое для создания и обновления цифровых двойников, а также повысят точность предсказаний и прогнозов, что сделает их мощным инструментом, незаменимым для решения сложных задач в различных областях науки и техники.

4. Бессерверные архитектуры и облачные технологии. Бессерверные архитектуры и облачные технологии играют ключевую роль в разработке и перспективах технологии цифровых двойников, обеспечивая масштабируемость, гибкость и экономическую эффективность. Облачные платформы предоставляют вычислительную мощность и ресурсы хранения, необходимые для обработки больших объемов данных цифровых двойников, позволяя создавать и поддерживать сложные модели без инвестиций в собственную инфраструктуру. Бессерверная архитектура позволяет оптимизировать затраты и упростить развертывание и обслуживание приложений цифровых двойников, платя только за используемые вычислительные ресурсы. Эти технологии делают создание и использование цифровых двойников более доступным для широкого круга организаций, обеспечивая быстрое внедрение и внедрение этой многообещающей технологии.

Применение технологии цифровых двойников в различных отраслях:

Цифровые двойники довольно гибкая технология позволяющая упрощать работу в различных отраслях. Ниже рассмотрим некоторые варианты внедрения цифровых двойников в определенную отрасль, для дальнейшего упрощения работы:

1. Цифровые двойники в энергетике и автомобилестроении [2]. Внедрение технологии цифровых двойников в промышленности, в частности в энергетику и автомобилестроение, приведет к существенному упрощению производственных процессов и повышению их эффективности. В энергетике, цифровые двойники позволят оптимизировать работу электростанций, прогнозировать потребление энергии, улучшить надежность энергосистем. В автомобилестроении, цифровые двойники компонентов автомобилей позволят улучшить процесс проектирования, провести виртуальные испытания, оптимизировать производственные линии, повысить качество продукции и обеспечить более эффективное обслуживание автомобилей. В целом, цифровые двойники позволят сократить время вывода новой продукции на рынок, снизить издержки, повысить надежность работы оборудования, а также улучшить качество принимаемых решений на всех этапах производственного цикла.

2. Цифровые двойники в здравоохранении [3]. Цифровые двойники пациентов на основе медицинских изображений, генетических данных и истории болезни позволяют врачам более точно моделировать индивидуальные характеристики и прогнозировать реакцию на различные виды лечения. Это позволяет применять персонализированный подход к лечению, повышая эффективность и снижая риск побочных эффектов. Виртуальное моделирование хирургических процедур с использованием цифровых двойников позволяет хирургам совершенствовать свои навыки и точнее планировать сложные операции, снижая риски для пациентов. Кроме того, цифровые двойники могут помочь в разработке новых лекарств и медицинских устройств, а также виртуально тестировать и оптимизировать конструкции. В целом цифровые двойники в здравоохранении могут помочь улучшить качество медицинской помощи, уменьшить количество медицинских ошибок и улучшить результаты лечения пациентов.

3. Цифровые двойники в сфере управления городами [4]. Внедрение технологии цифровых двойников в сфере городского управления позволит существенно повысить эффективность городского планирования и управления инфраструктурой. Цифровые двойники городов, созданные на основе данных о зданиях, дорогах, энергетических сетях, транспортных потоках и других городских системах, позволяют моделировать различные сценарии городского развития и оптимизировать работу инфраструктуры. Это поможет более эффективно решать проблемы, связанные с пробками на дорогах, загрязнением воздуха, утилизацией отходов, распределением ресурсов и другими сложными вопросами. Моделируя различные воздействия (изменение климата, рост населения и т. д.), городские власти могут принимать более обоснованные решения и предвидеть потенциальные проблемы. Цифровые двойники также могут повысить эффективность общественных работ, оптимизировать затраты на содержание инфраструктуры и улучшить качество жизни горожан.

4. Цифровые двойники в борьбе с изменением климата. Внедрение технологии цифровых двойников значительно упростит борьбу с изменением климата, предоставляя мощные инструменты для моделирования климатических процессов и тестирования различных стратегий смягчения последствий. Цифровой двойник климатической системы, основанный на данных о выбросах парниковых газов, температуре, осадках и других климатических параметрах, поможет ученым и политикам лучше прогнозировать будущие изменения климата и руководить реализацией различных мер по сокращению выбросов. Моделирование различных сценариев, включая влияние различных политик по сокращению выбросов, может помочь определить наиболее эффективные политики и оптимизировать распределение ресурсов. Цифровые двойники также могут помочь разработать и протестировать новые технологии улавливания и хранения углерода, лучше оценить риски и уязвимости различных регионов перед лицом изменения климата и разработать эффективные стратегии адаптации.

Потенциальные проблемы развития технологии цифровых двойников:

Хоть потенциал и удобства, предоставляемые технологией цифровых двойников довольно велики, у данной технологии все ещё имеются проблемы на пути развития. Некоторые наиболее важные из них будут описаны далее:

1. Обеспечение кибербезопасности и защита данных. Кибербезопасность и защита данных являются важными факторами, определяющими развитие и будущее технологии

цифровых двойников. Цифровые двойники часто содержат конфиденциальную информацию о физических активах, процессах и системах, поэтому их уязвимость к киберугрозам может иметь серьезные последствия, включая финансовые потери, нарушение производственных процессов и даже физический ущерб. Для обеспечения надежности и безопасности цифровых двойников необходимо внедрение многоуровневых систем информационной безопасности, включая шифрование данных, контроль доступа, обнаружение и предотвращение вторжений, а также регулярное обновление программного и аппаратного обеспечения. Надежная кибербезопасность необходима для широкого внедрения технологии цифровых двойников, поскольку доверие к безопасности данных имеет важное значение для пользователей и потенциальных инвесторов, а отсутствие адекватных мер безопасности может помешать развитию этой многообещающей технологии.

2. Необходимость стандартизации. Разработка единых стандартов для технологии цифровых двойников имеет важное значение для обеспечения ее широкого признания и эффективного использования. В настоящее время существует большое количество несовместимых платформ и форматов данных, что серьезно затрудняет обмен информацией и интеграцию между различными системами. Общие стандарты решают эту проблему, обеспечивая совместимость различных систем и платформ и позволяя создавать более сложные и интегрированные цифровые двойники. Это снижает стоимость разработки и внедрения цифровых двойников, повышает их надежность и точность, а также дает возможность создавать более сложные и масштабируемые системы. Кроме того, общие стандарты создадут более широкий рынок программного обеспечения и услуг, связанных с цифровыми двойниками, что повысит конкуренцию и будет способствовать инновациям. Четкие стандарты повысят доверие к технологии цифровых двойников и ускорят ее внедрение во всех отраслях.

3. Вопросы этики и ответственность за действия, предсказанные двойниками. Несмотря на свой огромный потенциал, технология цифровых двойников поднимает множество сложных этических проблем, связанных с защитой данных, ответственностью за решения, принятые на основе модели, алгоритмической предвзятостью и возможностью неправильного использования технологии. Например, цифровые двойники человека содержат конфиденциальную информацию, доступ к которой должен быть строго ограничен, а алгоритмы, лежащие в основе их создания и работы, должны быть прозрачными, чтобы не допускать предвзятости при принятии решений. Разработка и внедрение цифровых двойников требует четкого определения ответственности за результаты, достигаемые с помощью цифровых двойников, а также механизмов контроля и мониторинга для предотвращения злоупотреблений. Решение этих проблем требует междисциплинарного подхода, включая разработку строгих этических кодексов, законодательства, прозрачных механизмов надзора.

Будущее технологии цифровых двойников выглядит динамичным и многообещающим. Интеграция передовых технологий, таких как искусственный интеллект, машинное обучение и дополненная реальность, приведет к созданию более умных и адаптивных цифровых двойников. Это поможет решить более сложные проблемы в различных отраслях: от производства и энергетики до медицины и управления городскими системами. Однако для полного использования потенциала цифрового двойника необходимы дальнейшие исследования в области безопасности данных, разработки и стандартизации универсальных платформ. Только комплексный подход, сочетающий науку, технологии и инновационные

решения, позволит в полной мере использовать уникальные возможности этой передовой технологии и внести существенный вклад в развитие общества.

Список литературы

1. Цифровые двойники: прошлое, настоящее и будущее. Электронный ресурс. URL: [https://up-pro.ru/library/information_systems/automation_project/proshloe-nastoyaschee-i-budushee/] (дата обращения: 05.12.2024).
2. Цифровые двойники в промышленности: истоки, концепции, современный уровень развития и примеры внедрения. Электронный ресурс. URL: [https://digitaltwin.ru/articles/digital-twins-in-industry/] (дата обращения: 05.12.2024).
3. Цифровые двойники: от истока к будущему. Электронный ресурс. URL: [https://habr.com/ru/companies/sberbank/articles/845350/] (дата обращения: 05.12.2024).
4. Что такое цифровые двойники и где их используют. Электронный ресурс. URL: [https://trends.rbc.ru/trends/industry/6107e5339a79478125166eeb] (дата обращения: 05.12.2024).

References

1. Digital twins: past, present and future. Electronic resource. URL: [https://up-pro.ru/library/information_systems/automation_project/proshloe-nastoyaschee-i-budushee /] (date of reference: 05.12.2024).
 2. Digital twins in industry: origins, concepts, current level of development and examples of implementation. Electronic resource. URL: [https://digitaltwin.ru/articles/digital-twins-in-industry /] (date of access: 05.12.2024).
 3. Digital twins: from the source to the future. Electronic resource. URL: [https://habr.com/ru/companies/sberbank/articles/845350 /] (date of access: 05.12.2024).
 4. What are digital doubles and where are they used. Electronic resource. URL: [https://trends.rbc.ru/trends/industry/6107e5339a79478125166eeb] (date of access: 05.12.2024).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738

ИСПОЛЬЗОВАНИЕ LLDP В ОТЕЧЕСТВЕННЫХ ОС НА ЯДРЕ LINUX

¹Сизов И.М., Сулимов А.Д.

ФГАОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА",
Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail:
¹goga.sizov.04@mail.ru

Протокол LLDP (Link Layer Discovery Protocol) представляет собой стандарт сетевого взаимодействия, который позволяет производить обмен информацией между устройствами. Использование данного протокола помогает упростить настройку и мониторинг сетевых соединений. В настоящее время активно развиваются отечественные операционные системы на базе ядра Linux, что напрямую связано с импортозамещением и обеспечением технологической независимости. Использование протокола LLDP также упрощает процесс построения гибких и управляемых сетей, соответствующих современным требованиям. Цель исследования заключается в анализе особенностей использования протокола LLDP в отечественных ОС на ядре Linux и выявлении недостатков использования данного протокола.

Ключевые слова: LLDP, соседние устройства, коммутатор, локальная сеть, AutoAttach-таблица, перехват пакетов.

USING LLDP IN DOMESTIC OS BASED ON THE LINUX KERNEL

¹Sizov I.M., Sulimov A.D.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky prospekt, 65 k. 1), e-mail:
¹goga.sizov.04@mail.ru

The LLDP Protocol (Link Layer Discovery Protocol) is a network communication standard that allows the exchange of information between devices. Using this protocol helps simplify the configuration and monitoring of network connections. Currently, domestic operating systems based on the Linux kernel are actively developing, which is directly related to import substitution and ensuring technological independence. Using the LLDP protocol also simplifies the process of building flexible and managed networks that meet modern requirements. The purpose of the study is to analyze the features of using the LLDP protocol in domestic OS based on the Linux kernel and identify the disadvantages of using this protocol.

Keywords: LLDP, neighboring devices, switch, LAN, AutoAttach table, packet interception.

Теоретическая основа

LLDP (Link Layer Discovery Protocol) - протокол канального уровня, позволяющий коммутатору оповещать информацию о своем существовании в локальной сети и передавать эту информацию, аналогично он может и получать сведения от другого устройства. Каждое устройство LLDP может отправлять информацию о себе соседям независимо друг от друга. Устройство хранит информацию о соседях, но не перенаправляет её. [2, с. 1]

Для LLDP зарезервирован специальный MAC-адрес, коммутаторы с таким адресом получателя не будут передавать его дальше.

LLDP использует атрибуты, которые содержат описание типа, длины и значения. Они называются TLV (тип, длина, значение). Устройства, поддерживающие LLDP, используют TLV для отправки и получения информации своим непосредственно подключенным соседям. Вот пример некоторых основных TLV: описание порта TLV, имя системы TLV, описание системы TLV, возможности системы TLV, TLV-адрес управления.

Некоторые сетевые конечные устройства могут использовать LLDP для назначения VLAN или требований PoE (Power over Ethernet). Для этого было сделано усовершенствование, которое называется MED (Media Endpoint Discovery). Обычно это называется LLDP-MED. LLDP позволяет определить физическую топологию соединений устройств и визуализировать ее в удобном для восприятия человеком виде [1, с. 144].

Методы исследования

Тип исследования

Исследование носит экспериментально-аналитический характер. Эксперимент будет направлен на настройку и проверку работы протокола LLDP в локальной сети на примере двух устройств, функционирующих в роли коммутаторов. Конфигурация будет выполняться с использованием Open vSwitch (OVS) с предварительной установкой необходимых пакетов LLDP. После установки необходимых пакетов и проверки работы протокола будет смитирована атака на пакеты протокола LLDP.

Характеристика выборки

В рамках исследования была сформирована выборка оборудования и программного обеспечения:

- Два коммутатора
- Отечественные операционные системы на базе ядра Linux: Альт, РЕД ОС, ROSA Linux, Astra Linux
- Установленный пакет Open vSwitch (OVS) для настройки виртуальных коммутаторов
- Пакет LLDP для обеспечения поддержки протокола LLDP и возможности использования команды
- Инструмент Wireshark для захвата и анализа сетевого трафика

Методы сбора данных

Для сбора данных в рамках эксперимента использовались следующие методы:

- Была настроена сеть, состоящая из двух виртуальных коммутаторов на основе Open vSwitch (OVS), с включенной поддержкой LLDP.
- Был произведен сбор данных о работе протокола LLDP с использованием встроенных инструментов, таких как lldpctl, а также команд управления конфигурацией OVS (ovs-vsctl).
- Были проанализированы передаваемые LLDP-пакеты между коммутаторами.
- Было произведено описание устройств и имени системы через AutoAttach-таблицу.
- Была зафиксирована информация о соседних устройствах на каждом коммутаторе.

- Был произведен перехват пакетов с третьего устройства, просмотр данных пакетов и сброс трафика.

Описание процедуры проведения исследования

Для проведения исследования была подготовлена тестовая среда, состоящая из двух коммутаторов, работающих на основе Open vSwitch (OVS). Настройка протокола LLDP включала включение LLDP на сетевых интерфейсах коммутаторов с помощью команды `ovs-vsctl`. Далее проводилась оценка работы и надежности LLDP. Оценка работы LLDP в сети проводилась на основе данных о корректности отображения информации о соседних устройствах, анализе структуры передаваемых LLDP-сообщений. Оценка надежности работы LLDP проводилась путем просмотра перехваченных пакетов с использованием инструмента Wireshark сбросом трафика.

Методы обработки данных

- Проведен анализ работы протокола LLDP на каждом из двух коммутаторов.
- Просмотрена в ходе эксперимента информация о работе LLDP, такая как таблица AutoAttach, отображаемая информация о соседних устройствах.
- Выявлены рекомендации в ходе имитированной атаки на пакеты протокола.

Проведение исследования

Для проведения эксперимента будет реализована топология, изображенная на Рисунке 1. Для начала эксперимент будет проведен на операционной системе Альт. Топология включает в себя подключение коммутаторов друг к другу с использованием прямых соединений. Каждый коммутатор будет настроен для передачи и приема LLDP-сообщений, а также для отображения информации о соседних устройствах.



Рисунок 1. – Топология проведения эксперимента

Для начала настроим оба устройства в качестве коммутаторов. Для этого будет использоваться пакет Open vSwitch. С помощью следующих команд на машинах Альт произведем установку пакета:

```
apt-get update  
apt-get install openvswitch -y
```

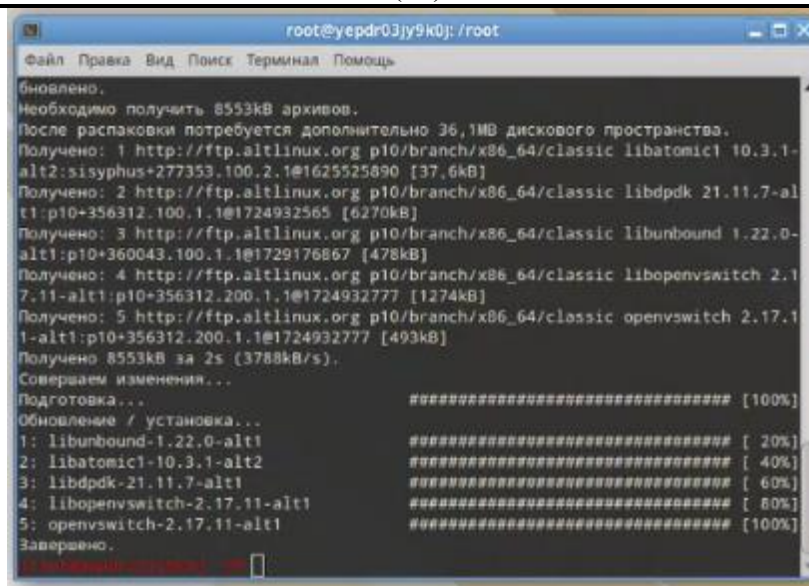



Рисунок 2 – Установка пакета Open vSwitch (Альт)

Далее произведем непосредственно настройку самих коммутаторов. Выполняется это с помощью следующих команд:

```
systemctl start openvswitch.service
ovs-vsctl add-br ovs0
ovs-vsctl add-port ovs0 enp0s3
```

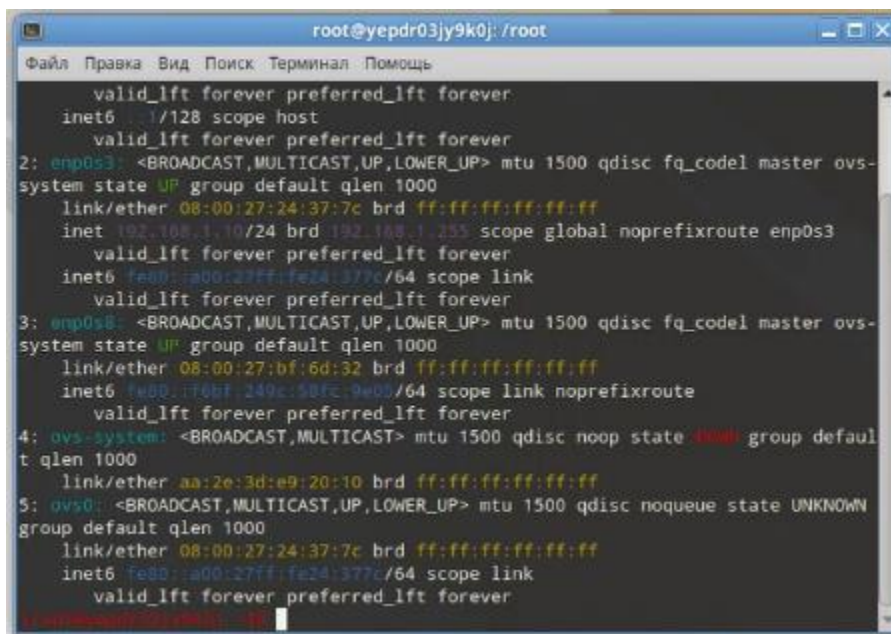
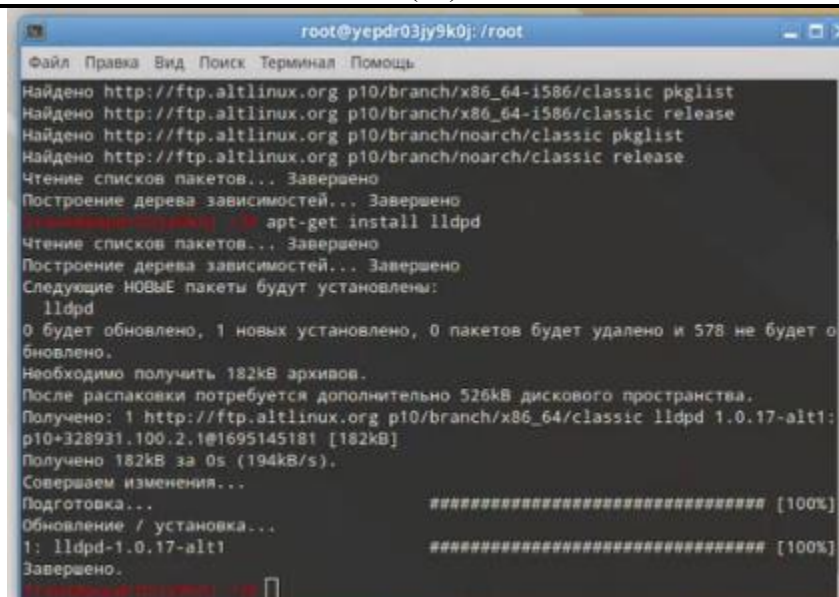


Рисунок 3 – Просмотр настройки коммутатора (Альт)

Чтобы начать настройку LLDP необходимо установить пакет на машину. Используем для этого следующие команды:

```
apt-get update
apt-get install lldpd
systemctl start lldpd
```

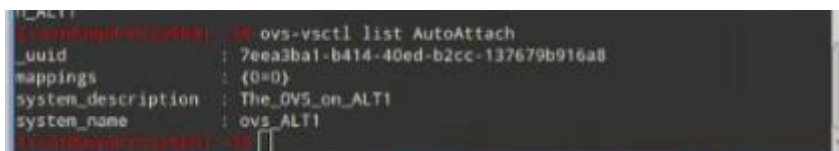


```
root@yepdr03jy9k0j: /root
Найдено http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist
Найдено http://ftp.altlinux.org p10/branch/x86_64-i586/classic release
Найдено http://ftp.altlinux.org p10/branch/noarch/classic pkglist
Найдено http://ftp.altlinux.org p10/branch/noarch/classic release
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
(AltLinux-03jy9k0j) ~# apt-get install lldpd
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
 lldpd
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 578 не будет о
бновлено.
Необходимо получить 182kB архивов.
После распаковки потребуется дополнительно 526kB дискового пространства.
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64/classic lldpd 1.0.17-alt1:
p10+328931.100.2.1@1695145181 [182kB]
Получено 182kB за 0s (194kB/s).
Совершаем изменения...
Подготовка... [100%]
Обновление / установка... [100%]
1: lldpd-1.0.17-alt1 [100%]
Завершено.
(AltLinux-03jy9k0j) ~#
```

Рисунок 4 – Установка пакета lldp (Альт)

Следующий шаг – произвести настройку LLDP на устройствах. Для этого нужно выполнить следующие команды:

```
ovs-vsctl set interface enp0s3 lldp:enable=true
ovs-vsctl add-aa-mapping ovs0 0 0
ovs-vsctl set AutoAttach . system_name="ovs_ALT1"
ovs-vsctl set AutoAttach . system_description="The_OVS_on_ALT1"
ovs-vsctl list AutoAttach
```



```
(AltLinux-03jy9k0j) ~# ovs-vsctl list AutoAttach
_uuid      : 7eea3ba1-b414-40ed-b2cc-137679b916a8
mappings   : {0=0}
system_description : The_OVS_on_ALT1
system_name : ovs_ALT1
(AltLinux-03jy9k0j) ~#
```

Рисунок 5 – Просмотр настройки таблицы AutoAttach (Альт)

Данные настройки производятся на обоих устройствах. Для просмотра информации о соседи используется команда `lldpctl show portlist enp0s3`:

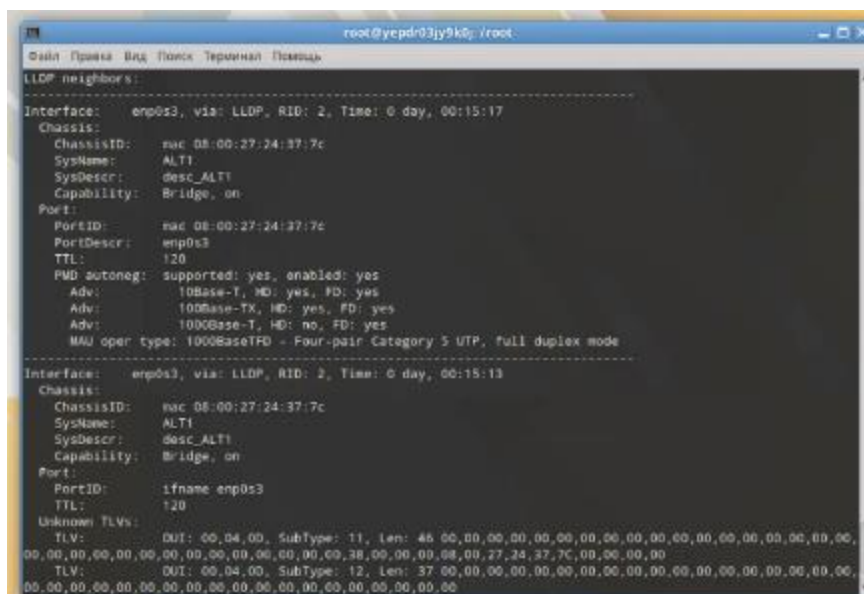


Рисунок 6 – Просмотр информации о соседе (Альт)

Со стороннего устройства выполним атаку на данный протокол. Для начала произведем перехват пакетов, далее выполним их просмотр и произведем сброс трафика. [3]

Для просмотра передаваемых пакетов необходимо на третье устройство установить Wireshark. С помощью следующих команд произведем установку:

```
sudo apt-get update  
sudo apt-get install wireshark
```

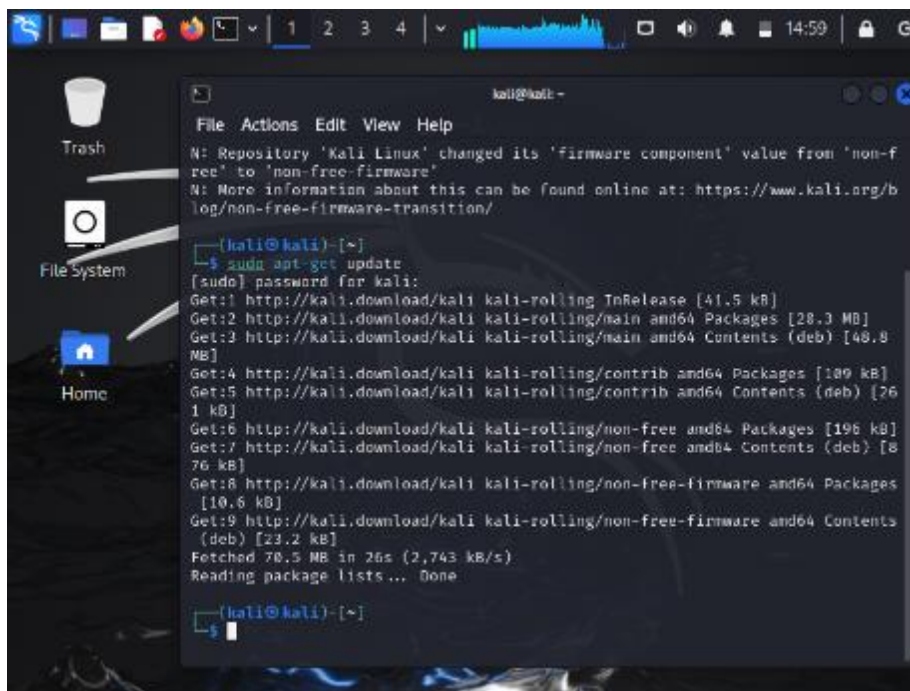


Рисунок 7 – Установка Wireshark

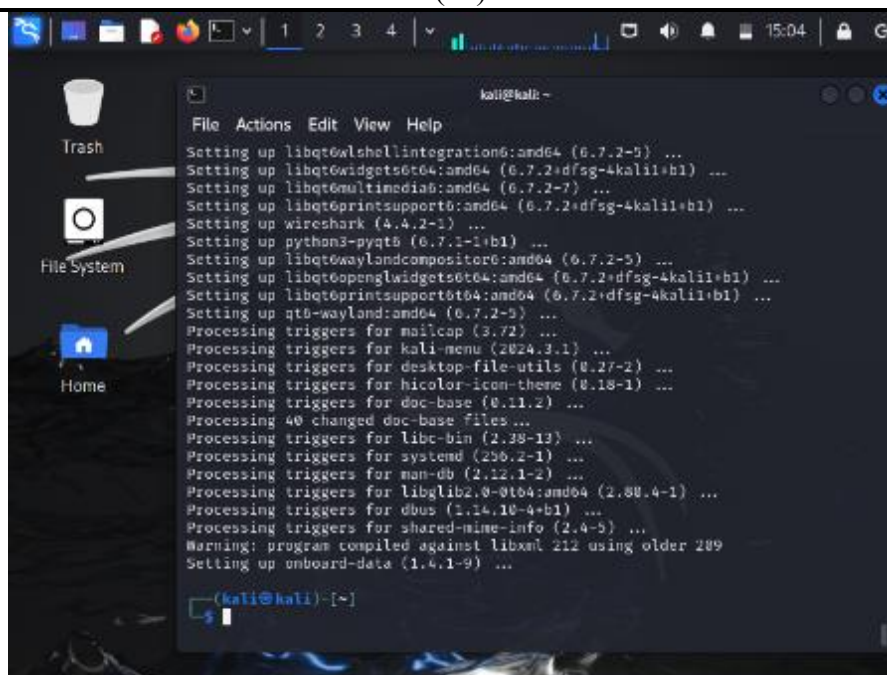


Рисунок 8 – Установка Wireshark

Теперь в самой программе посмотрим пакеты протокола LLDP.

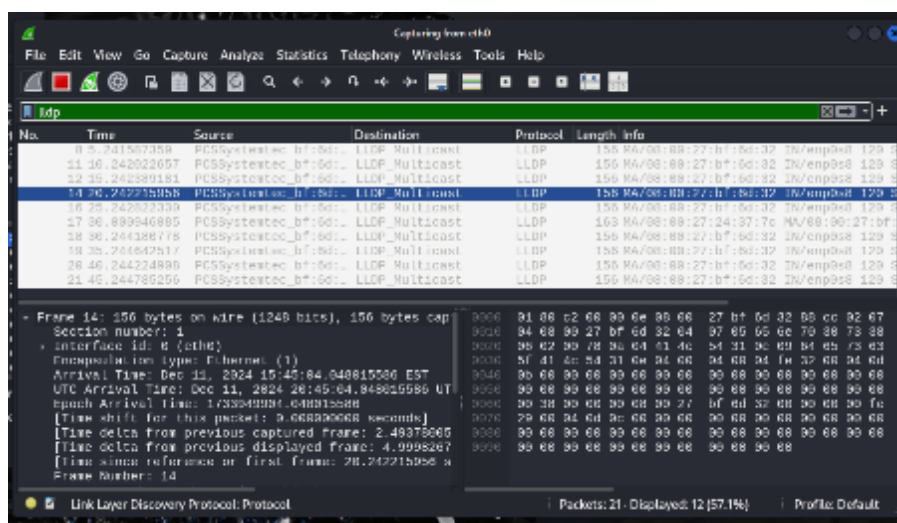


Рисунок 9 – LLDP-пакеты

Последним шагом остается сброс трафика LLDP.

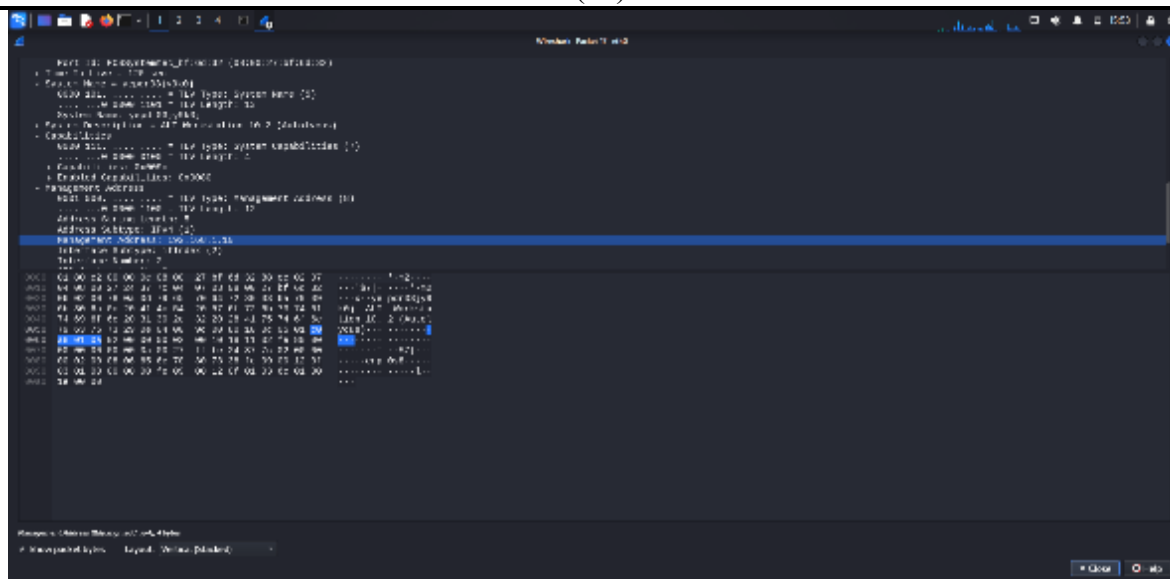


Рисунок 10 – Сброс трафика LLDP

Рассмотрим настройку LLDP на других отечественных операционных системах. Начнем с РЕД ОС. Для настройки коммутаторов и пакета LLDP будут использованы аналогичные команды [5]. Настройка коммутаторов:

```
sudo yum install openvswitch
sudo systemctl start openvswitch
sudo ovs-vsctl add-br br0
sudo ovs-vsctl add-port br0 enp0s3
```

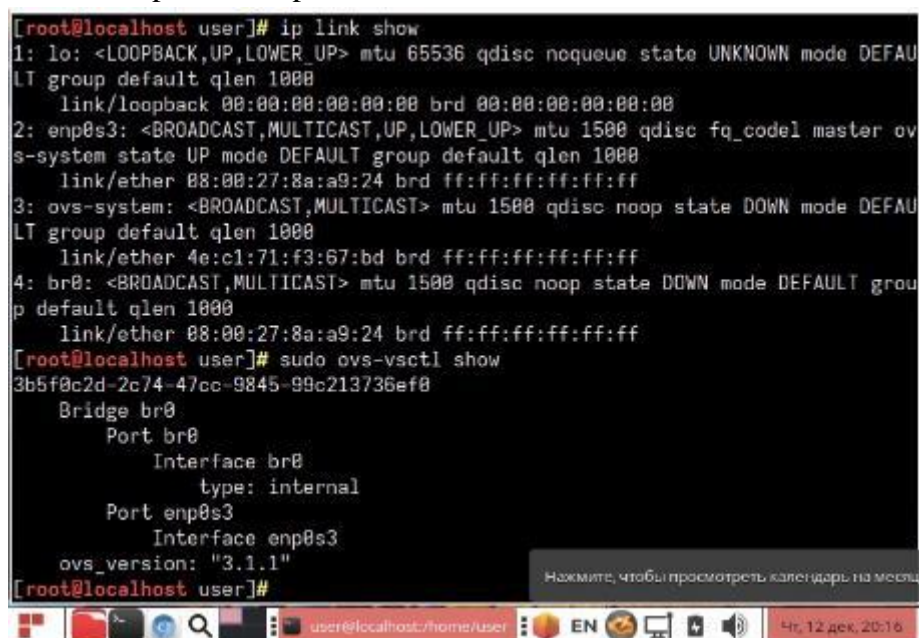


Рисунок 11 – Настройка коммутатора (РЕД ОС)

Для настройки LLDP выполним следующие команды:

```
sudo yum update
sudo yum install lldpd
```

```
sudo systemctl start lldpd
```

```
sudo ovs-vsctl set interface <имя_вашего_интерфейса> lldp:enable=true
```

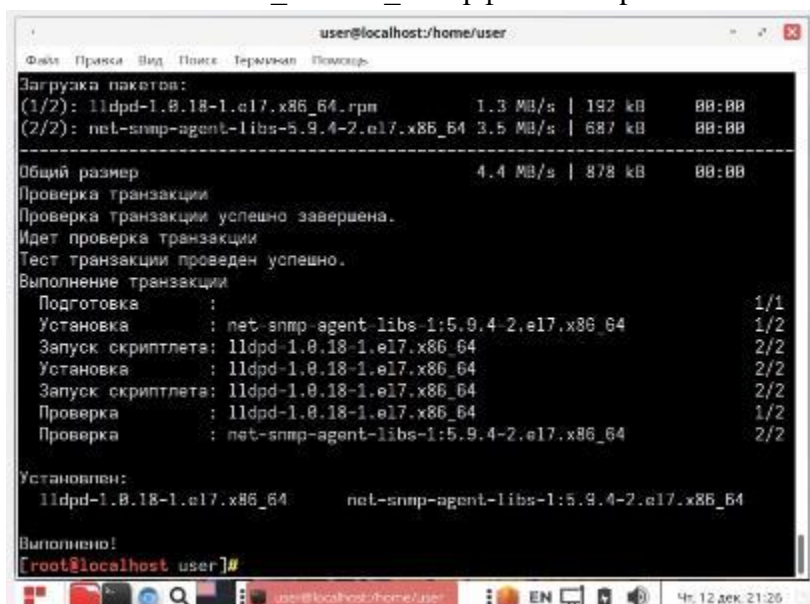


Рисунок 12 – Установка LLDP (РЕД ОС)

С помощью команды `lldpctl show enp0s3` посмотрим информацию о соседнем устройстве:

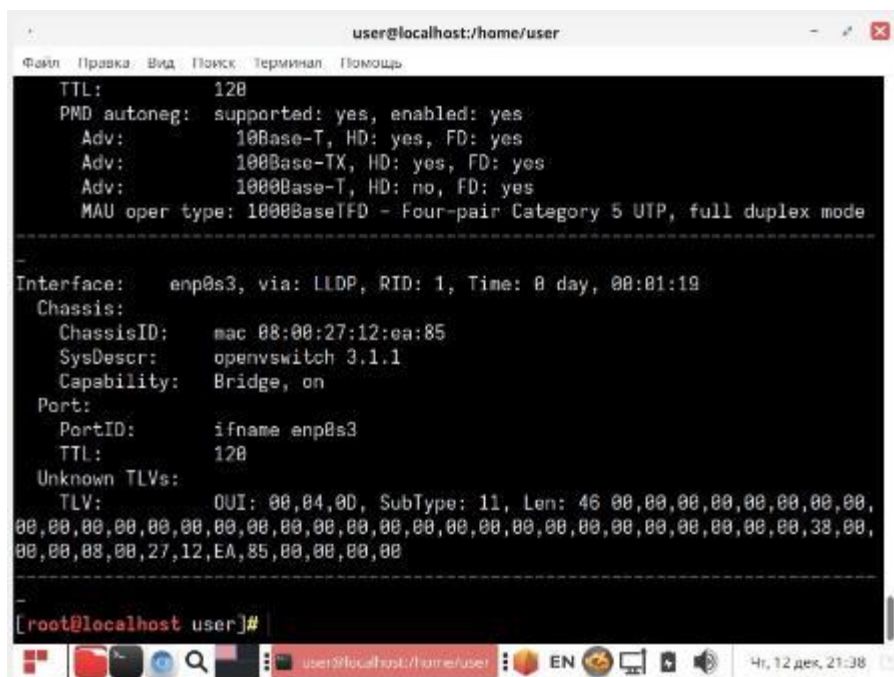


Рисунок 13 – Просмотр информации о соседе (РЕД ОС)

Настройка топологии и протокола LLDP на операционных системах ROSA Linux [7] и Astra Linux [6] производится с помощью аналогичных команд:

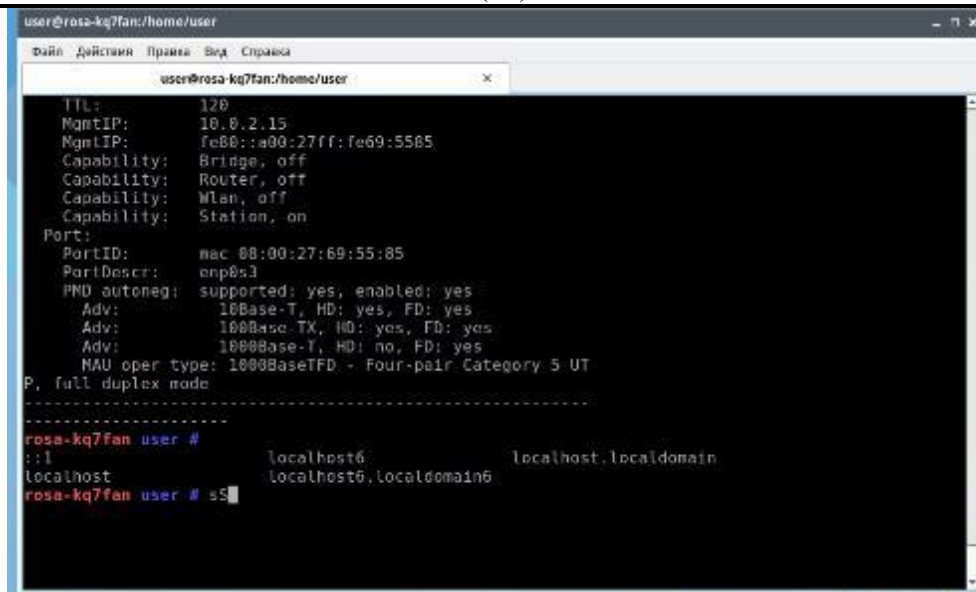


Рисунок 14 – Просмотр информации о соседе (ROSA Linux)

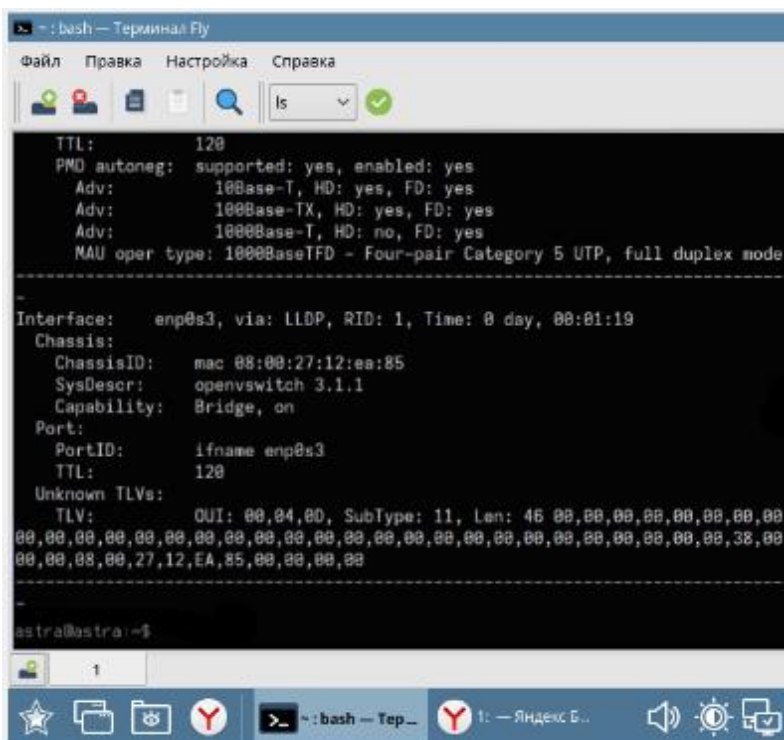


Рисунок 15 – Просмотр информации о соседе (Astra Linux)

Заключение

В ходе данного эксперимента была выполнена реализация работы протокола LLDP на устройствах с установленной на них отечественными операционными системами Альт, РЕД ОС, ROSA Linux, Astra Linux. Было показано, что протокол LLDP позволяет получать и просматривать информацию о соседних устройствах в сети. В данной части эксперимента так же было замечено, что AutoAttach - является не частью стандартной установки, а специфичной настройкой для операционной системы Альт. Другие дистрибутивы не имеют AutoAttach по умолчанию.

Второй частью данного эксперимента была произведенная на протокол атака, в ходе которой удалось просмотреть перехваченные пакеты и произвести сброс трафика. Это приводит к мысли о том, что в ходе подобной атаки злоумышленник может получить полезную для него информацию, выявить уязвимости коммутатора, которые он будет использовать в дальнейших целях. В связи с этим, будут предложены следующие рекомендации. В гостевых сетях протокол LLDP может быть включен по умолчанию, поэтому стоит его отключать на неиспользуемых интерфейсах. Таким образом, удастся прекратить транслирование данных и обеспечить защиту.

Список литературы

1. Компьютерные сети. L2–технологии : практикум / А.Г. Уймин. — Москва : Ай Пи Ар Медиа, 2024. — 191 с. (дата обращения: 29.11.2024)
2. Определение топологии с помощью протокола LLDP в сетях Juniper / Лагутин И.А. [Электронный ресурс]. URL: <https://www.elibrary.ru/> (дата обращения: 10.12.2024)
3. 5 Простых методов защиты маршрутизатора - включая атаку и анализ пакетов / Брэндон Хитцель [Электронный ресурс]. URL: <https://www.networkdefenseblog.com/post/> (дата обращения: 10.12.2024)
4. Документация NAG [Электронный ресурс]. URL: <https://nag.wiki/> (дата обращения: 10.12.2024)
5. База знаний РЕД ОС [Электронный ресурс]. URL: <https://redos.red-soft.ru/base/> (дата обращения: 10.12.2024)
6. База знаний Астра [Электронный ресурс]. URL: <https://wiki.astralinux.ru/kb/alfavitnyj-ukazatel-190914856.html> (дата обращения: 10.12.2024)
7. Системное Администрирование ОС Роса «Хром» / Мирзоян А.В. [Электронный ресурс]. URL: https://stage.rosalinux.ru/media/2024/05/rosa_basics.pdf (дата обращения: 10.12.2024)
8. Перехват и анализ сетевого трафика с помощью «Wireshark» / Мешкова Елена Владимировна [Электронный ресурс]. URL: <https://elibrary.ru/item.asp?id=27443875> (дата обращения: 10.12.2024)

References

1. Computer networks. L2 technologies : a practical course / A.G. Uimin. — Moscow : AI Pi Ar Media, 2024. — 191 p. (accessed: 11/29/2024)
2. Topology determination using the LLDP protocol in Juniper networks / Lagutin I.A. [Electronic resource]. URL: <https://www.elibrary.ru/> / (date of request: 10.12.2024)
3. 5 Simple methods of router protection - including attack and packet analysis / Brandon Hitzel [Electronic resource]. URL: <https://www.networkdefenseblog.com/post/> / (date of request: 10.12.2024)
4. NAG Documentation [Electronic resource]. URL: <https://nag.wiki/> / (date of request: 10.12.2024)
5. Knowledge base of the RED OS [Electronic resource]. URL: <https://redos.red-soft.ru/base/> / (date of request: 10.12.2024)
6. Astra knowledge base [Electronic resource]. URL: <https://wiki.astralinux.ru/kb/alfavitnyj-ukazatel-190914856.html> (date of application: 10.12.2024)

7. System Administration of Rosa "Chrome" OS / Mirzoyan A.V. [Electronic resource]. URL: https://stage.rosalinux.ru/media/2024/05/rosa_basics.pdf (date of application: 10.12.2024)
 8. Interception and analysis of network traffic using Wireshark / Meshkova Elena Vladimirovna [Electronic resource]. URL: <https://elibrary.ru/item.asp?id=27443875> (date of application: 10.12.2024)
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.421

МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ПОТОКОВЫХ ДАННЫХ ВЫСОКОЙ РАЗМЕРНОСТИ

Гультяев А.А.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ "МИФИ", Москва, Россия, (115409, город Москва, Каширское ш., д.31), e-mail: angultiaev@gmail.com

В статье рассматривается применимость алгоритмов машинного обучения, использующихся для решения задачи обнаружения аномалий, к непрерывным потокам данных высокой размерности, таким как показания датчиков и сенсоров или векторные представления последовательных данных, таких как части видеоряда. Ключевыми аспектами применимости алгоритмов являются возможности «холодного старта», онлайн-обучения, коррекции ответов, путем взаимодействия с оператором, а также вычислительная сложность и производительность. В статье рассмотрены детали реализации алгоритмов для возможности обработки данных высокой размерности, а также приведен сравнительный анализ их качества по нескольким метрикам машинного обучения.

Ключевые слова: Машинное обучение, искусственный интеллект, нейронная сеть, векторное представление, обнаружение аномалий.

ANOMALY DETECTION METHODS IN HIGH-DIMENSIONAL STREAMING DATA

Gulyaev A.A.

NATIONAL RESEARCH NUCLEAR UNIVERSITY MEPhI, Moscow, Russia, (115409, Moscow, Kashirskoye shosse, 31), e-mail: angultiaev@gmail.com

This paper addresses the applicability of machine learning algorithms used to solve the anomaly detection task to high dimensional continuous data streams such as sensor and sensor readings or vector representations of sequential data such as parts of a video sequence. Key aspects of the applicability of the algorithms are cold-start capabilities, online learning, correction of responses, through operator feedback, and computational complexity and performance. The paper discusses the implementation details of the algorithms to be able to process high dimensional data, and provides a comparative analysis of their quality on several machine learning metrics.

Keywords: Machine learning, artificial intelligence, neural network, vector embedding, anomaly detection.

Введение

Задача обнаружения аномалий, также известная как задача обнаружения выбросов – это задача выявления редких элементов, событий или наблюдений в данных, которые значительно отклоняются от подавляющего большинства.

Термин «аномалия» стал набирать популярность в XX веке, когда анализ данных стал включать в себя различные приложения, такие как обнаружение мошенничества и контроль качества. С появлением информатики в середине XX века акцент сместился на автоматизацию этих процессов. К концу 1990-х - началу 2000-х годов доступность больших массивов данных и достижения в области машинного обучения позволили разработать сложные методы обнаружения аномалий.

Существует три основных типа аномалий, встречающихся в данных:

1. Точечные аномалии. Один экземпляр данных, значительно отличается от остальной части набора данных. Примером точечной аномалии является транзакция на сумму 100 000 рублей в наборе данных, состоящем из типичных транзакций на сумму от 100 до 1000 рублей.
2. Контекстные аномалии. Экземпляр данных, является аномальным в определенном контексте, но не в других случаях. Контекстные аномалии характерны для временных рядов и пространственных данных. Примером контекстной аномалии является всплеск потребления электроэнергии в полночь, который необычен по сравнению с обычным полуночным использованием.
3. Коллективные аномалии. Некоторое количество данных в целом отклоняется от нормы, даже если отдельные точки данных не являются аномальными. Примером такой аномалии является последовательность сетевых запросов, происходящая при кибератаке.

Методы выявления аномалий широко используются в финансовой сфере, здравоохранении, информационной безопасности, маркетинге и продажах, промышленности и т.д.

Методы обнаружения аномалий разделяются на три основных категории: методы обучения с учителем (англ. supervised), методы обучения без учителя (англ. unsupervised) и методы обучения с частичным привлечением учителя (англ. semi-supervised). Алгоритмам обнаружения аномалий с учителем требуется размеченный набор данных для «нормальных» и «аномальных» событий. Для решения такой задачи могут быть использованы классические алгоритмы классификации, такие как машины опорных векторов [1], деревья решений [2], случайные леса [3] или многослойные перцептроны. Для обнаружения аномалий без учителя не требуется размеченный набор данных, а алгоритмы полагаются на неявные зависимости в данных для выявления аномальных событий. В этом случае могут быть использованы методы кластеризации, такие как DBSCAN [4], методы, основывающиеся на плотности распределения исходных данных, такие как Local Outlier Factor (LOF) [5] или Isolation Forest [6]. Методам обнаружения аномалий с частичным привлечением учителя также требуется размеченный набор данных, но только «нормальных» событий. Аномалии идентифицируются как отклонения от «выученных» шаблонов «нормальности» событий. Примерами таких методов является одноклассовый метод опорных векторов [7] или модели гауссовский смесей (англ. Gaussian Mixture Models) [8].

Методам обнаружения аномалий зачастую требуется набор данных, на котором модель может обучаться. Если такой набор данных недоступен, или данные приходят со временем, классические подходы к распознаванию аномалий не применимы. Ситуация, в которой набор исторических наблюдений недоступен на момент запуска работы модели, называется холодным стартом. Для решения такого рода задач необходимы алгоритмы, которые могут обучаться на новых данных, которые приходят со временем. Обучение таких моделей называется онлайн-обучением.

Помимо вышеуказанных проблем, алгоритм, еще не обученный на достаточном количестве данных будет часто ошибаться при решении задачи. Для более быстрого обучения, в алгоритм может быть внедрен механизм обратной связи с оператором. При ложноположительном или ложноотрицательном ответе алгоритма, оператор может вручную указать на факт отсутствия или присутствия аномалии в текущей части данных.

В статье рассмотрены алгоритмы обнаружения аномалий, такие как:

1. онлайн-метод k-ближайших соседей (Online k-NN);
2. онлайн-метод опорных векторов (Online SVM);
3. инкрементальная модель гауссовских смесей (Incremental GMM);
4. онлайн-случайный лес;
5. автокодировщик;
6. самоорганизующиеся карты;
7. методы обучения с подкреплением;
8. инкрементальный алгоритм DBSCAN.

Все алгоритмы могут обучаться на последовательно поступающих данных, а также прямо или косвенно допускать взаимодействие с оператором.

Сравнительный анализ алгоритмов

Онлайн-метод k-ближайших соседей (Online k-NN)

Алгоритм k-NN классифицирует точки данных на основе мажоритарных классов среди их ближайших соседей в пространстве признаков. Для обнаружения аномалий может быть использован порог метрики расстояния между наблюдениями. В таком случае, если расстояние до новой точки данных превышает этот порог, объект будет классифицирован как аномальный.

Алгоритм k-NN обучается путем сохранения исходной выборки данных для последующего расчета расстояний. Онлайн-обучение такого алгоритма достигается за счет добавления новых точек данных в исходную выборку.

Метод k-ближайших соседей прост в реализации, и поддерживает добавление исходных данных без обучения заново. Однако, с ростом обучающей выборки, расчет расстояний будет становиться более вычислительно сложным процессом [9], а выбор порога расстояния является нетривиальной задачей, требующей экспериментов и тонкой настройки алгоритма. Стоит также отметить, что алгоритм k-ближайших соседей работает менее эффективно на данных высокой размерности.

Онлайн-метод опорных векторов (Online SVM)

Метод опорных векторов стремится найти гиперплоскость, наилучшим образом разделяющую два класса, максимизируя расстояние между классами [1]. Онлайн-версия метода адаптирует этот подход для потоковых данных. Обучение начинается с минимального набора размеченных данных, и, с получением размеченных новых данных (например, от обратной связи с оператором), координаты гиперплоскости изменяются, а новые объекты классифицируются исходя того, с какой стороны от построенной гиперплоскости они находятся. [10]

Данный метод эффективен в пространствах высокой размерности. Модель может обновляться путем использования таких техник, как стохастический градиентный спуск, а функции ядер позволяют улавливать нелинейные зависимости в данных. Однако метод требует большое количество размеченных данных, а следовательно, интенсивного взаимодействия с оператором.

Инкрементальная модель гауссовских смесей (Incremental GMM)

GMM моделируют распределения данных как смесь нескольких гауссовских распределений, отражающих основные закономерности исходных данных. Модель обучается на данных, представляющих «нормальные» события. При классификации новой точки данных, модель рассчитывает оценку правдоподобия принадлежности этой точки данных смеси распределений [8]. Низкая оценка правдоподобия указывает на возможное наличие аномалии. С получением новых данных или путем взаимодействия с оператором, параметры модели обновляются с использованием инкрементального ЕМ-алгоритма [11].

Инкрементальная модель гауссовских смесей позволяет получать оценку правдоподобия для задачи распознавания аномалий, которую можно интерпретировать как вероятность аномалии. Тем не менее, модели такого типа склонны переобучаться, а использование инкрементального ЕМ-алгоритма является вычислительно сложной задачей.

Онлайновый случайный лес (Online Random Forest)

Случайный лес является ансамблевым алгоритмом, использующим несколько решающих деревьев для повышения эффективности классификации. Вместо классических деревьев решений в алгоритме использованы деревья VFDT (Very Fast Decision Tree), также известные как деревья Хеффдинга [12], которые позволяют обучаться на потоковых данных. Аномальность точки данных может быть определена в зависимости от того, насколько глубоко в дереве оказалась данная точка.

Алгоритм случайного леса в целом позволяет добиваться большей точности классификации, уменьшая разброс предсказаний, а также может предоставить информацию о том, какие признаки в обучающей выборке более важны. Несмотря на то, что данный способ подходит для большого количества данных, алгоритм VFDT достаточно сложен в реализации по сравнению с классическими деревьями решений, такими как CART [2], а также не может быстро адаптироваться к новым зависимостям, полученным из данных.

Автокодировщик (AutoEncoder)

Автокодировщики являются нейронными сетями, обучаемыми для реконструирования исходных данных по неявным зависимостям в них. Автокодировщики обычно состоят из двух частей: кодировщика и декодера. Первый представляет исходные данные в виде векторов меньшей размерности, а второй на основе данного вектора пытается восстановить исходные данные [13]. В задаче распознавания аномалий автокодировщик обучается на «нормальных» примерах. При получении новой точки данных, рассчитывается ошибка реконструирования (например, среднеквадратичная ошибка) данной точки. Поскольку, алгоритм не обучался на аномальных примерах, высокие значения такой ошибки могут являться индикаторами аномалий.

Автокодировщики являются мощными инструментами, т.к. могут улавливать сложные нелинейные зависимости, а также позволяют оперировать данными больших размерностей. Однако важно понимать, что обучение нейронных сетей достаточно трудоемкий процесс, а выбор архитектуры и гиперпараметров модели требует значительного опыта от разработчика.

Самоорганизующаяся карта (Self-Organizing Map, SOM)

Самоорганизующаяся карта является нейронной сетью, обучающейся без учителя. Данный алгоритм снижает размерность признакового пространства, при этом сохраняя

топологические характеристики исходных данных. Нейронная сеть обучается организовывать похожие точки данных ближе друг к другу в признаковом пространстве [14]. В данном случае, аномалиями будут являться точки данных, попавшие в области, в которых небольшое число экземпляров из обучающей выборки, или их нет совсем.

Самоорганизующиеся карты поддерживают онлайн обучение на новых примерах, однако могут терять свою эффективность на данных очень высокой размерности.

Методы обучения с подкреплением (Reinforcement Learning)

Обучение с подкреплением включает в себя обучение политике максимизации совокупного вознаграждения при взаимодействии с некой средой [15]. Для задачи обнаружения аномалий, точки данных представляют собой состояния среды, действиями модели являются решения об аномальности новой точки данных, модель получает вознаграждение, если оператор согласен с ее решением.

Данный подход, несмотря на свою эффективность при обучении сложными зависимостям и возможность прямого взаимодействия с оператором, сложен в реализации, а также требует большого количества контактов с оператором для эффективного обучения.

Инкрементальный алгоритм DBSCAN

Алгоритм DBSCAN использует предположение о достижимости одной точки исходных данных из других точек на основе выбранного порога метрики расстояния. Если точка недостижима из других точек обучающей выборки, она является выбросом [4]. В задаче выявления аномалий, индикатор выброса может служить индикатором аномального события.

Данный алгоритм поддерживает онлайн обучение по мере получения новых обучающих данных, и естественным образом подходит для задачи идентификации выбросов (аномалий), однако алгоритм очень чувствителен к выбору гиперпараметров, таких как метрика расстояния, количество точек или порог расстояния. Помимо этого, с ростом размера обучающей выборки, вычислительная сложность алгоритма также растет.

В таблице ниже приведена оценка каждого из рассмотренных методов по трем критериям: эффективность работы на больших выборках, эффективность работы на данных высокой размерности, а также субъективная оценка сложности реализации и настройки алгоритма.

Таблица 1- Оценки рассмотренных алгоритмов

Алгоритм\Критерий	Эффективность для больших выборок	Эффективность на данных высокой размерности	Сложность реализации и настройки
Online k-NN	Низкая	Низкая	Низкая
Online SVM	Средняя	Средняя	Средняя
Incremental GMM	Средняя	Высокая	Высокая
Online Random Forest	Высокая	Средняя	Средняя
Autoencoder	Высокая	Высокая	Средняя
Self-Organizing Map	Средняя	Низкая	Низкая
Reinforcement Learning	Высокая	Высокая	Высокая
Incremental DBSCAN	Средняя	Средняя	Средняя

Результаты экспериментов

Рассмотренные алгоритмы протестированы при решении задачи обнаружения аномалий. Размер выборки данных для решения задачи составляет 17 280 наблюдений, каждое наблюдение представляет собой вектор размерности 1024, а баланс классов составляет 99% «нормальных» событий и 1% аномалий. Процесс обучения каждой из моделей начинается с необученной модели, а данные передаются в модель последовательно.

В Таблице 2 ниже приведены оценки точности, полноты и f1-метрики рассмотренных алгоритмов при решении задачи распознавания аномалий на потоковых данных.

Таблица 2 - Метрики качества решения задачи обнаружения аномалий

Алгоритм\Метрика	Precision	Recall	f1-score
Online k-NN	0.28	0.3	0.29
Online SVM	0.54	0.68	0.60
Incremental GMM	0.64	0.72	0.68
Online Random Forest	0.36	0.78	0.49
Autoencoder	0.76	0.88	0.81
Self-Organizing Map	0.29	0.67	0.40
Reinforcement Learning	0.67	0.71	0.69
Incremental DBSCAN	0.43	0.52	0.47

Наихудшее качество показал алгоритм k-ближайших соседей, однако такой результат ожидаем в ситуациях, когда данные имеют высокую размерность.

Алгоритм онлайн-случайного леса и самоорганизующаяся карта показали достаточно высокую полноту, но плохую точность. Такой результат связан с тем, что по мере обучения случайного леса, деревья в нем становятся все глубже, и процесс обнаружения аномалий, опирающийся на глубину нахождения конкретной вершины усложняется. Процесс обнаружения аномалий для самоорганизующейся карты заключается в выявлении точек данных, попавших в области, в которых находятся мало примеров из обучающей выборки, или они отсутствуют вовсе. В данном случае, по мере обучения самоорганизующейся карты, она теряет способность распознавать аномалии из-за увеличения размера обучающей выборки, о чем и свидетельствуют результаты эксперимента.

Наиболее высокие значения метрик показали модели автокодировщика, гауссовских смесей и обучения с подкреплением. Однако, учитывая сложность модели обучения с подкреплением, для более высокого качества ей требуется больший размер обучающей выборки. Автокодировщик, учитывая его относительную простоту в реализации и в обучении, является лидирующим алгоритмом в решении задачи выявления аномалий в потоковых данных высокой размерности.

Заключение

Классические методы обнаружения аномалий имеют ограниченную область применения из-за необходимости наличия размеченных обучающих данных. В статье рассмотрены алгоритмы, которые позволяют эффективно бороться нехваткой данных и проблемой холодного старта, а также работать с последовательно поступающими данными.

Необходимыми критериями при выборе алгоритмов являлись поддержка онлайн-обучения и возможность прямого или косвенного взаимодействия с оператором.

Каждый из рассмотренных алгоритмов имеет свою область применения, преимущества и недостатки. Например, метод k-ближайших соседей и самоорганизующиеся карты хуже работают с данными высокой размерности, что подтверждается экспериментами. По результатам тестирования выявлено, что наилучшим образом с задачей выявления аномалий в потоковых данных высокой размерности справляются автокодировщики. Также с решением данной задачи хорошо справляются модели гауссовских смесей. Методы обучения с подкреплением также показывают перспективные результаты, однако из-за сложности реализации и обучения модели, а также необходимости большего количества данных для обучения, хуже подходят для решения поставленной задачи.

Стоит также отметить, что разные задачи могут иметь разную специфику, и использование алгоритмов машинного обучения может быть излишним при наличии в исходных данных сильных статистических зависимостей, а при реализации методов для решения задач выявления аномалий, помимо возможностей алгоритма следует также учитывать специфики конкретной задачи и обучающих данных.

Список литературы

1. Bishop C. M., Nasrabadi N. M. Pattern recognition and machine learning. – New York: Springer, 2006. – Т. 4. – №. 4. – С. 338-339.
2. Breiman L. Classification and regression trees. – Routledge, 2017.
3. Breiman L. Random forests //Machine learning. – 2001. – Т. 45. – С. 5-32.
4. Ester M. et al. A density-based algorithm for discovering clusters in large spatial databases with noise //kdd. – 1996. – Т. 96. – №. 34. – С. 226-231.
5. Breunig M. M. et al. LOF: identifying density-based local outliers //Proceedings of the 2000 ACM SIGMOD international conference on Management of data. – 2000. – С. 93-104.
6. Liu F. T., Ting K. M., Zhou Z. H. Isolation forest //2008 eighth ieee international conference on data mining. – IEEE, 2008. – С. 413-422.
7. Schölkopf B. et al. Estimating the support of a high-dimensional distribution //Neural computation. – 2001. – Т. 13. – №. 7. – С. 1443-1471.
8. Reynolds D. A. et al. Gaussian mixture models //Encyclopedia of biometrics. – 2009. – Т. 741. – С. 659-663.
9. Andoni A., Indyk P., Razenshteyn I. Approximate nearest neighbor search in high dimensions //Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018. – 2018. – С. 3287-3318.
10. Crammer K. et al. Online passive-aggressive algorithms //Journal of Machine Learning Research. – 2006. – Т. 7. – №. 3.
11. Neal R. M., Hinton G. E. A view of the EM algorithm that justifies incremental, sparse, and other variants //Learning in graphical models. – Dordrecht : Springer Netherlands, 1998. – С. 355-368.
12. Hulten G., Spencer L., Domingos P. Mining time-changing data streams //Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining. – 2001. – С. 97-106.

13. Zhai J. et al. Autoencoder and its various variants //2018 IEEE international conference on systems, man, and cybernetics (SMC). – IEEE, 2018. – С. 415-419.
14. Kohonen T. Self-organized formation of topologically correct feature maps //Biological cybernetics. – 1982. – Т. 43. – №. 1. – С. 59-69.
15. Sutton R. S., Barto A. G. Reinforcement learning: An introduction. – MIT press, 2018.

References

1. Bishop C. M., Nasrabadi N. M. Pattern recognition and machine learning. – New York: Springer, 2006. – Vol. 4. – No. 4. – pp. 338-339.
 2. Breiman L. Classification and regression trees. – Routledge, 2017.
 3. Breiman L. Random forests //Machine learning. – 2001. – Vol. 45. – pp. 5-32.
 4. Ester M. et al. A density-based algorithm for discovering clusters in large spatial databases with noise //kdd. – 1996. – Vol. 96. – No 34. – pp. 226-231.
 5. Breunig M. M. et al. LOF: identifying density-based local outliers //Proceedings of the 2000 ACM SIGMOD international conference on Management of data. – 2000. – pp. 93-104.
 6. Liu F. T., Ting K. M., Zhou Z. H. Isolation forest //2008 eighth ieee international conference on data mining. – IEEE, 2008. – pp. 413-422.
 7. Schölkopf B. et al. Estimating the support of a high-dimensional distribution //Neural computation. – 2001. – Vol. 13. – No. 7. – pp. 1443-1471.
 8. Reynolds D. A. et al. Gaussian mixture models //Encyclopedia of biometrics. – 2009. – Vol. 741. – pp. 659-663.
 9. Andoni A., Indyk P., Razenshteyn I. Approximate nearest neighbor search in high dimensions //Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018. – 2018. – pp. 3287-3318.
 10. Crammer K. et al. Online passive-aggressive algorithms //Journal of Machine Learning Research. – 2006. – Vol. 7. – No. 3.
 11. Neal R. M., Hinton G. E. A view of the EM algorithm that justifies incremental, sparse, and other variants //Learning in graphical models. – Dordrecht : Springer Netherlands, 1998. – pp. 355-368.
 12. Hulten G., Spencer L., Domingos P. Mining time-changing data streams //Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining. – 2001. – pp. 97-106.
 13. Zhai J. et al. Autoencoder and its various variants //2018 IEEE international conference on systems, man, and cybernetics (SMC). – IEEE, 2018. – pp. 415-419.
 14. Kohonen T. Self-organized formation of topologically correct feature maps //Biological cybernetics. – 1982. – Vol. 43. – No. 1. – pp. 59-69.
 15. Sutton R. S., Barto A. G. Reinforcement learning: An introduction. – MIT press, 2018.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.42

ИСПОЛЬЗОВАНИЕ ANTLR ДЛЯ АНАЛИЗА МЕТРИК ХОЛСТЕДА В ЯЗЫКАХ PYTHON И BML

Храпов А.А.

ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: khrapov@bk.ru

В данной статье рассматривается использование ANTLR (Another Tool for Language Recognition) для анализа исходного кода, написанного на языках Python и BML (BlockSet Modeling Language), с целью автоматизированного подсчета метрик Холстеда. Описан процесс создания грамматик для языков Python и BML и использования ANTLR для генерации парсеров, которые позволяют построить синтаксическое дерево. На основании этого дерева производится автоматизированный подсчет операторов и операндов, необходимых для вычисления ключевых метрик. В статье приводятся примеры реализации на языке Python, а также выделено преимущество автоматизации подсчета метрик в сравнении с ручным подходом. Применение ANTLR обеспечивает точность и стандартизацию анализа исходного кода программы, что особенно важно для оценки эффективности различных инструментов разработки веб-приложений. Проведенное исследование демонстрирует, как можно использовать синтаксический анализатор для объективного сравнения языков Python и BML, измерения сложности и объема кода.

Ключевые слова: ANTLR, метрики Холстеда, синтаксический анализ, Python, BML, Django.

USING ANTLR TO ANALYZE HALSTED METRICS IN PYTHON AND BML LANGUAGES

Khrapov A.A.

MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: khrapov@bk.ru

This article provides an overview of the most popular open source relational database management systems (DBMS), such as MySQL, PostgreSQL, MariaDB and SQLite. It covers the key aspects that distinguish these DBMS, including architecture, installation complexity, extensibility, performance monitoring, and ease of learning. The benchmarking also includes performance, compatibility, data backup and recovery capabilities, as well as support levels for ACID transactions and data integrity.

Keywords: ANTLR, Halstead metrics, parsing, Python, BML, Django.

Разработка веб-приложений требует не только создания функциональности, но и анализа эффективности используемых инструментов. Метрики Холстеда позволяют измерить сложность кода, его объем, временную нагрузку и другие характеристики [4]. Однако ручной подсчет метрик затруднителен, особенно для крупных проектов. Для автоматизации этого процесса можно использовать ANTLR (Another Tool for Language Recognition).

ANTLR – это библиотека, являющаяся мощным инструментом для описания грамматик языков и генерации кода для их синтаксического анализа [1]. В данной работе

рассматривается, как ANTLR может быть применен для анализа языков Python и BML (BlockSet), а также для автоматизированного подсчета метрик Холстеда.

Начнём с построения грамматики для высокоуровневого языка программирования Python [2]. Она включает лексические и синтаксические правила для идентификаторов, операторов и выражений. Одна из вариаций грамматики может выглядеть следующим образом:

```
grammar Python;
program: statement+;
statement: assignment | expression;
assignment: IDENTIFIER '=' expression;
expression: NUMBER | IDENTIFIER | '(' expression ')';
IDENTIFIER: [a-zA-Z_][a-zA-Z0-9_]*;
NUMBER: [0-9]+;
WHITESPACE: [ \t\r\n]+ -> skip;
```

Данная грамматика описывает простые операторы присваивания и некоторые выражения, что достаточно для демонстрации подсчета базовых метрик. В дальнейшем в грамматику будут включены более сложные конструкции языка, такие как условные операторы, циклы и вызовы функций.

Далее перейдём к построению грамматики для BML, который используется в BlockSet для декларативного описания данных и логики [3]. Она может быть описана так:

```
grammar BML;
model: '<model>' set+ '</model>';
set: '<set' 'name' '=' ''' IDENTIFIER ''' '>' block* '</set>';
block: '<block' 'name' '=' ''' IDENTIFIER ''' 'type' '=' ''' IDENTIFIER ''' '/>';
IDENTIFIER: [a-zA-Z_][a-zA-Z0-9_]*;
WHITESPACE: [ \t\r\n]+ -> skip;
```

Эта грамматика позволяет анализировать иерархическую структуру BML и извлекать информацию для подсчета метрик. В отличие от Python, структура BML более предсказуема и декларативна, что облегчает построение грамматики.

Для генерации парсеров ANTLR используются команды «antlr4 -Dlanguage=Python3 Python.g4» и «antlr4 -Dlanguage=Python3 BML.g4» [1].

Это создаст Python-классы для обработки синтаксического дерева, включая классы парсера и посетителя (Visitor). Сгенерированные парсеры способны преобразовывать исходный код в синтаксическое дерево, которое затем можно обрабатывать для извлечения операторов и операндов.

Сгенерированный код используется для обхода дерева синтаксиса. Его необходимо расширить логикой подсчета операторов и операндов (рисунок 1).

```
from PythonParser import PythonParser
from PythonVisitor import PythonVisitor

class HalsteadMetricsVisitor(PythonVisitor):
    def __init__(self):
        self.operators = set()
        self.operands = set()
        self.operator_count = 0
        self.operand_count = 0

    def visitAssignment(self, ctx):
        self.operators.add('=')
        self.operator_count += 1
        self.visit(ctx.expression())
        return None

    def visitExpression(self, ctx):
        if ctx.NUMBER():
            self.operands.add(ctx.NUMBER().getText())
            self.operand_count += 1
        elif ctx.IDENTIFIER():
            self.operands.add(ctx.IDENTIFIER().getText())
            self.operand_count += 1
        return self.visitChildren(ctx)
```

Рисунок 1 – Расширения класса для подсчёта операторов и операндов Python кода
Аналогичный класс можно создать и для BML (рисунок 2).

```
from BMLParser import BMLParser
from BMLVisitor import BMLVisitor

class HalsteadMetricsBMLVisitor(BMLVisitor):
    def __init__(self):
        self.operators = set()
        self.operands = set()
        self.operator_count = 0
        self.operand_count = 0

    def visitModel(self, ctx):
        self.operators.add('<model>')
        self.operators.add('</model>')
        self.operator_count += 2
        return self.visitChildren(ctx)

    def visitSet(self, ctx):
        self.operators.add('<set>')
        self.operators.add('</set>')
        self.operator_count += 2

        name = ctx.getChild(3).getText()
        self.operands.add(name)
        self.operand_count += 1
        return self.visitChildren(ctx)

    def visitBlock(self, ctx):
        self.operators.add('<block>')
        self.operator_count += 1

        name = ctx.getChild(3).getText()
        block_type = ctx.getChild(7).getText()
        self.operands.add(name)
        self.operands.add(block_type)
        self.operand_count += 2

        return self.visitChildren(ctx)
```

Рисунок 2 – Расширения класса для подсчёта операторов и операндов BML кода

В итоге, применение ANTLR позволит автоматически подсчитать метрики Холстеда, такие как:

- n_1 (уникальные операторы);
- n_2 (уникальные операнды);
- N_1 (общее количество операторов);
- N_2 (общее количество операндов);
- n (словарь программы);
- N (длина кода);
- Объем программы (V) и сложность (D) [4].

Для корректного подсчёта для языка Python выбран фреймворк Django – это высокоуровневый веб-фреймворк, который позволяет быстро создавать безопасные и поддерживаемые веб-приложения [5].

Например, для фрагмента Python-кода на Django (Рисунок 3) результатом подсчёта будут: $n_1 = 7$ («def», «=», «.», «()», «{ }», «:»); $n_2 = 3$ (request, random_game, Game и т.д.); $N_1 = 20$; $N_2 = 30$; $n = 23$, $N = 50$, $V \approx 226$; $D \approx 6,56$.

```
def home(request):
    random_game = Game.objects.order_by('?').first()
    top_games = Game.objects.order_by('-user_rating')[:10]
    recent_games = Game.objects.order_by('-id')[:10]
    return render(request, 'games/home.html', {
        'random_game': random_game,
        'top_games': top_games,
        'recent_games': recent_games,
    })
```

Рисунок 3 – фрагмент кода программы на Django

Для BML фрагмента (Рисунок 4) подсчитаны свои показатели: $n_1 = 5$ («model», «set», «block», «/set», «/model»); $n_2 = 6$ (games, top_game и т.д.); $N_1 = 7$; $N_2 = 6$; $n = 11$, $N = 13$, $V \approx 45$; $D \approx 2,5$.

```
<model>
  <set name="games">
    <block name="random_game" type="object" />
    <block name="top_games" type="list" />
    <block name="recent_games" type="list" />
  </set>
</model>
```

Рисунок 4 – фрагмент кода BML

Данные примеры ещё не являются полноценным веб-приложением, это лишь фрагменты, но уже можно сделать некоторые выводы:

- У BML декларативная структура, следовательно, меньший словарный запас языка;
- Вероятнее, более низкие объём и сложность кода по сравнению с Django (Python).

В заключение, можно отметить, что применение ANTLR позволит автоматизировать подсчет метрик Холстеда для различных языков, в данном случае для Python и BML. Это снизит нагрузку на разработчиков и обеспечит более высокую точность при анализе кода.

Результаты подсчета демонстрируют, как можно организовать процесс анализа кода и объективно оценить эффективность разработки с использованием разных инструментов.

Список литературы

1. Документация ANTLR. [Электронный ресурс] URL: <https://www.antlr.org/>. (дата обращения 09.12.2024).
2. Документация Python. [Электронный ресурс] URL: <https://docs.python.org> (дата обращения 10.12.2024).
3. Предпосылки формирования новой методологии разработки веб-узлов BlockSet и декларативного языка BML. Кейно П.П. [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/predposylki-formirovaniya-novoy-metodologii-razrabotki-veb-uzlov-blockset-i-deklarativnogo-yazyka-bml/viewer> (дата обращения 10.12.2024).
4. Программные показатели Холстеда – Разработка программного обеспечения. [Электронный ресурс] URL: <https://www.geeksforgeeks.org/software-engineering-halsteads-software-metrics/> (дата обращения 12.12.2024).

5. Django веб-фреймворк (Python). [Электронный ресурс] URL: <https://developer.mozilla.org/ru/docs/Learn/Server-side/Django/Introduction> (дата обращения 10.12.2024).

References

1. Documentation of ANTLR. [Electronic resource] URL: <https://www.antlr.org/> (accessed 09.12.2024).
 2. Documentation of Python. [Electronic resource] URL: <https://docs.python.org> (accessed 10.12.2024).
 3. Prerequisites for the formation of a new development methodology BlockSet and declarative BML language. P.P.Keyno. [Electronic resource] URL: <https://cyberleninka.ru/article/n/predposylki-formirovaniya-novoy-metodologii-razrabotki-veb-uzlov-blockset-i-deklarativnogo-yazyka-bml/viewer> (accessed 12.12.2024).
 4. Halstead's Software Metrics – Software Engineering. [Electronic resource] URL: <https://www.geeksforgeeks.org/software-engineering-halsteads-software-metrics/> (accessed 10.12.2024).
 5. Django web-framework (Python). [Electronic resource] URL: <https://developer.mozilla.org/ru/docs/Learn/Server-side/Django/Introduction> (accessed 10.12.2024).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

ОБЗОР БАНКОВСКОГО ПРОЦЕССА ПО УПРАВЛЕНИЮ ПРОБЛЕМНЫМИ ПРОЕКТАМИ НА ПЛАТФОРМЕ GREENDATA

¹ Иванова Н.А., ² Смоленцева Т.Е.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ¹ inadezda2003@gmail.com, ² smolenceva@mirea.ru

За стремительно развивающимся миром стоят не менее активные люди, владельцы малых, средних и крупных предприятий. Для развития бизнеса ряд управленцев обращаются в банк за финансовой помощью, однако не все заемщики могут оптимально оценить риски, и вследствие чего стать финансово неблагополучными заемщиками для банка. В данной статье рассмотрен способ обработки проблемных проектов в контексте процесса по изменению статуса проекта в банковской системе.

Ключевые слова: Признание проекта проблемным, разработка стратегии, прекращение признания проекта проблемным, BPMS, GreenData, показатель проблемности, изменение статуса проекта.

OVERVIEW OF THE BANKING PROCESS FOR MANAGING PROBLEMATIC PROJECTS ON THE GREEN DATA PLATFORM

¹ Ivanova N.A., ² Smolentseva T.E.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹ inadezda2003@gmail.com, ² smolenceva@mirea.ru

Behind the rapidly developing world there are no less active people, owners of small, medium and large enterprises. For business development, a number of managers apply to the bank for financial assistance, but not all borrowers can optimally assess the risks, and as a result become financially disadvantaged borrowers for the bank. This article discusses the method of processing problematic projects in the context of the process of changing the status of a project in the banking system.

Keywords: Recognition of the project as problematic, development of a strategy, termination of recognition of the project as problematic, BPMS, GreenData, indicator of problematic, change in the status of the project.

Банковские процессы обширны, особенно если дело касается работы с клиентами. В данной статье будут рассмотрены процессы, связанные с управлением проблемными проектами. А именно, с чего начинается процесс признания проекта проблемным и какие меры предпринимаются для его оздоровления.

Начнём с определения проблемного проекта — это проблемные активы, сделки и задачи, объединенные в один проект. Актив считается проблемным, если его контрагенты являются заемщиками, которые постоянно или периодически не выполняют обязательства перед банком [1]. Признание проекта проблемным начинается с заведения по нему задачи сотрудником блока аудита. Предварительный аудит и анализ проекта позволяют определить его категорию, а именно выявить, относится ли он к проблемным проектам. Если признак подтверждается,

запускается процесс по признанию проекта проблемным. В ином случае, при положительном аудите проекта, он не меняет свою категорию.

Далее по процессу проект переходит в подразделение активов, где начинается основной процесс подразделения — разработка стратегии по работе с проблемным активом (далее Стратегия). Стратегия утверждает план мероприятий, позволяющих вывести проект из проблемной зоны с целью оздоровления и продолжения сотрудничества или возврата задолженности банку, путем банкротства должника или взыскания его имущества для частичной компенсации долгов заемщика.

После успешной разработки стратегии и реализации плана мероприятий, утвержденных для оздоровления или взыскания задолженности по проекту, начинается процесс прекращения признания проекта проблемным. В процессе менеджер проекта снимает показатель проблемности, завершает стратегию, то есть переводит её в состояние «Завершено» и возвращает проект в блок, из которого он был передан в подразделение активов.

Рассматривая программную реализацию сложного банковского процесса, остановимся на решении GreenData компании ООО «Гриндата» — разработчике отечественной BPMS-системы (Business Process Management System) — программного обеспечения для поддержки концепции BPM и управления бизнес-процессами, позволяющего автоматизировать любые банковские процессы под ключ [2][3]. Стоит отметить, что в наше время BPMS-системы являются неотъемлемой частью экосистемы большинства крупных банков [4]. Платформа GreenData имеет ряд шаблонных решений, которые могут быть доработаны под нужды определенной компании. Описанный выше процесс реализован при помощи средств платформы и для упрощения понимания сокращен до основных подпроцессов, участвующих в «Изменении статуса проекта» (Рисунок 1). BPMS-система поддерживает разработку бизнес-процессов в нотации BPMN (Business Process Model and Notation) — это система условных обозначений и их описания для моделирования бизнес-процессов [5].

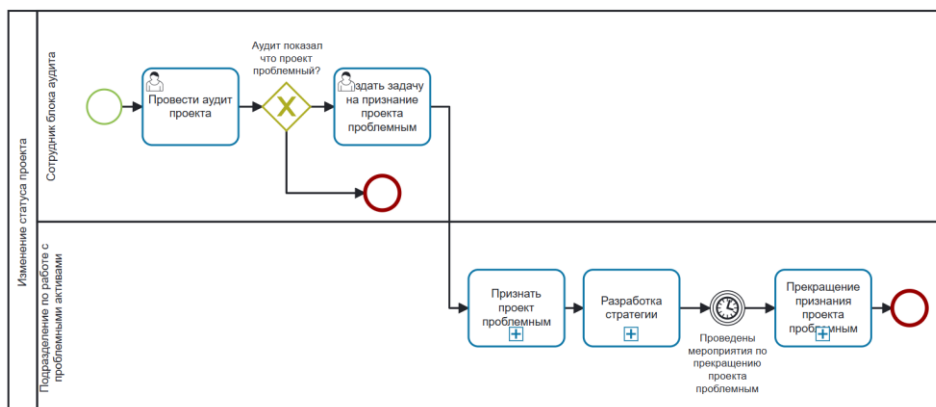


Рисунок 1 — Процесс «Изменение статуса проекта»

В подпроцессах раскрывается подробная логика по изменению статуса проекта, включающая сложные и многопользовательские функции, связанные между собой логической цепочкой. Текущая технология выполнения процесса использует платформу исключительно как систему для внесения изменений и фиксации этапов выполнения процесса. Однако инструменты BPMS-системы позволяют автоматизировать процессы таким образом, что менеджер проекта будет принимать только ключевые решения по процессу, например,

подтверждение признания проекта проблемным, создание стратегии или прекращение признания проекта проблемным. Он сможет влиять только на то, по какому условию пойдет процесс, все остальные нюансы платформа будет реализовывать автоматически при помощи алгоритмов и функций — это позволит минимизировать ошибки, связанные с человеческим фактором.

Анализ показал, что можно создать модуль для процесса «Изменения статуса проекта», который будет включать в себя управление проблемными проектами, а в частности реализацию процесса по прекращению признания проектов проблемными. Функционал системы GreenData открывает возможности для автоматизации системы и настройки процессов для удобной и эффективной работы пользователей.

Список литературы

1. Проблемный заемщик. Кого банки считают клиентами с повышенным риском [Электронный ресурс] – URL: <https://dzen.ru/a/XO5sjg2KxQCuRv7W> (дата обращения 26.11.2024)
2. GreenData. О компании. [Электронный ресурс] – URL: <https://greendata.store/company/> (дата обращения 26.11.2024)
3. Comindware. Что такое BPMS? [Электронный ресурс] – URL: <https://www.comindware.ru/blog/bpm-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B/> (дата обращения 26.11.2024)
4. Соловей, П.С. Место low-code платформ в цифровой экосистеме коммерческого банка / П.С. Соловей, Х.И. Аминов // Экосистема цифровой экономики : сборник статей / под ред. И.Л. Коршунова. – СПб.: Изд-во СПбГЭУ, 2021. – С. 33-39. (дата обращения 26.11.2024)
5. BPMN. [Электронный ресурс] – URL: <https://ru.wikipedia.org/wiki/BPMN> (дата обращения 26.11.2024)

References

1. A troubled borrower. Whose banks take into account high-risk customers [Electronic resource] - URL: <https://dzen.ru/a/XO5sjg2KxQCuRv7W> (accessed 26.11.2024)
 2. GreenData. About the company. [Electronic resource] - URL: <https://greendata.no.store/company/> (accessed 26.11.2024)
 3. Comindware. What is BPMS? [Electronic resource] - URL: <https://www.comindware.ru/blog/bpm-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B/> (accessed 26.11.2024)
 4. Solovey, P.S. The place of low-code platforms in the digital ecosystem of a commercial bank / P.S. Solovey, H.I. Aminov // The ecosystem of the digital economy : a collection of articles / edited by I.L. Korshunov. – St. Petersburg: Publishing House of Spbsetu, 2021. – pp. 33-39. (accessed 26.11.2024).
 5. BPMN. [Electronic resource] - URL: <https://ru.wikipedia.org/wiki/BPMN> (accessed 26.11.2024).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.942

РОБОТОТЕХНИКА В МЕДИЦИНЕ

¹ Мадатов Д.А., ² Борисов В.В., ³ Сивков В.С.

ФГБОУ ВО «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ», г. Самара, Россия (443010, г. Самара ул. Льва
Толстого, 23), e-mail: ¹ dima.madatov.2015@mail.ru, ² v.borisov@psuti.ru, ³ v.sivkov@psuti.ru

В этой статье рассматривается быстрое развитие и применение робототехники в медицине. В ней рассматриваются различные применения медицинских роботов: от хирургии и диагностики до реабилитации, на конкретных примерах. В статье также рассматриваются ключевые проблемы, связанные с интеграцией робототехники в здравоохранение, включая высокие затраты, проблемы безопасности, трудности с интеграцией в существующую инфраструктуру и этические соображения. Анализ потенциальных препятствий и возможных способов их преодоления помогает оценить перспективы развития медицинской робототехники и ее влияние на будущее здравоохранения.

Ключевые слова: Робототехника, искусственный интеллект, медицина, хирургия, реабилитация, роботы.

ROBOTICS IN MEDICINE

¹ Madatov D.A., ² Borisov V.V., ³ Sivkov V.S.

VOLGA REGION STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS,
Samara, Russia (443010, Samara st. Lev Tolstoy, 23), e-mail: ¹ dima.madatov.2015@mail.ru,
² v.borisov@psuti.ru, ³ v.sivkov@psuti.ru

This article examines the rapid development and application of robotics in medicine. It examines various applications of medical robots, from surgery and diagnostics to rehabilitation, using specific examples. The article also addresses key challenges associated with integrating robotics into healthcare, including high costs, security concerns, difficulties with integration into existing infrastructure, and ethical considerations. Analyzing potential obstacles and possible ways to overcome them helps assess the prospects for the development of medical robotics and its impact on the future of healthcare.

Keywords: Robotics, artificial intelligence, medicine, surgery, rehabilitation, robots.

Робототехника трансформирует современную медицину, предоставляя инновационные решения для диагностики, лечения и реабилитации пациентов. От минимально инвазивной хирургии до точной доставки лекарств и индивидуальной реабилитации – роботы открывают новые горизонты для улучшения качества медицинской помощи и повышения эффективности медицинских процедур. В этой статье мы рассмотрим область применения медицинских роботов на конкретных примерах. Однако, несмотря на впечатляющий потенциал, внедрение робототехники в медицину сопряжено с некоторыми серьезными проблемами, включая высокие затраты, проблемы безопасности и трудности интеграции. Мы более подробно рассмотрим эти ключевые проблемы и обсудим возможные пути для их решения.

Робототехника быстро изменяет сферу здравоохранения, предлагая новые возможности в диагностике, лечении и реабилитации пациентов. Рассмотрим некоторые варианты применения робототехники в медицине:

Хирургия. Робототехника в хирургии открывает множество новых возможностей, позволяя хирургам выполнять сложнейшие и точнейшие операции. Часть из этих возможностей мы рассмотрим дальше. Роботы, благодаря своей конструкции, могут выполнять высокоточные движения, которые человеку будет крайне сложно повторить. Благодаря этому преимуществу хирурги могут выполнять более деликатные операции, так как робот будет более точно позиционировать инструменты. С помощью роботов хирурги могут выполнять операции, не прибегая к большим разрезам, что в свою очередь снизит травмирование тканей, кровопотерю, время восстановления пациента и шанс появления рубцов. Конструкция роботов позволяет размещать в них высококачественные 3D-камеры, наличие этих камер предоставляет хирургам широкий и улучшенный обзор операционного поля, что соответственно позволяет увидеть те детали, которые невооруженному глазу трудно заметить. Манипуляторы роботов обладают большой гибкостью и отличным диапазоном движений, в следствии чего манипуляторам проще добраться до труднодоступны мест в теле человека. Часть роботов предоставляет доступ к дистанционным операциям. Данная особенность полезна, в случае необходимости важны операций в отдаленных местах или же при чрезвычайных ситуациях.

Самым ярким примером подобных роботов является хирургическая система da Vinci[1]. Она используется в различных хирургических областях, включая кардиохирургию, урологию, гинекологию и общую хирургию. Хирург управляет роботом с панели управления и просматривает операционное поле на большом экране.



Рисунок 1 - Хирургическая система da Vinci

Источник: изображение с сайта компании Intuitive

Реабилитация. Для реабилитации робототехника играет не менее важную роль. Она предлагает инновационные решения для восстановления функций поврежденных частей тела после травм, инсультов, нейродегенеративных заболеваний и т.д... Роботы ускорят процесс

реабилитации и сделаю его более эффективным. Ряд особенностей данного применения роботов рассмотрим далее. В контексте данного вида реабилитации подразумевается использование экзоскелетов. Это роботизированные устройства, которые крепятся к поврежденным конечностям помогая пациенту двигаться. Они даруют дополнительную устойчивость, помогают в движении и также могут адаптироваться к силе и диапазону движений больного. Такие устройства помогают в восстановлении мелкой моторики конечности, которая необходима нам для выполнения повседневных задач. Различные модель роботов оснащены по-разному, некоторые предоставляют реабилитацию в виде игры и интерактивных упражнений, другие автоматически «разминают» конечность. Устройства подобного типа тренируют память, внимательность и прочие когнитивные функции пациента. Тренировки когнитивных функций необходимы в случае повреждения их из-за инсульта и других заболеваний, наносящих урон нервной системе. Также в тренировках могут использоваться разные интерактивные элементы, для повышения мотивации пациента.

В качестве примера можно привести устройства серии LokomatPro[2]. Это полноценный роботизированный комплекс, моделирующий и воспроизводящий естественную походку человека, что благодаря объективной обратной связи и активному участию пациента приводит к активации сенсомоторной сети мозга, отвечающей за ходьбу.



Рисунок 2 - Роботизированный комплекс LokomatPro
Источник: изображение с сайта компании Бека РУС

Диагностика и лечение. Робототехника не оставила сферу диагностики и лечения без революций. Во многих областях медицины роботы предоставляют более точные, эффективные и менее инвазивные методы. Теперь рассмотрим способы их применений и их особенности. Роботы способны более точно забирать образцы тканей для биопсии, данная особенность очень важна в труднодоступных местах, так как человеку может не хватить места и гибкости для правильного забора. Также роботы позволяют хирургам получать более качественные образцы опухолей, минимизируя общее повреждение окружающих опухоль

тканей. Благодаря искусственному интеллекту, интегрированному в систему, можно с высокой точностью разбирать медицинские изображения (рентген, КТ, МРТ), в следствие чего подобный анализ может выявить те заболевания, которые невооруженный глаз человека мог бы не заметить. Роботы могут использоваться с целью доставки лечебных средств прямо в организм пациента, подобное необходимо при целевой терапии рака, а также благодаря этому можно минимизировать побочные эффекты и повысить эффективность лечения. Также сейчас ведутся исследования в области микророботов, с целью их использования для доставки лекарств непосредственно к опухолевым клеткам.

Хорошим примером является CyberKnife[3]. Это система, представляющая собой неинвазивное лечения раковых и неракковых опухолей, а также других состояний, требующих лучевой терапии. Она доставляет радиацию при помощи линейного ускорителя, который установлен непосредственно на роботе.



Рисунок 3 - Система CyberKnife

Источник: изображение с сайта компании Accuray

Робототехника обещает произвести революцию в здравоохранении, открыв новые возможности в диагностике, лечении и реабилитации. Однако путь к широкому внедрению медицинских роботов полон трудностей. Например, есть три довольно значимые проблемы:

- **Стоимость.** Высокая стоимость внедрения робототехники в медицине – сложный вопрос, включающий не только первоначальные затраты на приобретение дорогостоящего оборудования, но и многие сопутствующие расходы, которые часто недооцениваются. Например, первоначальная покупка роботизированных хирургических систем может стоить миллионы долларов, что не все могут себе позволить, особенно небольшие больницы.

Добавьте к этому значительные затраты на обслуживание и ремонт, для которых требуются высококвалифицированные специалисты и дорогие запасные части. Простой оборудования из-за отказа может привести к финансовым потерям, снижению операционной эффективности и задержкам в оказании помощи пациентам. Обучение медицинского персонала работе с новыми технологиями — длительный и дорогостоящий процесс, требующий специальных курсов, тренингов и симуляций. Наконец, продолжающиеся инвестиции в исследования и разработки, необходимые для улучшения существующих технологий и создания новых, также являются важным фактором, который увеличивает общую стоимость внедрения робототехники в медицине. В конечном итоге все эти факторы означают, что доступ к передовым роботизированным технологиям в здравоохранении остается ограниченным, несмотря на их огромный потенциал.

- **Безопасность.** Безопасность роботов в медицине — довольно сложная и многогранная проблема. Риски связаны не только с техническими аспектами, но также с человеческим фактором и этическими соображениями. С технической точки зрения потенциальные механические неисправности, такие как отказ двигателя, заклинивание механизмов или поломка датчиков, представляют собой угрозу, которая может привести к неожиданному движению робота во время операции, что может нанести вред пациенту. Проблемы с программным обеспечением, вызванные ошибками или вирусами, могут привести к неверным командам, неправильной интерпретации данных датчиков и потере управления роботом. Недостаточная надежность электросистемы также создает риски, поскольку внезапное отключение электроэнергии может нарушить критически важный процесс. Не менее важную роль играет человеческий фактор: неквалифицированный или плохо обученный персонал может неправильно использовать систему, не замечать предупреждающие знаки или допускать ошибки в настройке. Усталость хирурга и стресс во время длительной хирургической процедуры также могут увеличить риск ошибок. Кроме того, кибербезопасность становится все более важной проблемой, поскольку подключенные к сети медицинские роботы могут стать мишенью для хакеров, что может привести к удаленному управлению роботами или краже данных пациентов. Внедрение робототехники в медицину также поднимает ряд этических вопросов, таких как распределение ответственности в случае несчастного случая и риск увеличения неравенства в здравоохранении. Поэтому обеспечение безопасности роботизированных систем в медицине требует не только разработки надежного и отказоустойчивого аппаратного и программного обеспечения, но и подготовки медицинского персонала на высоком уровне, строгих мер безопасности, эффективных систем мониторинга и регулярного технического обслуживания. Необходимо также решить этические вопросы и обеспечить кибербезопасность медицинских роботов.

- **Интеграция в инфраструктуру.** Успешная интеграция робототехники в медицинскую инфраструктуру — задача, требующая решения множества взаимосвязанных проблем. На физическом уровне существующие здания больниц и клиник зачастую не оборудованы для размещения и эксплуатации крупных роботизированных систем. Это может потребовать дорогостоящей реконструкции помещений, установки новых систем связи, установки мощных источников питания и систем аварийного электроснабжения, а также введения дополнительных мер безопасности для предотвращения аварий. Также существует необходимость обеспечить надежную высокоскоростную сетевую инфраструктуру для удаленной связи и управления роботами, что может быть особенно сложно в старых зданиях

с устаревшими кабелями. Кроме того, интеграция робототехники в существующие информационные системы здравоохранения и другие программные приложения требует значительных усилий и затрат на разработку и адаптацию программного обеспечения, обеспечение совместимости и создание единой интегрированной системы. Организационные аспекты также создают серьезные проблемы. Медицинские работники должны пройти специальную подготовку для использования новых технологий, что требует времени, ресурсов и может быть дорогостоящим. Использование роботов может также потребовать внесения изменений в существующие медицинские процедуры и протоколы, которые должны быть согласованы всеми участниками процесса. Отсутствие единых стандартов и правил в секторе медицинской робототехники создает дополнительные проблемы. В конечном итоге решающую роль играют экономические соображения. Высокая стоимость приобретения, обслуживания и ремонта роботов, а также отсутствие четкой окупаемости инвестиций могут ограничить внедрение роботов, особенно в контексте ограниченных бюджетов здравоохранения. Поэтому успешная интеграция робототехники требует тщательного планирования, комплексного подхода, значительных финансовых инвестиций и решения всех вышеупомянутых проблем на ранней стадии.

Мы рассмотрели некоторые успешные примеры применения робототехники, демонстрирующие преимущества повышения точности, эффективности и безопасности медицинских процедур. Однако высокие затраты, проблемы безопасности, трудности интеграции и этические дилеммы требуют тщательного внимания и решения. Успешное внедрение медицинских роботов требует сотрудничества между производителями, поставщиками медицинских услуг, регулирующими органами и исследовательскими организациями для снижения затрат, повышения безопасности, разработки стандартов и решения этических вопросов. Только комплексный подход позволит в полной мере раскрыть потенциал медицинских роботов и сделать передовые технологии доступными для всех, кто в них нуждается.

Список литературы

1. Intuitive da Vinci. Электронный ресурс. URL: [<https://www.intuitive.com/en-us/products-and-services/da-vinci>] (дата обращения: 16.12.2024).
2. LokomatPro. Электронный ресурс. URL: [<https://beka.ru/katalog/mekhano-i-robotizirovannaya-terapiya/vosstanovlenie-navykov-khodby/lokomat-pro/>] (дата обращения: 16.12.2024).
3. CYBERKNIFE SYSTEM How It Works. Электронный ресурс. URL: [<https://cyberknife.com/cyberknife-how-it-works/>] (дата обращения: 16.12.2024).
4. Современная робототехника в медицине. Электронный ресурс. URL: [<https://robot-davinci.ru/nauchnye-publikacii/sovremennaya-robototekhnika-v-medicine/>] (дата обращения: 16.12.2024).

References

1. Intuitive da Vinci. Electronic resource. URL: [<https://www.intuitive.com/en-us/products-and-services/da-vinci>] (date of access: 12/16/2024).

2. Lokomotivpro. Electronic resource. URL: [<https://beka.ru/katalog/mekhano-i-robotizirovannaya-terapiya/vosstanovlenie-navykov-khodby/lokomat-pro/>] (accessed: 12/16/2024).
 3. CYBERKNIFE SYSTEM How It Works. Electronic resource. URL: [<https://cyberknife.com/cyberknife-how-it-works/>] (accessed: 12/16/2024).
 4. Modern robotics in medicine. Electronic resource. URL: [<https://robot-davinci.ru/nauchnye-publikacii/sovremennaya-robototekhnika-v-medicine/>] (accessed: 12/16/2024).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.4

ВВЕДЕНИЕ АДАПТИВНОГО ОКНА ПОСТРОЕНИЯ ГРАФИКА БАЗОВОЙ НАГРУЗКИ В РАСЧЕТАХ ПО ОПРЕДЕЛЕНИЮ ОБЪЕМА СНИЖЕНИЯ ЭЛЕКТРОПОТРЕБЛЕНИЯ

Ворожейкин Д.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: danilvda@gmail.com

В данной работе рассматривается задача повышения качества прогнозирования электропотребления при определении объемов снижения потребления в условиях событий по управлению спросом с использованием адаптивного окна графика базовой нагрузки (ГБН). Исследование показывает, что оптимальный размер окна варьируется в зависимости от отрасли, а его адаптивный выбор снижает ошибку прогнозирования. Для оценки эффективности подхода использовались метрики MAPE и статистические методы. Разработаны рекомендации по интеграции предложенного метода в существующие информационные системы.

Ключевые слова: Управление спросом, прогнозирование потребления, ГБН, адаптивное окно, асинхронные вычисления, микросервисная архитектура.

INTRODUCING OF AN ADAPTIVE WINDOW FOR BUILDING THE BASE LOAD SCHEDULE IN CALCULATIONS TO DETERMINE THE AMOUNT OF POWER CONSUMPTION REDUCTION

Vorozheikin D.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: danilvda@gmail.com

This paper considers the problem of improving the quality of electricity consumption forecasting in determining the amount of consumption reduction under demand management events using an adaptive baseload schedule window. The study shows that the optimal window size varies from industry to industry and its adaptive selection reduces the forecasting error. MAPE metrics and statistical methods were used to evaluate the performance of the approach. Recommendations for integrating the proposed method into existing information systems were developed.

Keywords: Demand response, consumption forecasting, consumption baseline, adaptive window, asynchronous computing, microservice architecture.

Введение

В последние годы управление спросом на электроэнергию стало важным инструментом для повышения стабильности и эффективности энергосистем. Этот механизм обеспечивает баланс между производством и потреблением электроэнергии, стимулируя конечных потребителей временно снижать свою активность, к примеру останавливать производство основной продукции, в обмен на оплату оказанных услуг. Снижение потребления в периоды высоких оптовых цен или при перегрузке энергосистемы помогает избежать пиковых нагрузок и минимизировать затраты на производство электроэнергии [1].

Целью исследования является разработка и внедрение подхода с адаптивным окном ГБН для повышения точности прогнозирования объема снижения потребления электроэнергии при определении объема снижения потребления в рамках событий управления спросом.

Определение объема снижения потребления

Одной из задач, решаемой в деловом процессе управления спросом, является определение объема снижения потребления электроэнергии в заданные часы. В классическом подходе для определения объема снижения выполняется сравнение фактической нагрузки энергопринимающего устройства с плановой нагрузкой, которая имела бы место при отсутствии рассматриваемого снижения [2]. Это позволяет вычислить разницу и определить объём разгрузки. Пример сравнения фактического и планового потребления энергии представлен на Рисунке 1.

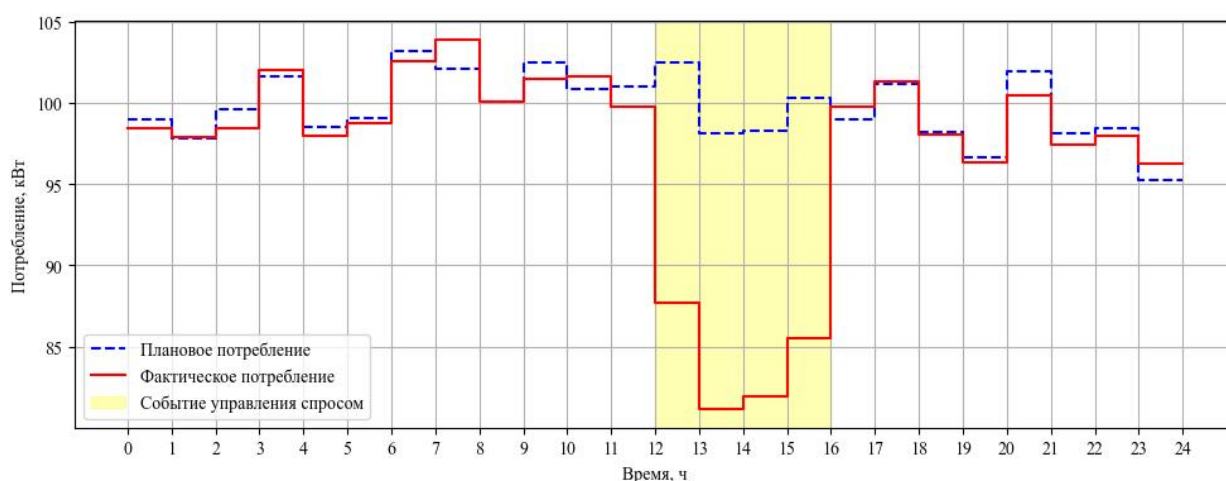


Рисунок 1 – Сравнение фактического и планового потребления энергии

Среди классических подходов можно выделить:

- график базовой нагрузки (ГБН),
- заявленный график нагрузки (ЗГН),
- максимальная базовая нагрузка (МБН).

Метод ГБН основывается на данных потребления за последние рабочие дни за исключением дней, которые не могут попасть в окно. Расчет ГБН осуществляется на основе средних значений потребления для каждого часа. Формула для расчета ГБН выглядит следующим образом:

$$\text{ГБН}(t) = \frac{1}{N} \sum_{i=1}^N P_i(t)$$

где:

- N – количество дней,
- $P_i(t)$ – потребление в час t на i -ый день.

ЗГН формируется самим потребителем и основывается на его предположениях о будущем электропотреблении в определенные периоды времени.

МБН используется для прогнозирования на основе наиболее высоких значений потребления за прошлые периоды.

Минусы этих подходов:

- ГБН может демонстрировать недостаточную адаптивность при использовании фиксированных параметров в расчёте, таких как размер окна, поскольку одинаковый подход для всех потребителей не учитывает индивидуальные особенности их характера потребления, что снижает точность прогнозов,
- ЗГН зависит от субъективной оценки потребителя и требует введения дополнительных проверок незаывшения графика в дни событий,
- МБН также требует введение дополнительных проверок.

Основным методом является ГБН из-за его простоты, понятности и устойчивости к манипулированию [2]. Опираясь на международный опыт, в качестве размера окна для расчётов ГБН обычно используют 10 дней [3].

Визуализация примера расчёта ГБН представлена на Рисунке 2.

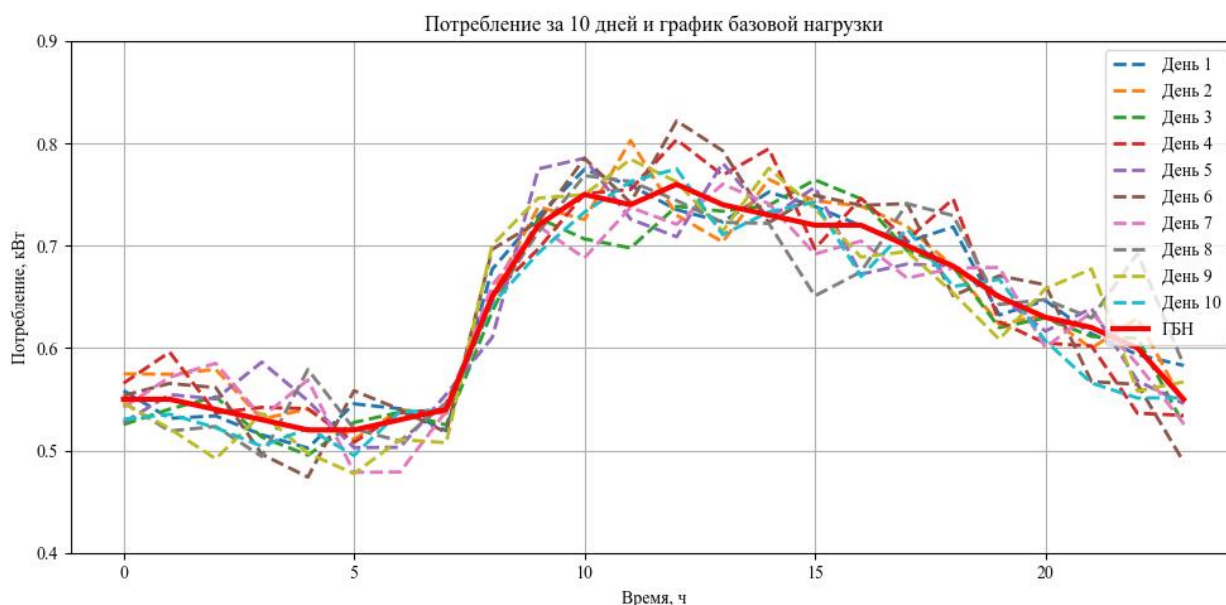


Рисунок 2 – Визуализация расчёта ГБН за 10 дней

Метрика проверки качества

Одной из ключевых метрик для оценки качества прогнозов является MAPE (Mean Absolute Percentage Error) – средняя абсолютная процентная ошибка. Этот показатель широко применяется благодаря своей простоте и наглядности, поскольку он количественно отражает степень отклонения фактических значений потребления от прогнозных.

Адаптивное окно и экспериментальная проверка

С момента запуска делового процесса по управлению спросом в России накопилось достаточное количество данных о электропотреблении, что позволяет провести анализ и определить, является ли стандартный размер окна в 10 дней действительно оптимальным.

Процесс поиска оптимального размера окна можно сформулировать как задачу минимизации ошибки MAPE, выраженную следующей формулой:

$$w_{opt} = \arg \min_{w \in W} MAPE(w)$$

где:

- W – набор возможных размеров окна,
- $MAPE(w)$ – средняя абсолютная процентная ошибка для размера окна w .

Был проведён расчет окон ГБН для всех энергопринимающих объектов с различным размером окна от 2 до 20 дней, с последующей оценкой метрики MAPE. В качестве исходных данных использовались условные среднестатистические данные потребления за один месяц. Результаты расчётов представлены в Таблице 1.

Таблица 1 – Результаты расчёта MAPE для окон разных размеров

Размер окна	MAPE
2	100.30
3	99.89
4	100.27
5	100.92
6	101.06
7	99.05
8	98.04
9	96.54
10	97.19
11	97.69
12	97.98
13	98.32
14	98.50
15	98.84
16	99.15
17	99.47
18	99.53
19	99.70
20	99.80

Результаты показали, что оптимальный размер окна отличается от значения 10 дней и равен 9 дням с разницей MAPE на 0,65.

Несмотря на то, что найденное значение может быть оптимальным в среднем для всех объектов, для конкретной отрасли может существовать своё собственное оптимальное значение размера окна. Это может быть связано с характером потребления энергии, зависящими от типа производства.

Учитывая данные особенности, был проведён расчёт оптимального размера окна для каждой отрасли в отдельности. Результаты данного расчёта представлены в Таблице 2.

Таблица 2 – Результаты расчётов метрик для окон разных размеров

Отрасль	Оптимальный размер окна	MAPE при оптимальном размере окна	MAPE при размере окна 10	p-value
Водоснабжение и водоотведение	6	8.87	9.13	0.40
Горнодобывающая промышленность	7	127.00	142.20	0.01
Дата-центры	9	301.24	302.23	0.90
Добыча нефти и газа	18	16.13	17.50	0.03
Котельные и электроотопление	18	29.11	30.40	0.05
Металлургия	18	20.68	21.08	0.62
Пищевая промышленность	18	12.42	13.83	0.06
Производство цемента, асфальта, кирпичей	11	15.08	15.12	0.99
Базовые станции сотовой связи	12	3.61	3.83	0.01
Спортивные сооружения	20	40.62	43.73	0.03
Торгово-развлекательные центры	6	47.08	47.51	0.09
Транспортировка нефти и газа	4	21.29	22.20	0.70
Химическое производство	12	13.27	13.45	0.59
Целлюлозно-бумажная промышленность	20	32.75	33.88	0.03

Полученные результаты показали, что каждая отрасль может иметь своё собственное оптимальное значение размера окна. Для проверки и подтверждения эффективности данного подхода был проведен анализ полученных результатов, в ходе которого окна оптимального размера сравнивались со стандартными окнами размером 10 дней. Чтобы обосновать выявленные улучшения, использовались такие методы, как критерий Уилкоксона, парный t-тест, а также оценка p-value, результаты которых представлены в Таблице 2.

Критерий Уилкоксона применялся в случаях, когда данные не соответствовали нормальному распределению, парный t-тест – когда распределение данных было близко к нормальному.

P-value также рассчитывался для каждого теста, что позволяло определить значимость различий. Если значение p-value оказывалось ниже 0,05, разница считалась статистически значимой, что указывало на то, что использование оптимального окна действительно улучшает точность прогноза [4].

Практическая значимость различий оценивалась отдельно, чтобы определить их реальное влияние на качество прогноза. Например, снижение значения MAPE на более чем

5% рассматривалось как значительное достижение, которое заметно повышает точность расчёта объёмов потребления.

Статистически значимые улучшения наблюдаются в следующих отраслях:

- горнодобывающая промышленность,
- добыча нефти и газа,
- базовые станции сотовой связи,
- спортивные сооружения,
- целлюлозно-бумажная промышленность.

Оценка практической значимости отражена в Таблице 3.

Таблица 3 – Отрасли с практической значимостью

Отрасль	Процент снижения ошибки
Горнодобывающая промышленность	10.70
Добыча нефти и газа	7.83
Пищевая промышленность	10.20
Базовые станции сотовой связи	5.74
Спортивные сооружения	7.12

В большинстве остальных отраслей разница в MAPE не является статистически значимой, а снижение ошибки не превышает 4%.

Проверка сезонности

Вопрос о наличии сезонных изменений в оптимальном размере окна является важным для точного прогнозирования потребления. Сезонные колебания и изменения в модели потребления могут существенно влиять на выбор подходящего интервала для усреднения данных. Чтобы определить, существует ли связь между временем и оптимальным размером окна, был проведён анализ данных по месяцам.

В качестве примера была рассмотрена отрасль «Горнодобывающая промышленность», для которого определены оптимальные размеры окна в нескольких месяцах. Результаты исследования представлены в Таблице 4.

Таблица 4 – Оптимальный размера окна для одной отрасли по месяцам

Месяц	Оптимальный размер окна	MAPE при оптимальном размере окна	MAPE при размере окна 10	Процент улучшения
Май	5	19.53	20.53	4.87
Июнь	6	28.04	29.39	4.60
Июль	15	224.91	240.72	6.57
Август	7	127.00	142.20	10.69
Сентября	12	8.12	8.36	2.87
Октябрь	5	38.04	40.22	5.42
Ноябрь	6	33.18	34.20	2.98

Данные из таблицы показывают, что размер окна существенно изменяется в зависимости от месяца. В результате, для поддержания высокой точности прогнозирования необходимо периодически пересчитывать оптимальный размер окна для каждой отрасли.

Реализация

Так как данный расчёт является ресурсоёмкой задачей, его выполнение может значительно нагружать основную систему и замедлить её работу. Поэтому целесообразно вынести вычисления в отдельный микросервис, который будет производить расчёты и периодически обновлять оптимальный размер окна для каждой отрасли. Чтобы эффективно управлять процессом обновления и интеграцией результатов, можно использовать брокер сообщений, к примеру, RabbitMQ [5]. Это позволит запускать процесс расчёта по запросу или в заданное время, а также получать результаты асинхронно, без нагрузки на основную информационную систему.

Пример взаимодействия информационной системы управления спросом на электроэнергию с сервисом расчётом представлен на Рисунке 3.

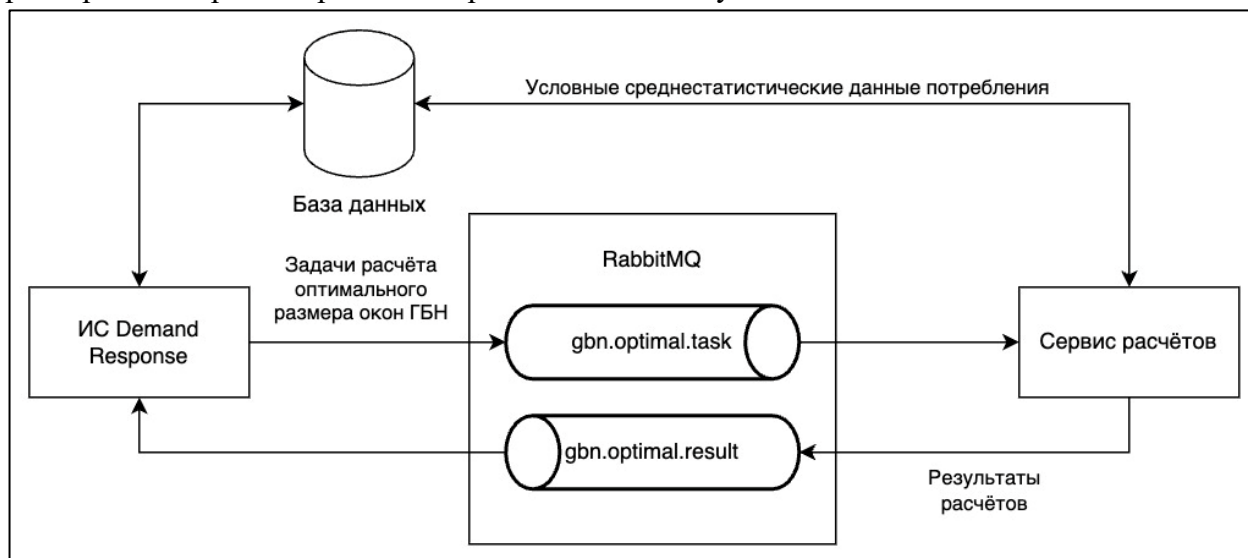


Рисунок 3 – Пример взаимодействия основной системы с сервисом расчётов

Заключение

Проведённое исследование показало, что использование адаптивного окна графика базовой нагрузки (ГБН) повышает точность прогнозирования электропотребления при определении объёмов снижения потребления в рамках событий управления спросом. Установлено, что оптимальный размер окна варьируется в зависимости от отрасли и изменяется со временем под влиянием сезонных и отраслевых факторов, что требует его регулярного пересчёта. Внедрение адаптивного подхода позволило снизить среднюю абсолютную процентную ошибку (MAPE) на 2–10% в ряде отраслей, подтверждая практическую значимость метода. Для автоматизации расчётов оптимального размера окна предложено использовать вычислительный микросервис с применением брокера сообщений. Таким образом, адаптивное окно ГБН демонстрирует высокую эффективность, улучшая точность прогнозирования с учётом отраслевых особенностей и динамики потребления.

Список литературы

1. Дзюба А.П., Соловьева И.А. Управление спросом на электропотребление в России // Стратегические решения и риск-менеджмент. 2018. №1. С. 72-79. URL: <https://doi.org/10.17747/2078-8886-2018-1-72-79>.
2. Поддубный А.А., Акимов Д.А., Юдина К.В., Николаев А.В. Анализ основных методов построения графика базовой нагрузки при управлении спросом // Электроэнергия. Передача и распределение. 2021. №1 (64). С. 64-69. URL: <https://elibrary.ru/item.asp?id=44765514>.
3. The Demand Response Baseline // EnerNoc. 2011. URL: https://www.naesb.org/pdf4/dsmee_group3_100809w3.pdf.
4. Муслов С.А., Зайцева Н.В., Чистяков М.В. Почему 0,05? // Современные тенденции развития науки и мирового сообщества в эпоху цифровизации. 2023. С. 436-440. URL: <https://www.elibrary.ru/item.asp?id=54102680>.
5. Тришин Е.А. Исследование брокеров сообщений в приложениях с микро-сервисной архитектурой // Вестник науки. 2024. №6 (75). URL: <https://cyberleninka.ru/article/n/issledovanie-brokerov-soobscheniy-v-prilozheniyah-s-mikro-servisnoy-arhitekturoy>.

References

1. Dzyuba A.P., Soloveva L.A. Electrical energy demand management in Russia // Strategic decisions and risk management. 2018. No. 1. P. 72-79. URL: <https://doi.org/10.17747/2078-8886-2018-1-72-79>.
 2. Poddubniy A.A., Akimov D.A., Yudina K.V., Nikolaev A.V. Analysis of main methods of plotting the basic load curve under demand control // Electricity. Transmission and distribution. 2021. No. 1 (64). P. 64-69. URL: <https://elibrary.ru/item.asp?id=44765514>.
 3. The Demand Response Baseline // EnerNoc. 2011. URL: https://www.naesb.org/pdf4/dsmee_group3_100809w3.pdf.
 4. Muslov S.A., Zaitseva N.V., Chistyakov M.V. Why 0.05? // Modern trends in the development of science and the world community in the era of digitalisation. 2023. P. 436-440. URL: <https://www.elibrary.ru/item.asp?id=54102680>.
 5. Trishin E.A. Research of message brokers in applications with microservice architecture // Vestnik nauki. 2024. №6 (75). URL: <https://cyberleninka.ru/article/n/issledovanie-brokerov-soobscheniy-v-prilozheniyah-s-mikro-servisnoy-arhitekturoy>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738

ВЫБОР ТЕХНОЛОГИИ АСИНХРОННОЙ ПЕРЕДАЧИ ДАННЫХ В РЕАЛЬНОМ ВРЕМЕНИ ПРИ ПРОЕКТИРОВАНИИ ВЕБ-МЕССЕНДЖЕРОВ

Сергеев Д.Н.

ФГБОУ ВО "КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМ. А.Н. ТУПОЛЕВА-КАИ», Казань, Россия (420111, Республика
Татарстан, город Казань, ул. Карла Маркса, д.10), e-mail: sergeevDanil2301@gmail.com

В данной статье рассматриваются пять основных технологий асинхронной передачи данных для интерактивного взаимодействия клиента с сервером: Long Polling, Server-Sent Events (SSE), WebSocket, WebRTC, WebTransport. Описываются основные принципы работы этих технологий, а также рассматриваются ключевые аспекты взаимодействия с ними, выделяются их сильные и слабые стороны в контексте разработки веб-мессенджеров, анализируется потенциальная сложность проектирования информационной системы, а также по совокупным показателям выбирается наиболее оптимальная технология для проектирования веб-мессенджеров.

Ключевые слова: Передача данных в реальном времени, способы коммуникации, асинхронная передача данных, веб-мессенджер, веб-сайт.

SELECTION OF REAL-TIME ASYNCHRONOUS DATA COMMUNICATIONS TECHNOLOGY IN WEB MESSENGER DEVELOPMENT

Sergeev D.N.

«KAZAN NATIONAL RESEARCH TECHNICAL UNIVERSITY. A.N. TUPOLEV-KAI», Kazan,
Russia (420111, Republic of Tatarstan, Kazan, Karl Marx st., 10), e-mail:
sergeevDanil2301@gmail.com

This article reviews five main technologies of asynchronous data transfer for interactive client-server communication: Long Polling, Server-Sent Events (SSE), WebSocket, WebRTC, WebTransport. Describes the basic principles of operation of these technologies, and also considers the key aspects of interaction with them, highlights their strengths and weaknesses in the context of web messenger development, analyzes the potential complexity of information system design, and by aggregate indicators selects the most optimal technology for the design of web messengers.

Keywords: Real-time data transfer, communication methods, asynchronous data communication, web messenger, website.

С развитием технологий передачи данных возросла популярность мессенджеров. В современном мире веб-мессенджеры стали неотъемлемой частью повседневной жизни – они позволяют пользователям общаться, делиться информацией, решать рабочие вопросы и быть в курсе последних событий. Однако проектирование таких систем требует особого внимания к выбору технологий передачи данных в реальном времени. Существует ряд проблем, которые могут возникнуть при разработке веб-мессенджера. К ним можно отнести следующие проблемы: проблемы с производительностью [1], проблемы с безопасностью [2], проблемы излишней сложности проектирования системы [3]. В данной статье мы рассмотрим основные

аспекты и критерии выбора подходящих технологий для создания эффективных и надёжных веб-мессенджеров.

Веб-разработка часто требует реализации механизмов обновления контента на странице в реальном времени. При работе с современными веб-приложениями реального времени незаменима возможность отправлять события с сервера на клиент. Именно этой необходимостью продиктовано то, что за годы работы было изобретено несколько методов для этой цели, каждый с собственным набором достоинств и недостатков. Есть разные ситуации, когда требуется передача информации в режиме реального времени. Например, при создании веб-мессенджера пользователю нужны постоянные уведомления о том, что сообщение отправлено, прочитано, отредактировано или удалено. Все эти сценарии объединяет одна общая черта: источник обновления данных находится на стороне сервера, поэтому для асинхронного получения информации о событиях требуется взаимодействие с серверной стороной. Передача данных в режиме реального времени в веб-приложениях позволяет отправлять и получать данные без необходимости перезагружать страницу.

В данной статье мы рассмотрим пять подходов к реализации этой функциональности: Long Polling, Server-Sent Events (SSE), WebSocket, WebRTC, WebTransport. Мы проанализируем каждый метод, выявим их плюсы, минусы и сложность реализации в разрезе проектирования веб-мессенджера.

В начале 2000-х годов Long Polling был одним из первых методов обновления контента на странице в режиме реального времени, предшествуя появлению более современных технологий, таких как WebSocket и Server-Sent Events. Этот подход стал популярным благодаря возможности преодолеть ограничения традиционного веб-протокола HTTP, который не поддерживает двустороннюю связь.

Принцип работы заключается в следующем: клиент отправляет HTTP-запрос на сервер, сервер в ответ может отправлять несколько порций данных перед отправкой окончательного результата и закрытием соединения. К преимуществам данного подхода можно отнести простоту реализации. Данный подход не является нативным, то есть HTTP запрос не совсем предусмотрен для такого типа взаимодействия. В связи с этим можно наблюдать следующие недостатки: задержки в передаче данных из-за ожиданий и таймаутов, высокая нагрузка на сервер из-за большого количества открытых соединений. Такой подход неэффективен при постоянном потоке данных, который потенциально может генерировать веб-мессенджер.

Server-Sent Events (SSE) — это технология, позволяющая серверу отправлять клиенту поток событий через однонаправленное соединение. Чтобы поддерживать открытое соединение, сервер может периодически отправлять пустые события, предотвращая закрытие соединения браузером из-за таймаута. SSE определён в спецификации HTML5 и поддерживается большинством современных браузеров. Этот подход можно использовать при создании веб-мессенджера, однако в этом случае сообщения от клиента должны отправляться с использованием стандартных HTTP-запросов.

Преимущества: Простая реализация на стороне сервера и клиента. Широкая поддержка как браузерами, так и веб-фреймворками. Автоматическое восстановление соединения при разрыве связи.

Недостатки: только односторонняя передача данных от сервера к клиенту, отсутствие полноценной поддержки старыми браузерами.

WebSocket стандартизирован в 2011 году как передовое решение для устойчивых двусторонних каналов связи между клиентом и сервером через единственное TCP-соединение. Этот механизм обеспечивает непрерывное соединение браузера с сервером без необходимости постоянного обновления страницы, позволяя данным мгновенно передаваться в обе стороны. После первоначального HTTP/HTTPS-запроса для установки соединения, происходит автоматическое переключение на специализированный бинарный протокол WebSocket через заголовок Upgrade[4]. TCP-поддержка гарантирует надежность и целостность передаваемой информации – ключевой фактор при разработке веб-мессенджеров, так как важность гарантированного уведомления пользователей стоит на первом месте.

Преимущества: WebSocket предлагает гибкую, полноценную двустороннюю асинхронную связь в реальном времени. Это наиболее универсальное решение с минимальными ограничениями для реализации разнообразных интерактивных сценариев на веб-платформах.

Недостатки: WebSocket характеризуется высокой ресурсоемкостью и, как правило, требует разработки отдельного серверного приложения для своей интеграции в проекты.

WebRTC (англ. web real-time communications — коммуникации по сети в реальном времени) - технология с открытым исходным кодом, ориентированная на прямую передачу потоковых данных между браузерами и другими поддерживающими устройствами. Данная технология имеет преимущество при проектировании аудио-видео связей, так как в WebRTC используются два аудиокодека, G.711 и Opus, а также видеокодеки VP8 и H.264. В WebRTC встроен протокол DTLS — протокол датаграмм безопасности транспортного уровня, он позволяет приложениям, основанным на коммуникациях посредством датаграмм, общаться безопасным способом, предотвращающим перехват, прослушивание, вмешательство, не нарушая защиты целостности данных или подделку содержимого сообщения [4].

Техническая особенность данной технологии в том, что она создавалась для взаимодействия между клиентами, без участия сервера, хотя она также применима и для коммуникации вида сервер-клиент, но в роли сервера будет выступать другое клиентское приложение, которое будет выполнять серверные функции, такие как обработка сообщений пользователей, запись данных сообщений в базу данных и т.д. То есть всего лишь будет происходить имитация сервера. Поэтому чтобы разработать структуру, в которой WebRTC будет работать корректно в рамках веб-мессенджеров, всё равно понадобится общий сервер событий, который будет работать по архитектуре веб-сокетов или Server-Sent Events. Именно поэтому WebRTC не может называться полноценной заменой вышеуказанных технологий.

WebTransport API — инновационный стандарт на базе WebSocket для оптимальной связи веб-клиентов и серверов, обеспечивающий сверхэффективную передачу данных за счёт HTTP/3 QUIC протокола. Особенности технологии выступают мультипоточковая отправка (включая неупорядоченные данные) как через надежные[5], так и ненадежные каналы. Для организации надежных каналов по аналогии с WebSocket выступает протокол TCP. Высокая надёжность в каналах TCP обеспечивается проверкой контрольных сумм и подтверждением приёма полученных данных без нарушений их состояния и смысла. Это требует дополнительных запросов между устройствами, но обеспечивает большую стабильность канала связи. А для организации высокопроизводительных, но менее надежных каналов используется протокол UDP. Это идеальный инструмент для разработки приложений с

высокими требованиями к сетевой производительности — в частности, веб-конференций и голосовых звонков в веб-мессенджерах.

WebTransport является обновленной версией WebSocket, поэтому он получил все преимущества вышеуказанной технологии. Но важно отметить, что в настоящее время WebTransport пребывает в состоянии рабочего проекта (working draft)[6] и пока не пользуется широкой популярностью в сообществе. По состоянию на декабрь 2024 года WebTransport не поддерживается в браузере Safari, а также не имеет нативной поддержки в таких популярных фреймворках как Node.js, Laravel. Поэтому при использовании WebTransport сложность проектирования веб-мессенджера значительно увеличивается.

Преимущества: имеет все преимущества WebSocket, работа с аудио-видео связью.

Недостатки: Сложность технологии, отсутствие полной поддержки браузерами.

Мы рассмотрели 5 основных популярных технологий интерактивного взаимодействия клиента с сервером для получения данных. При проектировании веб-мессенджера, среди наиболее удобных решений было выделено две технологии: WebSocket, как основу для передачи уведомлений о получении, прочтении, удалении, редактировании сообщений, благодаря гарантированной передаче данных с наименьшими задержками и полноценной двусторонней асинхронной связью между клиентом и сервером и WebRTC для предоставления возможности для аудио- и видеосвязи, так как данная технология имеет поддержку аудиокодеков G.711 и Opus, а также видеокодеков VP8 и H.264. Комбинация данных технологий способна заложить основу для создания эффективных и надежных веб-мессенджеров.

Список литературы

1. Николай Мацеевский. Разгони свой сайт. Методы клиентской оптимизации веб-страниц. – М.: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2009. – 264 с.
2. Тутубалин П.И. Основные задачи прикладной теории информационной безопасности АСУ. Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007. № 39. С. 63-72.
3. Кожевников А.Ю., Тутубалин П.И., Кирпичников А.П., Мокшин В.В. О построении подсистемы удалённого мобильного доступа к информационным ресурсам некоторой организации. Вестник Технологического университета. 2018. Т. 21. № 2. С. 139-147.
4. Моисеев В.С., Тутубалин П.И. К задаче определения вероятностных характеристик информационной безопасности разрабатываемых автоматизированных систем управления. Депонированная рукопись ВИНТИ № 26-B2007 11.01.2007.
5. Кожевников А.Ю., Тутубалин П.И., Кирпичников А.П., Мокшин В.В. О разработке математических моделей, методов и программного обеспечения для проектирования перспективных изделий запрос-ответной аппаратуры. Вестник Технологического университета. 2018. Т. 21. № 2. С. 155-162.
6. Рахманов А.С., Тутубалин П.И. Автоматизация тестирования безопасности веб приложений. В сборнике: Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований. Материалы IV Всероссийской национальной научной конференции студентов, аспирантов и молодых учёных. В 4-х частях. Редколлегия: Э.А.

Дмитриев (отв. ред.), А.В. Космынин (зам. отв. ред.). Комсомольск-на-Амуре, 2021. С. 298-301.

References

1. Nikolai Matsievsky. Disperse your site. Methods of client optimization of web pages. - M.: Internet University of Information Technologies, Binom. Laboratory of Knowledge, 2009. – p.264
 2. Tutubalin P.I. The main tasks of the applied theory of information security of automated control systems. Scientific and Technical Bulletin of the St. Petersburg State University of Information Technologies, Mechanics and Optics. 2007. No. 39. pp. 63-72.
 3. Kozhevnikov A.Yu., Tutubalin P.I., Kirpichnikov A.P., Mokshin V.V. On the construction of a subsystem for remote mobile access to information resources of an organization. Bulletin of the Technological University. 2018. Vol. 21. No. 2. pp. 139-147.
 4. Moiseev V.S., Tutubalin P.I. On the problem of determining the probabilistic characteristics of information security of automated control systems under development. Deposited manuscript of VINITI No. 26-In 2007 11.01.2007.
 5. Kozhevnikov A.Yu., Tutubalin P.I., Kirpichnikov A.P., Mokshin V.V. On the development of mathematical models, methods and software for the design of promising products of request-response equipment. Bulletin of the Technological University. 2018. Vol. 21. No. 2. pp. 155-162.
 6. Rakhmanov A.S., Tutubalin P.I. Automation of web application security testing. In the collection: Youth and science: current problems of fundamental and applied research. Materials of the IV All-Russian National Scientific Conference of students, postgraduates and young Scientists. In 4 parts. Editorial board: E.A. Dmitriev (editor's note), A.V. Kosmynin (Deputy editor's note). Komsomolsk-on-Amur, 2021. pp. 298-301.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.623

АНАЛИЗ ПОЛЬЗОВАТЕЛЬСКИХ ЗАПРОСОВ НА НАЛИЧИЕ СЕТЕВОЙ АТАКИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

Дубиков Д.Э.

ФГАОУ ВО "МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ", Москва, Россия
(107023, город Москва, Большая Семёновская ул., д. 38), e-mail: Orp7ptdQtr@yandex.ru

В процессе функционирования сетей, в том числе Интернета, их узлы, принимающие входящие запросы, сталкиваются с проблемой различения в них полезных и вредоносных. Такие запросы могут приводить к несанкционированному доступу к узлу сети и, как следствие, к отказу системы, утечке конфиденциальной информации и иным нежелательным последствиям. В статье рассматривается ситуация, при которой через сеть поступает множество пользовательских запросов, часть из которых представляют собой сетевую атаку. Целью исследования является анализ пользовательских запросов на наличие сетевой атаки и автоматизация этого процесса с использованием технологий больших данных. Для анализа выбран датасет с данными о совершённых сетевых атаках. При помощи языка программирования Python и специальных библиотек pandas и sklearn реализована его автоматизация путём создания нейронной сети. Полученная нейронная сеть имеет высокую точность и может быть использована для анализа пользовательских запросов на практике в любой сфере человеческой деятельности, требующей работы с сетью Интернет. Созданный алгоритм может быть использован для обучения нейронной сети на любых других данных, имеющих свою специфику.

Ключевые слова: Сетевая атака, сетевой запрос, большие данные, нейронная сеть.

ANALYSIS OF USER REQUESTS FOR THE PRESENCE OF NETWORK ATTACK USING BIG DATA TECHNOLOGIES

Dubikov D.E.

MOSCOW POLYTECHNIC UNIVERSITY, Moscow, Russia (107023, Moscow, Semyonovskaya str., 38.), e-mail: Orp7ptdQtr@yandex.ru

In the process of functioning of networks, including the Internet, their nodes that receive incoming requests face the problem of distinguishing between normal and malicious units. Such requests can lead to unauthorized access to a network node and, as a consequence, to system failure, leakage of confidential information and other undesirable consequences. The article considers a situation in which many user requests are received through the network, some of which represent a network attack. The purpose of the study is to analyze user requests for a network attack and automate this process using big data technologies. For the analysis, a dataset with data on committed network attacks was selected, using the Python programming language and special libraries pandas and sklearn, its automation was implemented by creating a neural network. The resulting neural network has high accuracy and can be used to analyze user requests in practice. The created algorithm can be used to train the neural network on other data with different specifics. The developed neural network can be applied in any area of human activity that requires working with the Internet.

Keywords: Network attack, network request, big data, neural network.

Введение

Ещё в недалёком прошлом технологии, позволяющие соединять технические устройства в единую сеть, были доступны только самым крупным компаниям, поскольку стоили больших

денег по причине слабой развитости соответствующих сфер знаний человечества и отсутствия продвинутых технологий серийного производства соответствующего оборудования. Однако в современном мире подавляющее большинство людей имеют множество сложных технических устройств, часто соединённых в единую всемирную сеть — Интернет, что обуславливает актуальность настоящего исследования. Если недавно к таким устройствам относились лишь компьютеры и смартфоны, то сегодня с развитием интернета вещей в эту категорию попадают и иная бытовая техника от холодильников и микроволновок до камер видеонаблюдения [4].

Стремительное развитие сетевых технологий неизбежно влечёт за собой необходимость развития соответствующих протоколов безопасности взаимодействия узлов сети между собой. Эта необходимость обусловлена, в первую очередь, сохранением конфиденциальности информации, которую хранят и которой оперируют технические устройства, но также нужда в ней обуславливается и обеспечением в целом правильной работоспособности сети, то есть её защиты от попыток дестабилизации нормальной работы [4].

Сетевые атаки являются серьёзным препятствием для штатной работы сети, поскольку имитируют обычные запросы, предназначенные для взаимодействия узлов в сети, имея своей реальной целью дестабилизацию работы системы. Различение обычных пользовательских запросов и запросов, представляющих собой элементы сетевой атаки, представляет собой важную часть концепции защиты сети, которая должна быть учтена в протоколах безопасности.

Таким образом, целью исследования является построение анализатора пользовательских запросов на наличие в них сетевой атаки с использованием технологий больших данных.

Материалы и методы

Материалы для анализа

Для анализа пользовательских запросов на наличие в них сетевой атаки используем набор данных, содержащий различную информацию о пользовательских запросах, а также имеющий поле, обозначающее, являлся ли фактически запрос элементом сетевой атаки.

Датасет содержит 257674 строки и 49 столбцов, из которых 1 обозначает наличие атаки, 1 — тип атаки, 1 — идентификатор записи в датасете и 46 — параметры запроса, предположительно являющегося сетевой атакой.

Исходные сетевые пакеты набора данных были созданы с помощью инструмента IXIA PerfectStorm в лаборатории Cyber Range Австралийского центра кибербезопасности (ACCS) для создания гибрида реальных современных повседневных действий и синтетических современных атак. В этом наборе данных есть девять типов атак: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode и Worms.

Метод анализа

Для анализа данных пользовательских запросов на наличие в них сетевой атаки используем нейронную сеть. Этот мощный инструмент, получающий всё более широкое распространение за счёт распараллеливания обработки информации и способности к самостоятельному обучению, то есть созданию обобщений, где под «обобщением» понимается получение результата, основываясь на данных, не встречавшихся во время обучения [1].

Использование нейронных сетей обеспечивает следующие полезные свойства системы [1]:

1. Нелинейность. Является особенно важным свойством, когда механизм формирования входного сигнала также не считается линейным, что позволяет значительно расширить области применения нейросетевых технологий.
2. Отображение входной информации в выходную.
3. Адаптивность. Это свойство означает, что нейронные сети имеют способность адаптировать синаптические веса к происходящим при анализе изменениям. Так, например, нейронная сеть, обученная в определённой среде, может быть переобучена для новых условий.
4. Очевидность ответа. Нейронная сеть даёт однозначный ответ на запрос, взвешивая все вероятности по ходу своей работы.
5. Контекстная информация.
6. Отказоустойчивость. Неблагоприятные условия не оказывают значительного влияния на производительность системы. Так, например, если какой-либо нейрон оказывается повреждён, то извлечь усвоенную им информацию трудно, однако с учётом распределённого характера хранения информации можно утверждать, что существенного влияния на работу нейронной сети в целом это не оказывает.
7. Масштабируемость.

Инструменты анализа

Анализ данных пользовательских запросов на наличие в них сетевой атаки автоматизируем при помощи соответствующих инструментов. В качестве такого инструмента автоматизации выберем язык программирования Python, имеющий ряд преимуществ [5]:

1. Качество программного обеспечения. Python разработан специально для того, чтобы отличаться от остальных языков программирования читабельностью и согласованностью.
2. Продуктивность труда разработчиков. За счёт, в том числе, динамической типизации переменных Python значительно снижает трудоёмкость процесса разработки.
3. Переносимость программ. Код, написанный на Python, практически всегда работает одинаково на всех платформах компьютеров, в том числе при переносе на другую операционную систему.
4. Поддерживаемые библиотеки. Так называемая «стандартная библиотека» Python включает в себя множество инструментов самого разного рода для решения наиболее часто требуемых для разработчиков задач, в том числе, узкоспециализированного профиля.
5. Интеграция компонентов. Python позволяет работать с библиотеками, написанными для других языков программирования, таких как C++. Это в значительной степени расширяет его возможности, в том числе, производительность.

В рамках использования Python используем специальные библиотеки для анализа данных. Для преобразования исходного датасета в переменную, пригодную для работы, используем встроенные инструменты библиотеки pandas, являющейся центром обширной экосистемы исследования данных. Преимуществом pandas является её универсальность по части сочетаемости с другими библиотеками, представляющими более широкие возможности для анализа данных [2]. Для собственно работы с датасетом выберем библиотеку sklearn. Scikit-Learn очень проста в использовании, но при этом эффективно реализует множество

алгоритмов машинного обучения, поэтому является отличной отправной точкой для работы с инструментами машинного обучения [3].

Для обучения нейронной сети используем 75% исходного датасета, для тестирования — оставшиеся 25%.

Результаты

Для заявленной автоматизации анализа пользовательских запросов на наличие в них сетевой атаки была написана программа на языке программирования Python с использованием библиотек для анализа данных pandas и sklearn. Код представлен в листинге 1.

Листинг 1 — Код программы, автоматизирующей анализ пользовательских запросов на наличие в них сетевой атаки

```
import pandas as pd
from sklearn.metrics import accuracy_score
from sklearn.model_selection import train_test_split
from sklearn.tree import DecisionTreeClassifier

df = pd.read_csv('UNSW_NB15_training-set.csv')

df = df.fillna("")

df = df.drop(['proto', 'service', 'state', 'attack_cat'], axis=1)

X = df.drop('label', axis=1)
y = df['label']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.25)
clf = DecisionTreeClassifier()
clf.fit(X_train, y_train)
preds = clf.predict(X_test)

print(accuracy_score(y_test, preds))
```

Согласно коду, столбец «label» датасета использован в качестве выходного параметра, а остальные — в качестве входных параметров для нейронной сети, причём четыре столбца — «proto», «service», «state», «attack_cat» — были признаны несущественными и не учитывались при обучении.

Для тестовой выборки использовалась последняя четверть датасета, а для обучения нейронной сети — его первые три четверти. Библиотека pandas была использована для преобразования исходного датасета к виду, доступному для работы с библиотекой sklearn, при помощи которой, в свою очередь, с использованием представляющих её инструментов был проведён собственно анализ исходных данных.

После обучения и тестирования программа рассчитывает и выводит пользователю точность полученной нейронной сети: 0,9821015538893805, то есть приблизительно 98,21%.

Такой показатель означает, что нейронная сеть имеет высокую точность и способна давать в значительной степени достоверный результат при использовании, в том числе, в реальных практике. Такой высокий показатель обеспечен в значительной степени универсальностью использованных средств автоматизации анализа данных, не требующих от пользователя глубоких теоретических знаний, в том числе, по части выбранных специальных библиотек.

Обсуждение

Получена нейронная сеть, способная с высокой точностью анализировать пользовательские запросы на наличие в них сетевой атаки. Также разработан соответствующий алгоритм обучения и тестирования полученной нейронной сети, для которого могут быть использованы не только исходные для текущего исследования данные, но и иные, специфические для той или иной области деятельности или, более узко, конкретного предприятия.

Разработанная нейронная сеть может найти широкое применения в самых разных областях человеческой жизнедеятельности — на любых предприятиях и компаниях, использующих Интернет в качестве сети для обмена информацией между внутренними и внешними техническими устройствами. Созданная нейронная сеть способна распознавать сетевые атаки, направленные на дестабилизацию работы предприятия, и уведомлять об этом иные соответствующие системы, разработанные, например, для отсеивания входящего трафика, что, в свою очередь, обеспечивает защиту оборудования от несанкционированного доступа, перегрузки бесполезными запросами и иных способов негативного влияния на часть сети Интернет, локальную для защищаемого предприятия.

Область применения разработанной нейронной сети и соответствующего алгоритма для её обучения столь же широка, сколь широко использование больших объёмов данных с подключением соответствующих технических устройств к Интернету.

Заключение

Таким образом, по ходу проведения исследования получена нейронная сеть для анализа пользовательских запросов на наличие в них сетевой атаки. Точность созданной нейросети получилась высокой, что означает, что разработанный алгоритм её обучения является качественным, а полученная нейронная сеть может быть использована на практике. Алгоритм и нейронная сеть могут найти своё применение в любой сфере деятельности, где проводится работа с использованием технологий и устройств, задействующих для своего функционирования Интернет или иные сети.

Список литературы

1. Лутц М. Изучаем Python // Диалектика. 2019. С. 40–60.
2. Пасхавер Борис. Pandas в действии // Питер. 2023. С. 30–34.
3. Рашка С. Python и машинное обучение // ДМК Пресс. 2017. С. 68–73.
4. Форшоу Дж. Атака сетей на уровне протоколов // ДМК Пресс. 2021. С. 18–19.
5. Хайкин С. Нейронные сети: полный курс // Вильямс. 2006. С. 31–37.

References

1. Lutz M. Learning Python // Dialektika. 2019. P. 40–60.
 2. Paskhaver B. Pandas in Action // Piter. 2023. P. 30–34.
 3. Rashka S. Python Machine Learning // DMK Press. 2017. P. 68–73.
 4. Forshow J. Attacking Network Protocols // DMK Press. 2021. P. 18–19.
 5. Haykin S. Neural Networks: A Comprehensive Foundation // Williams. 2006. P. 31–37.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

ПРИМЕНЕНИЕ PROCESS MINING ДЛЯ ИДЕНТИФИКАЦИИ УЗКИХ МЕСТ В БИЗНЕС-ПРОЦЕССАХ

Калиберда С.И.

*ФГБОУ ВО «ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ И. А. БУНИНА»,
Елец, Россия, (399770, Липецкая область, город Елец, ул. Коммунаров, д. 28,1), e-mail:
nondeadd@yandex.ru*

Статья посвящена технологии Process Mining как инструменту анализа и оптимизации бизнес-процессов на основе данных. Рассматриваются ключевые компоненты технологии, такие как журналы событий и алгоритмы анализа, позволяющие выявлять реальные узкие места и отклонения от запланированных моделей. Приводятся примеры применения в банковской и логистической сферах, демонстрирующие повышение эффективности процессов. Process Mining рассматривается как стратегический подход, позволяющий принимать решения на основе объективных данных и повышать производительность процессов.

Ключевые слова: Бизнес-процесс, узкие места, анализ, оптимизация.

APPLICATION OF PROCESS MINING TO IDENTIFY BOTTLE PLACES IN BUSINESS PROCESSES

Kaliberda S.I.

*YELETS STATE UNIVERSITY NAMED AFTER I. A. BUNIN, Yelets, Russia, (399770, Lipetsk region,
Yelets, Kommunarov st., 28,1), e-mail: nondeadd@yandex.ru*

The article focuses on Process Mining as a tool for analyzing and optimizing business processes based on data. It explores key components of the technology, such as event logs and analysis algorithms, which help identify real bottlenecks and deviations from planned models. Practical applications in banking and logistics sectors are provided, demonstrating process efficiency improvements. Process Mining is presented as a strategic approach enabling data-driven decision-making and enhancing process productivity.

Keywords: Business process, bottlenecks, analysis, optimization.

В эпоху цифровых преобразований и усиливающейся рыночной борьбы организации вынуждены постоянно исследовать и совершенствовать свои операционные процессы. Операционная деятельность компаний зачастую остается непрозрачной для менеджмента, так как фактическое исполнение операций может существенно расходиться с запланированными схемами. Process Mining выступает как технологическое решение, позволяющее объединить теоретические модели с практической реализацией, предлагая методы исследования рабочих процессов на базе фактических операционных данных.

Главным достоинством Process Mining является возможность получения достоверной картины бизнес-процессов. В противовес классическому методу, включающему опросы персонала или изучение устаревших схем, Process Mining базируется на актуальных данных. Это превращает его в эффективный инструмент для выявления проблем и улучшения

процессов. Система позволяет не просто отслеживать выполнение операций, но и выявлять проблемные участки, отступления от норм и зоны неэффективности. К примеру, один крупный логистический оператор с помощью Process Mining обнаружил, что главным фактором задержек в доставке являлись многократные согласования маршрутов с заказчиками, занимавшие до 20% общего времени [1].

Process Mining также отличается широкими возможностями применения. Технология эффективна в различных сферах деятельности - от промышленного производства до медицинских услуг. На практике данный инструмент применяется как для мониторинга текущих операций, так и для их совершенствования. Так, страховая организация смогла сократить длительность обработки страховых заявок с пяти до трех дней, внедрив автоматизированную проверку документации.

Актуальные решения Process Mining, включая Celonis, Disco и ProM, обеспечивают не только визуальное представление процессов, но и взаимодействие с другими программными комплексами. В частности, с BPM-системами типа Camunda 8. Подобная интеграция способствует автоматизации процессов, оптимизированных на основе аналитики Process Mining. Это приобретает особую значимость для компаний, нацеленных на комплексную цифровую трансформацию [1].

Process Mining базируется на анализе информации, регистрируемой в корпоративных информационных системах ERP, CRM или специализированных BPM-платформах. Эти системы автоматически генерируют логи событий (event logs), которые включают детальные сведения о каждой стадии процесса: уникальный идентификатор, наименование операции и хронологическую отметку. На основе этих сведений формируется комплексное представление о реализации бизнес-процессов. К примеру, исследование кредитных заявок может выявить, что основные задержки возникают при согласовании бумаг, а не при проверке комплектности документации, как предполагалось изначально. Event logs включают три ключевых компонента:

1. Case ID - уникальный идентификатор экземпляра процесса, например, идентификационный номер заявки или заказа.
2. Activity - определенное действие в рамках процесса, такое как «Верификация документации» или «Проведение платежа».
3. Timestamp - конкретный момент времени совершения операции.

Таблица 1 - Пример структуры журнала событий

Case ID	Activity	Timestamp
001	Проверка документов	2024-12-01 09:00:00
001	Согласование	2024-12-01 10:00:00
002	Проверка документов	2024-12-01 07:00:00

После накопления информации она обрабатывается специализированными алгоритмами для создания визуальных схем, отражающих структуру процесса [2]. Полученный граф демонстрирует:

Фактический порядок операций. К примеру, процесс мог планироваться как последовательный, однако реальные данные свидетельствуют о том, что определенные этапы реализуются одновременно или с временными промежутками.

Интенсивность выполнения действий. На графе можно увидеть наиболее востребованные пути реализации процесса.

Временные характеристики этапов. Это позволяет обнаружить временные задержки и проблемные участки процесса.

Узкие места представляют собой компоненты или стадии процесса, которые снижают его эффективность в целом. К ним относятся:

1. Затянутое исполнение операций на конкретном этапе.
2. Чрезмерная нагрузка на ресурсы (человеческие, технические или финансовые).
3. Лишние или дублирующие операции.

Узкие места приводят к временным задержкам, росту издержек и падению результативности бизнес-процессов. Их идентификация и ликвидация является приоритетной задачей Process Mining. Данная технология предоставляет подробные сведения о ходе процессов на основе реальных данных. С её помощью возможно:

1. Исследовать длительность выполнения задач.
2. Используя event logs, Process Mining рассчитывает усредненное, минимальное и максимальное время реализации каждой стадии. На процессной диаграмме узкие места отмечаются как этапы с наибольшей продолжительностью выполнения.
3. Определять степень загрузки ресурсов.
4. Process Mining позволяет контролировать уровень загруженности персонала и систем. Например, отдельный работник может обрабатывать обращения эффективнее коллег, что нарушает баланс распределения работы.
5. Выявлять типовые маршруты и отклонения.
6. Зачастую узкие места возникают при отступлении от стандартного процесса. Process Mining демонстрирует все возможные варианты выполнения задачи, включая отклонения, и обозначает проблемные зоны.
7. Обнаруживать повторяющиеся действия.

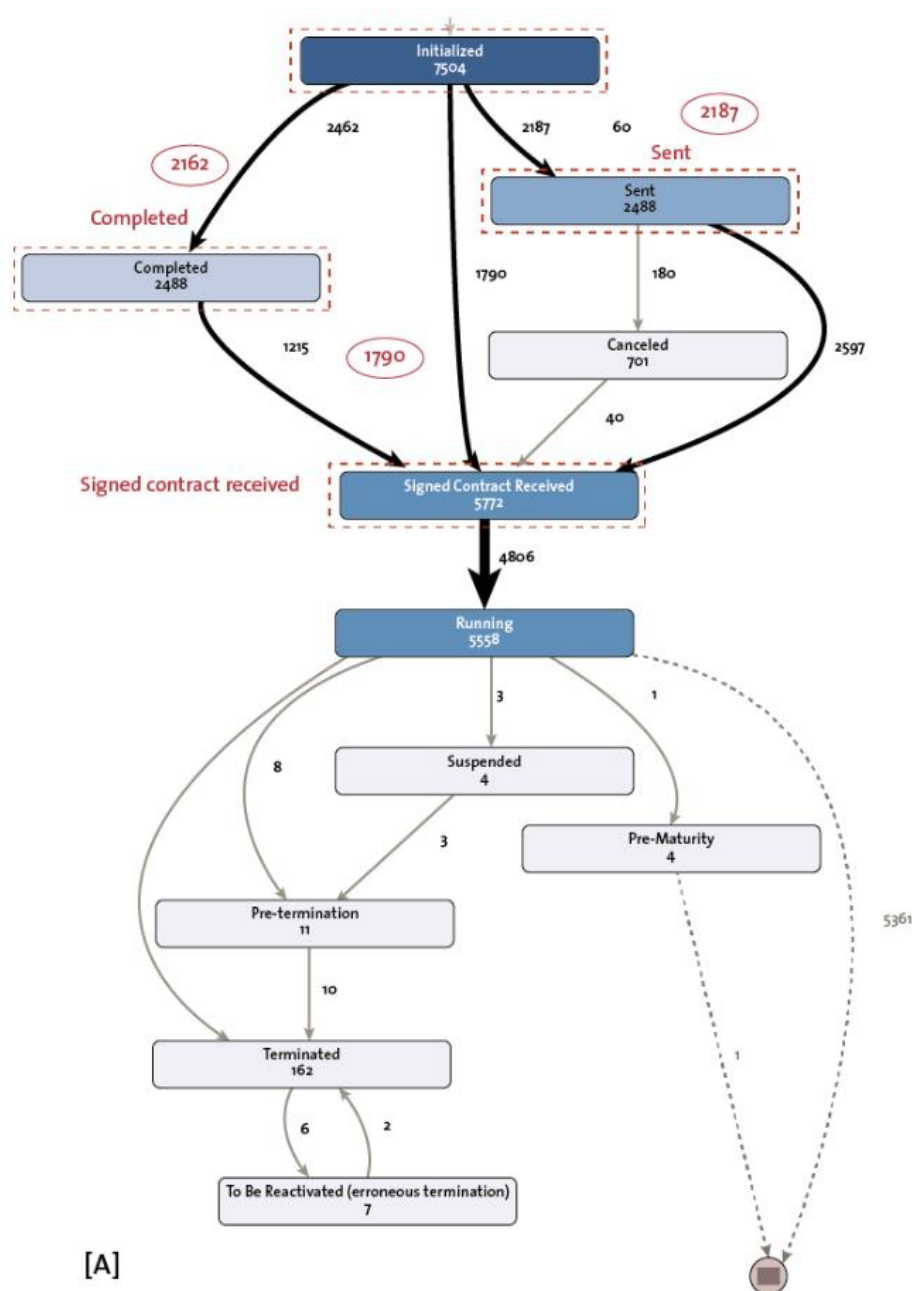


Рисунок 1 - Узкие места (темные узлы графа) в бизнес-процессе

Методики поиска узких мест посредством Process Mining базируются на исследовании данных о реализации процессов, их графическом представлении и сравнении с эталоном. Основной метод заключается в анализе временных затрат на выполнение задач. Для каждого этапа процесса определяются параметры, включая среднее, минимальное и максимальное время исполнения. Это помогает обнаружить этапы с наибольшей продолжительностью и оценить стабильность выполнения через анализ временных отклонений. Узкие места проявляются как участки с длительным выполнением операций или значительной нестабильностью [3].

Другой существенный подход основан на мониторинге использования ресурсов. Process Mining позволяет контролировать равномерность распределения задач между сотрудниками или системами. Выявление перегруженных ресурсов указывает на вероятные узкие места. Например, если большинство задач сконцентрировано на одном работнике, это может вызывать задержки на его участке.

Методики также предполагают сопоставление действующего процесса с референсной моделью. Анализируя фактические показатели в сравнении с планируемой последовательностью действий, Process Mining позволяет идентифицировать несоответствия, такие как пропуски операций, повторяющиеся этапы или нарушения порядка исполнения задач. Это помогает определить источники и причины затруднений, замедляющих весь процесс.

Более того, Process Mining результативно обнаруживает дублирование действий. Например, повторная верификация данных на определенном этапе может указывать на несовершенство предшествующих стадий. Исследование интенсивности выполнения операций и маршрутов выявляет не только узкие места, но и сегменты процесса, нуждающиеся в оптимизации. Следовательно, интегрированное применение этих методик формирует целостное представление о проблемных зонах и способствует целевому совершенствованию процесса [4].

Process Mining выступает как эффективный инструмент для исследования и оптимизации бизнес-процессов. Технология устраняет несоответствие между теоретическими моделями и практической реализацией задач, давая организациям возможность наблюдать реальное состояние процессов, включая узкие места, отклонения и неэффективные элементы. На основе анализа event logs компании могут выявлять ключевые проблемы, такие как временные задержки, перегрузка ресурсов или избыточные операции, что недостижимо при использовании классических методов управления процессами.

Использование Process Mining создает объективную базу для принятия решений, направленных на повышение эффективности. Организации получают не только сведения о существующих проблемах, но и предложения по их устранению, включая автоматизацию типовых операций, оптимизацию нагрузки и упрощение процессов [4].

Таким образом, Process Mining становится фундаментальным компонентом цифровой трансформации, содействуя адаптации организаций к динамичным рыночным условиям и усилению их конкурентных преимуществ. Это не просто аналитический инструмент, а стратегический подход к управлению бизнес-процессами, обеспечивающий прозрачность, результативность и устойчивое развитие. Внедрение Process Mining становится обязательным элементом современного бизнеса, открывая новые возможности для анализа и совершенствования процессов на базе объективных данных.

Список литературы

1. Jans M., Alles M., Vasarhelyi M. A. A Field Study on the Use of Process Mining of Event Logs as an Analytical Procedure in Auditing. – New York: Rutgers Business School, 2014. – с.45
2. Rozinat A., Günther C. W., Song M., van der Aalst W. M. P. Process Mining in Practice: A Handbook for Practice-Oriented Business Process Management. – Eindhoven: Eindhoven University of Technology, 2009. – с.124

3. Burattin A. Process Mining Techniques in Business Environments: Theoretical Aspects, Algorithms, Techniques and Open Challenges. – Berlin: Springer, 2015. – с.211
4. Dumas M., La Rosa M., Mendling J., Reijers H. A. Fundamentals of Business Process Management. 2nd ed. – Berlin: Springer, 2018. – с.527

References

1. Jans M., Alles M., Vasarhelyi M. A. A Field Study on the Use of Process Mining of Event Logs as an Analytical Procedure in Auditing. – New York: Rutgers Business School, 2014. – p.45
 2. Rozinat A., Günther C. W., Song M., van der Aalst W. M. P. Process Mining in Practice: A Handbook for Practice-Oriented Business Process Management. – Eindhoven: Eindhoven University of Technology, 2009. – p.124
 3. Burattin A. Process Mining Techniques in Business Environments: Theoretical Aspects, Algorithms, Techniques and Open Challenges. – Berlin: Springer, 2015. – p.211
 4. Dumas M., La Rosa M., Mendling J., Reijers H. A. Fundamentals of Business Process Management. 2nd ed. – Berlin: Springer, 2018. – p.527
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ АТАКЕ ТИПА «ПОДМЕНА МАРШРУТА» (BGP HIJACKING)

Бютнер С.И.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
serafimkavasaki@gmail.com

BGP hijacking, или подмена маршрута, — это атака на протокол маршрутизации Border Gateway Protocol (BGP), которая позволяет злоумышленникам перенаправлять или перехватывать интернет-трафик. Такие атаки могут использоваться для шпионажа, кражи данных или саботажа. В статье обсуждаются методы противодействия BGP hijacking, включая использование RPKI, мониторинг аномалий и внедрение криптографической защиты в BGP. Эти меры способны повысить устойчивость сети и снизить вероятность компрометации маршрутов.

Ключевые слова: BGP hijacking, подмена маршрута, маршрутизация, RPKI, кибербезопасность, защита сети, аномалии трафика.

METHODS OF COUNTERING A "ROUTE SUBSTITUTION" TYPE ATTACK (BGP HIJACKING)

Buetner S.I.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

BGP hijacking, or route hijacking, is an attack on the Border Gateway Protocol (BGP) that allows attackers to redirect or intercept internet traffic. These attacks can be used for espionage, data theft, or sabotage. The article explores methods to counter BGP hijacking, including the use of RPKI, anomaly monitoring, and cryptographic protection in BGP. These measures can enhance network resilience and reduce the likelihood of route compromise.

Keywords: BGP hijacking, route hijacking, routing, RPKI, cybersecurity, network protection, traffic anomalies.

Введение

Протокол BGP (Border Gateway Protocol) является основой современной маршрутизации в Интернете, связывая автономные системы (AS) между собой для обеспечения глобальной передачи данных. Однако из-за отсутствия встроенных механизмов аутентификации и проверки маршрутов, BGP уязвим к атакам, известным как BGP hijacking или подмена маршрута. В рамках этой атаки злоумышленники могут объявлять неверные маршруты, перенаправляя трафик через подконтрольные им сети, что может привести к утечке данных, отказу в обслуживании и даже созданию условий для массовых атак.

BGP hijacking остаётся серьёзной угрозой как для крупных провайдеров, так и для малых сетей. Известные случаи, такие как перенаправление трафика финансовых организаций или шпионаж через ложные маршруты, показывают, насколько разрушительными могут быть

такие атаки. Учитывая ключевую роль протокола BGP в функционировании Интернета, разработка эффективных методов противодействия этим атакам становится приоритетной задачей для операторов сетей и специалистов по кибербезопасности.

Методы противодействия атаке типа «подмена маршрута»

Атака типа BGP hijacking начинается с того, что злоумышленник отправляет неверные анонсы маршрутов в BGP. Эти ложные маршруты могут быть направлены на перенаправление трафика через вредоносную автономную систему, создание "чёрной дыры" (blackhole) для блокировки доступа к ресурсам или проведение атаки "человек посередине" (MITM), чтобы перехватывать данные. Главная причина уязвимости BGP заключается в его архитектуре, где маршруты принимаются на веру, без проверки их достоверности[1].

Для противодействия таким атакам разрабатываются различные методы защиты, которые можно условно разделить на три категории: криптографические решения, мониторинг аномалий и организационные меры.

Одним из наиболее перспективных методов защиты от BGP hijacking является использование RPKI. Эта технология позволяет провайдерам удостоверять подлинность объявляемых маршрутов с помощью цифровых подписей. С помощью RPKI маршруты проверяются на соответствие авторитетным записям, что исключает возможность анонсирования несанкционированных маршрутов. Однако RPKI сталкивается с рядом проблем, включая сложность внедрения и необходимость участия большого количества автономных систем для достижения глобального эффекта[2].

Ещё одним важным аспектом защиты является мониторинг аномалий в BGP-объявлениях. Сервисы, такие как BGPmon и RIPE Atlas, позволяют отслеживать подозрительные изменения маршрутов, например, внезапное увеличение количества объявляемых префиксов или изменение маршрутов крупных сетей. Операторы могут настроить автоматическое уведомление о таких событиях, что позволяет быстро реагировать на возможные атаки[3].

Фильтрация маршрутов предполагает настройку списков доступа и политик BGP для ограничения приёма маршрутов только от доверенных источников. Например, крупные провайдеры могут заранее договариваться о фильтрации неверных маршрутов на основе договорённостей с соседними автономными системами (AS). Эта мера снижает вероятность успешной атаки, но требует значительных ресурсов для поддержания актуальных списков[4].

Хотя BGP изначально не был разработан с учётом безопасности, современные инициативы, такие как BGPsec, направлены на интеграцию механизмов шифрования и аутентификации. BGPsec использует цифровые подписи для проверки аутентичности маршрутов, передаваемых через сети. Несмотря на преимущества, внедрение BGPsec сопряжено с высокими затратами и сложностями, связанными с необходимостью обновления оборудования и программного обеспечения[4].

Организационные меры включают в себя повышение осведомлённости о рисках BGP hijacking среди сетевых администраторов и внедрение стандартов, таких как MANRS (Mutually Agreed Norms for Routing Security). MANRS предлагает набор рекомендаций для операторов сетей, включая улучшение фильтрации маршрутов, предотвращение спуфинга (подделки источников IP-адресов) и обмен информацией о возможных угрозах[5].

В реальном мире даже небольшие автономные системы могут стать участниками крупных атак из-за отсутствия должной настройки маршрутов. Например, в 2018 году ложный маршрут, объявленный одной из азиатских телекоммуникационных компаний, привёл к перенаправлению трафика Google через Россию и Китай. Этот случай продемонстрировал, насколько критично глобальное сотрудничество и согласованность в сфере маршрутизации.

Заключение

BGP hijacking остаётся одной из наиболее серьёзных угроз для глобальной маршрутизации в Интернете. Учитывая отсутствие встроенных механизмов безопасности в протоколе BGP, атаки на маршруты могут использоваться как для кражи данных, так и для масштабного саботажа.

Методы противодействия, такие как внедрение RPKI, использование инструментов мониторинга и фильтрации маршрутов, а также криптографическая защита, являются ключевыми инструментами в борьбе с этой угрозой. Однако их эффективность напрямую зависит от готовности операторов сетей инвестировать в новые технологии и сотрудничать на глобальном уровне.

Для обеспечения надёжной защиты необходимо не только внедрять технические меры, но и следовать стандартам безопасности, таким как MANRS, которые способствуют повышению устойчивости всей маршрутизационной экосистемы. В эпоху растущих угроз BGP hijacking играет всё более важную роль в дискуссиях о будущем Интернета, подчёркивая необходимость совместных усилий в области сетевой безопасности.

Список литературы

1. 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.
2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. Лаврова Д. С. и др. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 3. – С. 70-77.
4. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
5. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры / А. М. Гельфанд, В. В. Сигачева, А. В. Архипов, Л. К. Сиротина // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2023. – № 3. – С. 21-27. – DOI 10.46418/2079-8199_2023_3_3. – EDN BKGRAY.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
 2. Lesnova E. M., Pestov I. E. Development of a method error detection and correction for a distributed information network based on big data //Regional Informatics and Information Security. - 2018. – pp. 236-240.
 3. Lavrova D. S. et al. Preventing Dos attacks by predicting the values of correlation parameters of network traffic //Problems of information security. Computer systems. – 2018. – No. 3. – pp. 70-77.
 4. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 5. Analysis and risk management of information security of an object of critical information infrastructure / A.M. Gelfand, V. V. Sigacheva, A.V. Arkhipov, L. K. Sirotina // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2023. – No. 3. – pp. 21-27. – DOI 10.46418/2079-8199_2023_3_3. – EDN BKGRAY.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.42

МОДЕЛЬ ПРОГРАММНОГО ИНТЕРФЕЙСА ДЛЯ ИСПОЛЬЗОВАНИЯ В НЕЙРОННОМ ПРОТЕЗЕ КОНЕЧНОСТИ ПРЯМОГО ПОДКЛЮЧЕНИЯ

¹Мухортов А.А., ²Усюкин Н.А.

¹НАО КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ, Алматы, Казахстан (50040, г.Алматы, Бостандыкский район, проспект Аль-Фараби, дом 71), e-mail: artur.mukhortov@gmail.com

²АО "КАЗАХСТАНСКО-БРИТАНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ", Алматы, Казахстан (50000, г.Алматы, Алмалинский район, улица Толе Би, дом 59).

В работе представлено исследование, посвящённое созданию технологий управления нейропротезами, основанных на прямом взаимодействии с нервной системой. Потеря конечностей существенно снижает качество жизни и социально-экономическое положение человека, что делает развитие протезов актуальной задачей современной медицины. Авторами была проведена сравнительная оценка проводимости нервной и мышечной тканей, что подтвердило более высокую эффективность нервных тканей для передачи электрических сигналов. Разработана программная модель нейронного интерфейса, включающая симуляцию активности мотонейронного пула и алгоритм преобразования нейронных сигналов в управляющие команды для протезных систем. Результаты моделирования продемонстрировали, что использование нервных сигналов позволяет значительно повысить точность управления протезом, снизить утомляемость мышц и расширить функциональные возможности искусственных конечностей. Работа закладывает теоретические основы для разработки более совершенных и доступных протезных устройств, которые смогут улучшить качество жизни людей с ампутацией и двигательными нарушениями.

Ключевые слова: Нейропротезы, мотонейроны, нервная ткань, электроды, программное моделирование, управление протезами, нервные сигналы.

A SOFTWARE INTERFACE MODEL FOR USE IN A NEURAL PROSTHETIC LIMB OF DIRECT CONNECTION

¹Mukhortov A.A., ²Usyukin N.A.

¹AL-FARABI KAZAKH NATIONAL UNIVERSITY, Almaty, Kazakhstan (50040, Almaty, Bostandyk District, Al-Farabi Avenue, 71), e-mail: artur.mukhortov@gmail.com

²KAZAKH-BRITISH TECHNICAL UNIVERSITY, Almaty, Kazakhstan (50000, Almaty, Almaly district, Tole Bi Street, 59).

This study presents the development of technologies for controlling neuroprosthetics based on direct interaction with the nervous system. Limb loss significantly reduces quality of life and socio-economic status, making the development of prosthetics a critical goal in modern medicine. The authors conducted a comparative evaluation of nerve and muscle tissue conductivity, confirming the superior efficiency of nerve tissues for signal transmission. A software model of a neural interface was developed, incorporating motor neuron pool activity simulation and an algorithm for converting neural signals into control commands for prosthetic systems. The modeling results demonstrated that utilizing nerve signals significantly improves prosthetic control accuracy, reduces muscle fatigue, and expands the functional capabilities of artificial limbs. This research establishes a theoretical foundation for the development of more advanced and accessible prosthetic devices, capable of improving the quality of life for individuals with amputations and motor impairments.

Keywords: Neuroprosthetics, motor neurons, nerve tissue, electrodes, software modeling, prosthetic control, neural signals.

Введение

Потеря конечности негативно влияет на качество жизни человека, ограничивая его функциональные возможности и создавая серьёзные социальные и экономические трудности. Восстановление утраченных функций остаётся актуальной задачей здравоохранения. Хотя современные технологии позволяют создавать роботизированные и бионические протезы, их функциональность всё ещё уступает естественным конечностям. Такие устройства зачастую неудобны, сложны в управлении и имеют ограниченные возможности [1].

Около 90% современных протезов зависят от миоэлектрических сигналов, возникающих при сокращении мышц [2]. Хотя миоэлектрические протезы представляют собой значительное достижение, они имеют недостатки: замедленная реакция на сигналы затрудняет выполнение плавных движений, сложность обеспечения обратной связи снижает эффективность управления, а произвольные мышечные сокращения вызывают нежелательные движения [3].

Для решения этих проблем мы предлагаем технологии протезирования с прямым подключением к нервной системе, которые потенциально имеют значительные преимущества.

Цель данного исследования заключается в создании основы для разработки устройств, способных считывать и обрабатывать нейронные сигналы — основного компонента будущих нейропротезов.

Научная и практическая значимость работы заключается в создании базы для разработки протезов, функционально приближенных к естественным конечностям. Новизна исследования состоит в разработке технологии, пока ограниченно используемой в мировой практике. Практическая значимость работы — в создании систем, способных эффективно восстанавливать функции конечностей, улучшая качество жизни и способствуя восстановлению работоспособности.

Морфология и физиология нейрона; анатомические основы нервной системы

Нейрон — это специализированная клетка, обладающая способностью проводить и передавать электрические импульсы. Основу её электрической активности составляет цитоплазматическая мембрана.

Нейрон состоит из тела, называемого «сомой» (диаметр от 5 до 100 мкм), и цитоплазматических выростов — дендритов и аксона.

Дендриты проводят импульсы от периферии к телу нейрона. В зависимости от количества отростков нейроны классифицируются на:

- униполярные (имеют один отросток, выполняющий функции аксона и дендрита),
- биполярные (имеют по одному аксону и дендриту),
- псевдоуниполярные (один аксон, разделённый на две ветви),
- мультиполярные (один аксон и несколько дендритов).

Дендриты формируют синаптические контакты с другими нейронами или преобразуются в структуры, преобразующие внешние воздействия в электрическую активность.

Аксон — одиночный вырост цитоплазмы, ответственный за передачу импульсов от тела нейрона к периферии. На его концах расположены специализированные мембранные и

цитоплазматические структуры, обеспечивающие либо синаптическую передачу, либо нейросекреторную активность [4].

Нервная система условно делится на центральную (ЦНС) и периферическую (ПНС).

- ЦНС включает головной и спинной мозг;
- ПНС состоит из 12 пар черепных нервов, выходящих из черепа и направленных к органам чувств, другим органам, коже или мышцам головы и шеи; 31 пары спинномозговых нервов, а также нервных узлов и сплетений;

Черепные нервы подразделяются по функциям:

- чувствительные: I, II, VIII пары;
- двигательные: III, IV, VI, XI, XII пары;
- смешанные: V, VII, IX, X пары [5].

Спинные нервы относятся к смешанным и соединяются со спинным мозгом, регулируя передачу двигательной и сенсорной информации между периферией и ЦНС.

Эфферентные двигательные волокна передают сигналы от мотонейронов передних рогов спинного мозга к скелетным мышцам через нервно-мышечные соединения. Они подразделяются на:

- альфа-волокна, иннервирующие экстрафузальные мышечные волокна;
- гамма-волокна, иннервирующие волокна мышечных веретен.

Естественные движения тела обеспечиваются эфферентными сигналами, идущими от ЦНС к ПНС для активации мышц. Одновременно сенсорная информация от механорецепторов и проприорецепторов передаётся в ЦНС по афферентным волокнам.

Нейронная активность проявляется в виде миллисекундных всплесков мембранного потенциала (80–100 мВ), известных как потенциалы действия или «спайки» [6]. Интенсивность сигналов кодируется частотой импульсов по периферическим аксонам [7].

Анализ типов протезов верхних конечностей

С функциональной точки зрения протезы верхних конечностей делятся на три основные категории: механические, моторизованные и гибридные, которые объединяют характеристики первых двух.

Механические протезы обычно представляют собой систему тросов или кабелей, соединяющих терминальное устройство с наплечным ремнём. При натяжении троса за счёт движений плеча или руки происходит открытие или закрытие протезной кисти или крюка. Однако такая система позволяет управлять лишь одной степенью свободы движения. Моторизованные протезы приводятся в действие электрическим мотором, питаемым от батареи. Они подразделяются на два типа: миоэлектрические и управляемые сигналами центральной нервной системы, различающиеся по способу получения управляющих сигналов [1].

Миоэлектрические протезы используют электромиографические сигналы для активации функций руки или кисти. Несмотря на коммерческую доступность и прогресс, эти протезы ограничены в степенях свободы, требуют сложного управления и часто неудобны. Проблемы включают избыточный вес, ограниченную ёмкость батарей и трудности с несколькими степенями свободы. Слабая подгонка гнезда и потоотделение также снижают эффективность [1]. Кроме того, использование миоэлектрических протезов часто не является интуитивно понятным, поскольку сигналы генерируются мышцами для выполнения функций, не

соответствующих их естественному предназначению (например, сокращение бицепса для закрытия протезной кисти). Это создаёт особые трудности для пользователей с ампутацией на уровне плечевого сустава или выше. Несмотря на достижения в этой области, уровень отказа от использования протезов верхних конечностей остаётся высоким [8].

Протезы, управляемые центральной нервной системой, функционируют благодаря корковым сигналам, позволяя осуществлять контроль над протезом через интерфейс «мозг-компьютер». Данный метод использует как инвазивные, так и неинвазивные технологии для регистрации и интерпретации сигналов центральной и периферической нервной системы [9]. В ранних исследованиях интерфейс «мозг-компьютер» применялся у приматов в виртуальной среде для управления конкретными действиями посредством обратной связи от нервной системы, что позволило животным контролировать нейропротез, закреплённый на стационарной платформе. Другие исследования показали точное соответствие между началом стимуляции нейронов и выполняемым движением через прямую корковую стимуляцию [10, 11]. Дальнейшее развитие интерфейса «мозг-компьютер» привело к исследованию, в котором человеку с тетраплегией была предоставлена возможность управлять движением стационарного моторизованного протеза [12].

Обзор существующих протезных интерфейсов и электродов

Электроды играют ключевую роль в регистрации и стимуляции нейронной активности. Типы электродов, используемых во взаимодействии с ПНС, могут включать, но не ограничены, следующими типами устройств: электроды-манжеты [13], внутripучковые электроды [14] и проникающие микроэлектродные матрицы [10]. Помимо этого, имеются примеры регенеративных подходов к вживлению электродов [11].

Манжетные электроды получили широкое распространение в качестве интерфейсов периферических нервов из-за их относительной простоты изготовления и усовершенствования [13]. В классическом варианте электрод-манжета с разъемным цилиндром представляет собой цилиндрическую трубку, разрезанную в продольном направлении и помещенную вокруг нерва [10]. Электрические контакты внутри трубки могут быть концентрическими или продольными, а размер электрода должен быть заранее определен в соответствии с нервом-мишенью [15]. Одним из вариантов манжетных электродов являются спиральные манжетные электроды. Эти устройства состоят из электродов, встроенных в самозакручивающуюся изолированную оболочку, которая имеет спиральное поперечное сечение. Их основным преимуществом является возможность подстраиваться под диаметр нерва, что позволяет использование даже в случае отека нервов [16], который является одной из реакций на имплантацию [17].

В нерве с несколькими пучками группы мотонейронов рассеяны среди пучков. Эти пучки расположены в нерве по-разному, поэтому их избирательная стимуляция может быть достигнута с помощью электродов, расположенных по соседству [14]. Существует два основных типа внутripучковых электродов в зависимости от способа их крепления: продольный внутripучковый электрод (LIFE) и поперечный внутripучковый многоканальный электрод (TIME) [10]. Эти электроды обеспечивают непосредственный контакт с нервными волокнами, что повышает точность регистрации и стимуляции [18].

Другой метод внутripучкового взаимодействия заключается в использовании проникающей микроэлектродной матрицы, вводимой поперечно в периферический нерв. Эти

устройства состоят из множества крошечных электродов, позволяя регистрировать и стимулировать нейронную активность в широком диапазоне [10]. Микроэлектродные матрицы захватывают сигналы от нейронов либо по отдельности (от одного нейрона), либо многократно (от нескольких нейронов). Благодаря своей близости одиночные и множественные сигналы призваны обеспечить большую специфичность в кодировании двигательной информации [19].

Регенеративные электроды стимулируют рост нервных волокон на поверхности электрода, обеспечивая долговременную стабильность контакта. Для индукции роста нервных волокон на электроде были предложены различные методы, такие как использование топографических сигналов, хемоаттрактантов, покрытий и биологических препаратов [11]. Примером является полиимидный сетчатый электрод, который имплантируется в перерезанный нерв и стимулирует регенерацию миелиновых волокон [11].

Даже спустя десятилетия после ампутации периферическая нервная система сохраняет способность передавать произвольные двигательные команды фантомной конечности [20]. Как в случае моторных, так и сенсорных протезов, нейронный интерфейс может находиться на корковом уровне, включая черепные нервы; на уровне спинного мозга; или на периферическом уровне нервной системы [19]. Нейронные электроды представляют собой инвазивную сенсорную систему обратной связи. Управление протезом может быть достигнуто с помощью двигательных команд, генерируемых импульсами нейронов. Каждый сигнал содержит различные характеристики, такие как полоса частот и амплитуда, но все они могут нести информацию о намерениях движения [21]. Потенциалы действия или спайки, возникающие в результате срабатывания отдельных нейронов, могут быть извлечены из необработанных сигналов, записанных с помощью микроэлектродной матрицы, для управления или интуитивной активации роботизированной конечности [22].

Эксперименты сравнительной проводимости мышцы и нерва

Для оценки сравнительной проводимости проведены два вскрытия на взрослых озёрных лягушках (*Pelophylax ridibundus*) согласно методике в Работе 1: «Приготовление нервно-мышечного препарата лягушки» [23]. Подготовленный нервно-мышечный препарат фиксировался вертикально: бедренная кость закреплена на кронштейне кимографа, ахиллово сухожилие — на рычаге с пишущей иглой. Скорость вращения барабана выставлялась на минимальное значение, частота раздражения — 1 Гц.

Электростимуляция проводилась двумя электродами: сначала оба подключались к мышце, затем анод — к нерву, а катод оставался на мышце. Наибольшая амплитуда сокращений регистрировалась при подключении анода к нерву, что указывает на более эффективное распределение сигнала через нервную ткань. Напротив, прямая мышечная стимуляция вызывала повышенную утомляемость и снижение амплитуды сокращений.

Сравнительная характеристика, показанная на Рисунке 1 свидетельствует о том, что стимуляция с подключением к нерву и к мышце имеет более высокие показатели сокращения, чем простое раздражение мышцы током, которая является исполнительным органом. Это наглядно демонстрирует факт того, что нервная ткань является более благоприятной средой для проведения импульса, а значит и наиболее подходящей для точного снятия управляющего сигнала, по сравнению с мышцами.

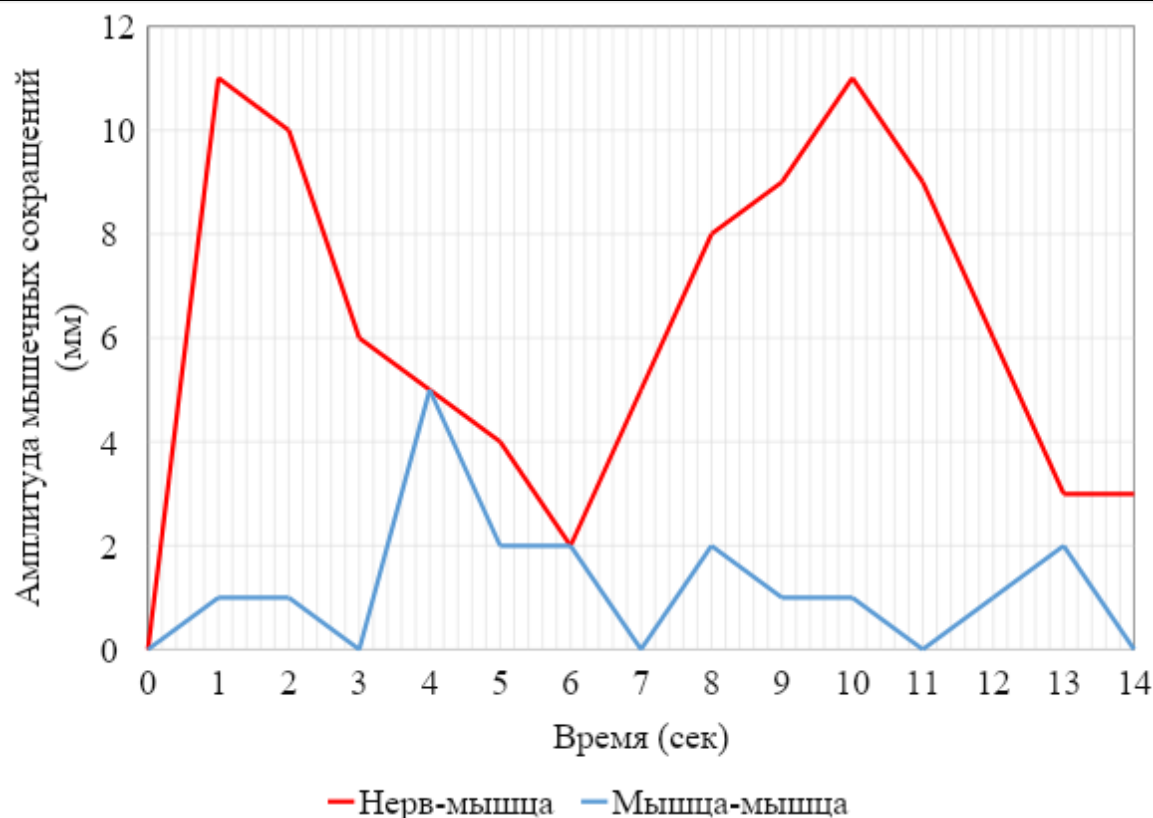


Рисунок 1 - График сравнительной характеристики мышечных сокращений при разном подключении стимулирующих электродов (к мышце и нерву, к мышце и мышце)

Концепция моделирования нейронной активности

В рамках данного исследования была создана программная модель нейропротеза, включающая симуляцию активности мотонейронов и системы управления протезом. Цель состояла в разработке алгоритмов, способных интерпретировать нейронные сигналы и преобразовывать их в управляющие команды для протеза.

Модель основывалась на физиологических особенностях мотонейронов, которые являются не просто проводниками сигналов, но и компонентами сложных сетей. Мотонейроны организованы в пулы, иннервирующие конкретные мышцы, а связь между мышцей и пулом мотонейронов является взаимно однозначной. Один мотонейрон может иннервировать множество мышечных волокон, образуя двигательную единицу, а сила сокращения мышцы регулируется частотой импульсации и правилом Хеннемана [24].

Получение и обработка нейронных сигналов

Согласно гипотезе, нервная ткань может использоваться как проводник сигналов, к которому подключается биосовместимый микроэлектрод. Через этот электрод биоэлектрические сигналы считываются, обрабатываются и преобразуются в команды для протеза, такие как сгибание. Система алгоритмов симулировала активность пула мотонейронов, а полученные сигналы преобразовывались в угловую скорость конечности. Физическое моделирование взаимодействия нейронов и электродов не проводилось; использовались программно сгенерированные сигналы, выделенные в общий компонент, обозначающий сокращение мышцы.

Для разработки эффективной системы управления протезом была создана программная модель, имитирующая активность мотонейронного пула и преобразующая эту активность в управляющие сигналы для протезной системы. Основой модели послужили физиологические особенности управления движением конечностей, где сгибание и разгибание в суставе контролируются двумя противоположными группами мышц — сгибателями и разгибателями, которые должны работать согласованно.

Модель была реализована на языке C++, а результаты симуляции сохранялись в CSV-файлы для последующей обработки. Для визуализации данных использовались скрипты на Python с библиотекой Matplotlib.

Моделирование мотонейронной активности

Во время сокращения одной группы мышц противоположная группа должна подавляться для предотвращения противоположного усилия. Это подавление осуществляется тормозными интернейронами в спинном мозге [24]. В нашей модели учтена эта особенность через включение тормозных нейронов, влияющих на активность пула мотонейронов противоположной мышцы.

Для симуляции активности нейронной сети использовалась программа с открытым исходным кодом, имплементирующая математическую модель Ижикевича, описывающая динамику нейронов с помощью системы дифференциальных уравнений:

$$\begin{cases} C_m \frac{dv}{dt} m = k (V_m - V_r)(V_m - V_t) - U_m + I_{ex} + I_{syn} \\ \frac{dU_m}{dt} = a(b(V_m - V_r) - U_m) \end{cases}$$

Если $V_m \geq V_{peak}$, то

$$\begin{cases} V_m = c \\ U_m = U_m + d, \end{cases}$$

где C_m — ёмкость нейрона пкФ, V_m — мембранный потенциал мВ, V_{peak} — пиковое значение мембранного потенциала, при достижении которого происходит генерация спайка и сбрасывание значений V_m и U_m , V_r , V_t — это вспомогательные параметры, имеющие размерность напряжения, c — значение мембранного потенциала, к которому сбрасывается состояние нейрона при возникновении спайка, U_m — вспомогательная переменная. I_{syn} и I_{ex} — суммарный синаптический ток и постоянный внешний приложенный ток, соответственно, пкА, a , b , d , k — вспомогательные параметры нейрона [25].

Далее мы приступили непосредственно к симуляции. Для проведения симуляции были использованы основные данные о моторных единицах двуглавой мышцы плеча человека, представленные в таблице 1. Эти данные основаны на эмпирических исследованиях [26, 27, 28, 29].

Одним из ключевых параметров симуляции является соотношение числа ингибирующих нейронов к возбуждающим, которое составляет 1:10 согласно литературным данным [30, 31].

Вероятность связей между нейронами также была взята из научных исследований и составляет 10% (0,1) [32]. Все необходимые параметры моделирования были занесены в Таблицу 2.

Таблица 1. - Данные по моторным единицам двуглавой мышцы плеча

Мышца	Количество моторных аксонов	Количество мышечных волокон	Коэффициент иннервации
Двуглавая мышца плеча (<i>biceps brachii</i>)	312 ± 51	194 138 ± 59 896	622

Таблица 2. - Параметры моделирования сгибания руки в локтевом суставе (общие для осциллограмм и спайковой активности)

Номер симуляции	Число нейронов		Вероятность связи	Время симуляции (мс)
	Возбуждающие	Тормозные		
1	250	25	0,1	1000
2	260	26	0,1	1000
3	270	27	0,1	1000
4	280	28	0,1	1000
5	290	29	0,1	1000
6	300	30	0,1	1000
7	310	31	0,1	1000
8	320	32	0,1	1000
9	330	33	0,1	1000
10	340	34	0,1	1000
11	350	35	0,1	1000

В соответствии с данными в Таблице 2 было проведено моделирование нейронной активности пула мотонейронов с выводом результатов биоэлектрической активности, которые можно видеть на Рисунке 2.

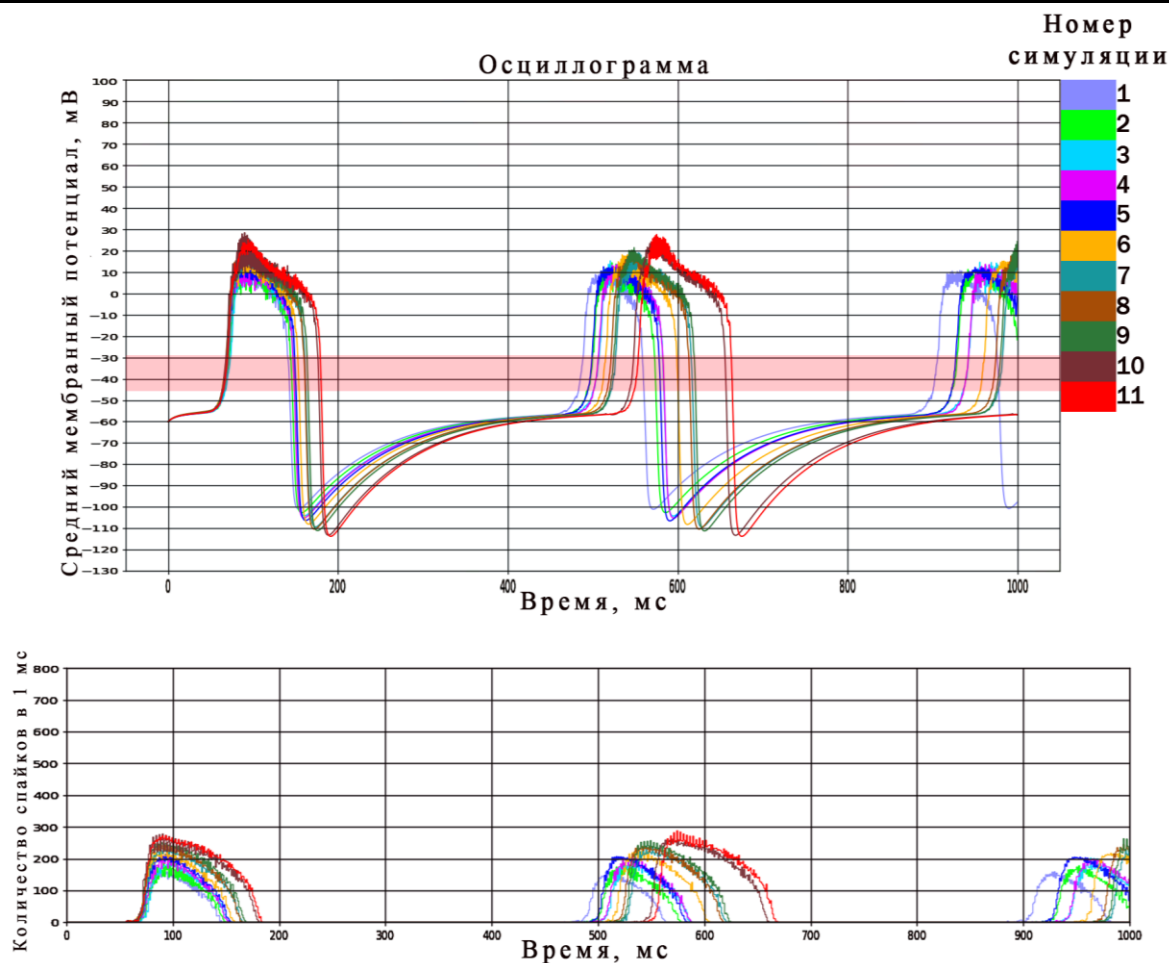


Рисунок 2. - Осциллограмма и график спайковой активности в соответствии с табличными данными

Программная интеграция нейронных сигналов в протезные системы

На основе анализа результатов моделирования мотонейронной активности был разработан алгоритм, который принимает входные данные от модели и генерирует управляющий сигнал, определяющий функционирование протеза.

Алгоритм функционирует следующим образом. На вход подаются данные, сформированные в рамках модели мотонейронной активности, описанной в предыдущих разделах. Эти данные обрабатываются для определения относительной силы сокращения искусственной «мышцы» протеза. Общая логика работы алгоритма включает следующие этапы:

- определение активации искусственной мышцы. На основании осциллограммы (Рисунок 2) проверяется, достигает ли напряжение порогового значения (-55 мВ, обозначено красным). Если порог не достигается, протез остаётся в режиме ожидания;
- считывание числа спайков. При активации искусственной мышцы алгоритм анализирует число спайков, зарегистрированных в одну миллисекунду (Рисунок 2). Эти данные выступают в роли ключевого параметра для расчёта последующих величин.

- расчёт силы сокращения. На основе числа спайков определяется сила сокращения мышцы. Для этого учитывается максимальное количество мотонейронов, способных активировать мышцу в заданных моделируемых условиях. Расчёт производится в относительных величинах, что позволяет учитывать различия в моделируемых параметрах.
- определение угловой скорости и угла сгибания. На основании силы сокращения алгоритм вычисляет угловую скорость конечности и угол её сгибания. Эти параметры определяют точное положение протеза в каждый момент времени. Константы взяты из данных исследования [33], где максимальная угловая скорость руки в локтевом суставе составляет 1248 градусов в секунду, минимальный угол равен 0 градусам, а максимальный — 135 градусов.

Особенностью предложенного алгоритма является использование осциллограммы в роли "выключателя" для активации искусственной мышцы. Это позволяет минимизировать вероятность ложных активаций и обеспечивает стабильность работы системы в условиях неопределённости входных сигналов.

Результаты симуляции, включающие графики, демонстрирующие взаимосвязь между активностью нейронов и сокращением искусственной мышцы протеза, представлены на рисунке 3. Эти результаты подтверждают, что алгоритм способен надёжно интерпретировать нейронные сигналы и преобразовывать их в управляющие команды, обеспечивая плавное и точное движение протеза.

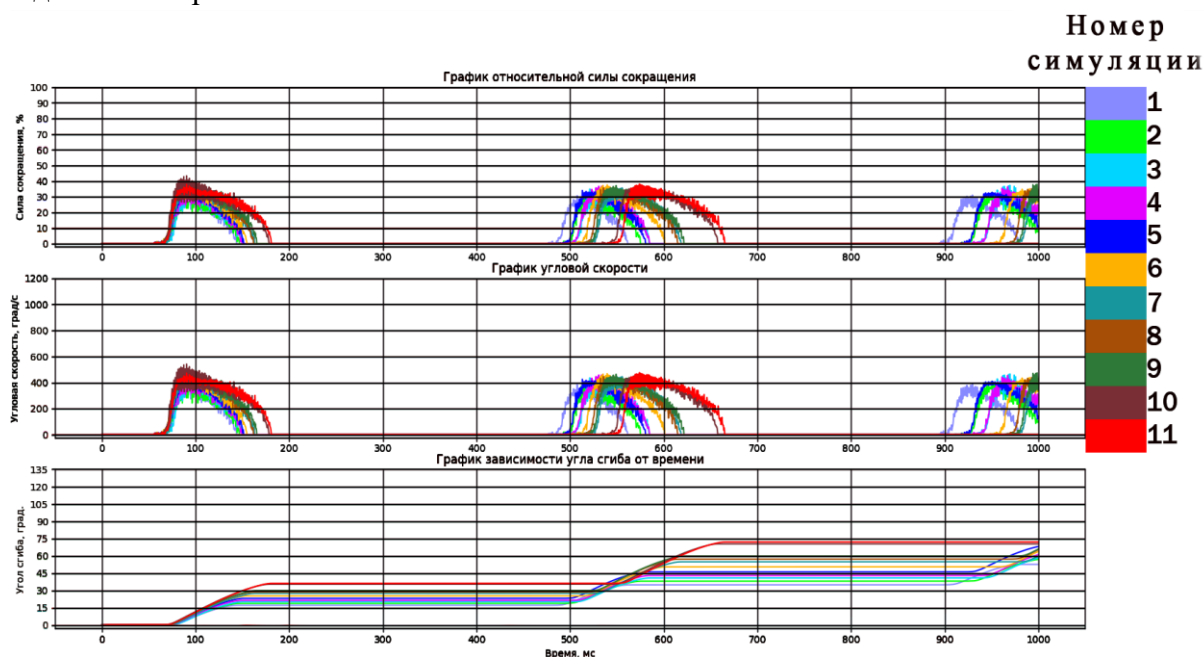


Рисунок 3. - Графики относительной силы сокращения, угловой скорости и угла сгиба конечности в зависимости от результатов симуляции активности мотонейронного пула

Выводы

В результате проведённых экспериментов было подтверждено, что нервная ткань является более благоприятной средой для проведения импульсов по сравнению с мышечной тканью. Проведённые опыты показали, что стимуляция нервной ткани вызывает более сильные и продолжительные сокращения мышц. Это подтверждает гипотезу о возможности использования нервных сигналов для управления нейропротезами. Так как мышца является,

по большей части, исполнительным органом и снятие с неё сигнала, как это происходит в большинстве нынешних протезных системах, является не самым оптимальным решением. Снятие же управляющего сигнала с нервной ткани дало нам возможность получить менее искаженный выходной сигнал, что потенциально должно повысить точность протезной системы. На основании этой информации была проведена симуляция нейронной активности по модели Ижикевича. Для простоты моделирования, в качестве примера человеческой конечности мы брали руку, а конкретно её локтевой сустав. Антагонизм работы сгибателя и разгибателя локтевого сустава лежал в основе моделирования нейронной активности, которая затем была использована для написания собственной программы, интерпретирующей активность сети в один из аспектов управляющего сигнала. В нашем случае был взят угол сгиба руки в локтевом суставе в определённую единицу времени (секунда). Зная, что угловая скорость сгибания руки в рамках заданного времени не должна превышать 1248 град/с, мы написали программу, которая регистрировала активность нейронной сети на основе данных симуляции по модели Ижикевича. Далее алгоритм выводил соответствующий угол сгиба за единицу времени, что позволяло оценить преодолимое расстояние конечности при разных степенях стимулирующего сигнала.

На основании проведённого исследования была доказана гипотеза о том, что паттерны электрических нейронных сигналов могут быть использованы в качестве основы для формирования управляющих сигналов нейропротеза человеческой конечности, а нервная ткань потенциально является более благоприятной средой для проведения сигнала, что делает её перспективной проводящей системой для снятия сигнала с минимальными искажениями.

Эти результаты подтверждают выдвинутую гипотезу и закладывают теоретические основы для создания более совершенных протезных систем, что в перспективе может значительно улучшить качество жизни людей с ампутациями и другими двигательными нарушениями.

Список литературы

1. Паскуина П.Ф., Перри Б.Н., Миллер М.Е., Линг Г.Ф., Цао Ю.В. Последние достижения в области биоэлектрических протезов. Неврологическая клиника. Апрель 2015 г.;5(2):164-170. doi: 10.1212/CPJ.0000000000000132. PMID: 29443190; PMCID: PMC5764448.
2. Брэк Р., Амалу Э. Обзор технологий, материалов и научно-исследовательских разработок в области протезирования верхних конечностей для повышения удобства использования. Июль 2020, 25 декабря;23:88-96. doi: 10.1016/июль 2020.12.009. PMID: 33442223; PMCID: PMC7787923.
3. Чедвелл А., Кенни Л., Тис С., Галпин А., Хэд Дж. Реальность миоэлектрических протезов: понимание того, что затрудняет управление этими устройствами для некоторых пользователей. Фронтальный нейроробот. 22 августа 2016 г.,10:7. doi: 10.3389/fnbot.2016.00007. Ошибка в: Front Neurorobot. 03 апреля 2018,12:15. doi: 10.3389/fnbot.2018.00015. PMID: 27597823; PMCID: PMC4992705.
4. В.В. Жуков, Е.В. Пономарева. Анатомия нервной системы: Высшее образование / Калин. ун-т. - Калинин, 1998. - 68 с. - ISBN 5-88874-092-6.

5. А. А. Швырев ; под общ. ред. Р. Х. Морозовой. — Изд. 8-е, стер. — Ростов-на-Дону : Хеникс, 2015. — 411, [1] с. : ил. : 21 см — (Серия "Среднее медицинское образование");; ISBN 978-5-222-23982-7.
6. Кандел, Эрик Р., Джеймс Х. (Джеймс Харрис) Шварц и Томас М. Джасселл. Принципы нейронауки. 4-е изд. Нью-Йорк: McGraw-Hill, Отдел медицинских профессий, 2000. Печать.
7. Наварро Х., Крюгер Т. Б., Лаго Н., Микера С., Стиглиц Т. и Дарио П. (2005). Критический обзор интерфейсов с периферической нервной системой для управления нейропротезами и гибридными бионическими системами. Журнал периферической нервной системы, 10 (3), 229-258. <https://doi.org/https://doi.org/10.1111/j.1085-9489.2005.10303.x>
8. Биддисс, Э. А., & Чау, Т. Т. (2007). Использование протезов верхних конечностей и отказ от них: обзор за последние 25 лет. Международная организация по протезированию и ортопедии, 31 (3), 236-257. <https://doi.org/10.1080/03093640600994581>
9. Валлабханени, Т. Ванг, Б. Хе, Интерфейс мозг—компьютер в области нейронной инженерии (Спрингер, Бостон, Массачусетс, 2005), стр. 85-121 https://doi.org/10.1007/0-306-48610-5_3
10. Ёылдыз К. А., Шин А. Ю., Кауфман К. Р. (2020). Взаимодействие с периферической нервной системой для управления нейропротезированной конечностью: обзор. Журнал нейроинженерии и реабилитации, 17 (1), 43. <https://doi.org/10.1186/s12984-020-00667-5>
11. Томпсон К. Х., Зоратти М. Дж., Лангхалс Н. Б. и Перселл Э. К. (2015). Регенеративные электродные интерфейсы для нейронных протезов. Тканевая инженерия, часть В: Обзоры, 22 (2), 125-135. <https://doi.org/10.1089/ten.teb.2015.0279>
12. Коллинджер Дж. Л., Водлинджер Б., Дауни Дж. Э., Ванг У., Тайлер-Кабара Э. С., Веллисте М., Бонингер М. Л. и Шварц А. Б. (2013). Высокоэффективное нейропротезирование у человека с тетраплегией. The Lancet, 381(9866), 557-564. [https://doi.org/10.1016/S0140-6736\(12\)61816-9](https://doi.org/10.1016/S0140-6736(12)61816-9)
13. Лиссандрелло К. А., Гиллис У. Ф., Шен Дж., Пирр Б. В., Витале Ф., Паскуали М., Холински Б. Дж., Чу Д. Дж., Уайт А. Э. и Гарднер Т. Дж. (2017). Наноклипс, пригодный для печати в микромасштабе, предназначен для электростимуляции и регистрации работы мелких нервов. Журнал нейронной инженерии, 14 (3), 36006. <https://doi.org/10.1088/1741-2552/aa5a5b>
14. Велтинк П. Х., ван Вин Б. К., Струйк Дж. Дж., Холсхаймер Дж., Бум Х. Б. К. (1989). Модельное исследование стимуляции нервных пучков. IEEE Transactions on Biomedical Engineering, 36 (7), 683-692. <https://doi.org/10.1109/10.32100>
15. Рассел К., Рош А. Д. и Чакрабартти С. (2019). Бионический интерфейс для периферических нервов: обзор электродов. International Journal of Intelligent Robotics and Applications, 3 (1), 11-18. <https://doi.org/10.1007/s41315-019-00086-3>
16. Нейплс, Грегори Г. и др. "Спиральный нервный манжетный электрод для стимуляции периферических нервов". Труды IEEE по биомедицинской инженерии 35.11 (1988): 905-916.
17. Андерсон Д.М., Родригес А., Чанг Д.Т. Реакция инородного тела на биоматериалы. Иммунол. Апрель 2008 г.;20(2):86-100. doi: 10.1016/j.smim.2007.11.004. Epub, 26 декабря 2007. PMID: 18162407; PMCID: PMC2327202.

18. Рейнбек, Э. Х., Элевелд, Н., Олтуис, У. (2018). Обновленная информация об электродах для периферических нервов для нейропротезирования с замкнутым контуром. Рубежи в нейронауке, 12. <https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2018.00350>
19. Осборн Л. Э., Беттхаузер Дж. Л. и Такор Н. В. (2019). Нейронные протезы. В Энциклопедии электротехники и электроники Уайли (стр. 1-20). <https://doi.org/https://doi.org/10.1002/047134608X.W1424.pub2>
20. Цзя, Х., Кениг, М. А., Чжан, Х., Чжан, Дж., Чен, Т. и Чен, З. (2007). Остаточный двигательный сигнал при длительном повреждении периферических нервов у человека и возможность создания искусственной конечности, управляемой нервными сигналами. Журнал хирургии кисти, 32 (5), 657-666. <https://doi.org/10.1016/j.jhsa.2007.02.021>
21. Осборн Л. Э., Искарюс М. М. и Такор Н. В. (2020). Глава 22 - Сенсорика и управление протезами кистей в клинических и исследовательских целях. Розен и П. У. Фергюсон (ред.), "Носимая робототехника" (стр. 445-468). Academic Press. <https://doi.org/https://doi.org/10.1016/B978-0-12-814659-0.00022-9>
22. Веллисте М., Перель С., Сполдинг М. С., Уитфорд А. С. и Шварц А. Б. (2008). Кортикальный контроль протеза руки для самостоятельного питания. Nature, 453 (7198), 1098-1101. <https://doi.org/10.1038/nature06996>
23. Маркеева С.С., Сраилова Г.Т., Аскарова З.А. Руководство к лабораторным занятиям по физиологии человека и животных: учебное пособие. – Алматы: Қазақ университеті, 2012. – 151 с. ISBN 978-601-247-545-6
24. Книрим, Дж., 2022. Двигательные единицы и мышечные рецепторы (раздел 3, глава 1) Neuroscience Online: Электронное учебное пособие для отделения неврологии | нейробиологии и анатомии Медицинской школы Техасского университета в Хьюстоне. [онлайн] Nba.uth.tmc.edu. Доступно по адресу: <https://nba.uth.tmc.edu/neuroscience/m/s3/chapter01.html>
25. Исир П. М., Симонов А. А. «ВВЕДЕНИЕ в ПЕРСОНАЛЬНЫЙ ГПГПУ ДЛЯ МОДЕЛИРОВАНИЯ ДИНАМИКОВ спайковых нейронных СЕТЕЙ» Учебно-методическое пособие.: маг-ридис. Радиофизика: 011800. - Нижний Новгород, 2014. http://hpc-education.unn.ru/files/5-100-Materials/7.1.3_Publications/16/Esir_gpgpu_last.pdf
26. Бухтал Ф. И Шмальбрух Х. (1980). Двигательная единица мышц млекопитающих. Физиологические обзоры, 60 (1), 90-142. <https://doi.org/10.1152/physrev.1980.60.1.90>
27. Доэрти Т. Дж., Браун В.Ф. Оценочное количество и относительные размеры тенарных двигательных единиц, выбранных при многоточечной стимуляции у молодых и пожилых людей. Мышечный нерв. 1993, апрель;16(4):355-66. doi: 10.1002/mus.880160404. Идентификационный номер: 8455648.
28. Лекселл Дж., Хенрикссон-Ларсен К., Винблад Б., Шестрем М. Распределение различных типов волокон в скелетных мышцах человека: влияние старения изучается на поперечных срезах целых мышц. Мышечный нерв. Октябрь 1983 г.;6(8):588-95. doi: 10.1002/mus.880060809. PMID: 6646161.
29. Энока Р.М. Морфологические особенности и паттерны активации двигательных единиц. Клиника нейрофизиологии. Ноябрь 1995 г.;12(6):538-59. doi: 10.1097/00004691-199511000-00002. PMID: 8600170.

30. Свенсон О. К., Маффей А. (2019). От найма к увольнению: активация тормозных нейронов и их вовлечение в поведение. Рубежи молекулярной нейронауки, 12. <https://doi.org/10.3389/fnmol.2019.00168>
31. Рамирес-Яркин, ООН, Лазо-Гомес, Р., Товар-и-Ромо, Л. Б., и Тапия, Р. (2014). Спинномозговые тормозные цепи и их роль в дегенерации двигательных нейронов. Нейрофармакология, 82, 101-107. <https://doi.org/https://doi.org/10.1016/j.neuropharm.2013.10.003>
32. Кин О. Расшифровка организации спинномозговых цепей, управляющих локомоцией. Nat Rev Neurosci. 2016, апрель;17(4):224-38. doi: 10.1038/nrn.2016.9. Epub, 3 марта 2016. PMID: 26935168; PMCID: PMC4844028.
33. Вернер С.Л., Джонс Д.Г., Гвидо Дж.А., Брюне М.Е. Кинематика и кинетика подачи элитного софтбольного мяча на ветряной мельнице. Am J Sports Med. 2006, апрель;34(4):597-603. doi: 10.1177/0363546505281796. Опубликовано 10 ноября 2005 года. PMID: 16282576.

References

1. Pasquina PF, Perry BN, Miller ME, Ling GSF, Tsao JW. Recent advances in bioelectric prostheses. Neurol Clin Pract. 2015 Apr;5(2):164-170. doi: 10.1212/CPJ.0000000000000132. PMID: 29443190; PMCID: PMC5764448.
2. Brack R, Amalu EH. A review of technology, materials and R&D challenges of upper limb prosthesis for improved user suitability. J Orthop. 2020 Dec 25;23:88-96. doi: 10.1016/j.jor.2020.12.009. PMID: 33442223; PMCID: PMC7787923.
3. Chadwell A, Kenney L, Thies S, Galpin A, Head J. The Reality of Myoelectric Prostheses: Understanding What Makes These Devices Difficult for Some Users to Control. Front Neurobot. 2016 Aug 22;10:7. doi: 10.3389/fnbot.2016.00007. Erratum in: Front Neurobot. 2018 Apr 03;12:15. doi: 10.3389/fnbot.2018.00015. PMID: 27597823; PMCID: PMC4992705.
4. В.В. Жуков, Е.В. Пономарева. Анатомия нервной системы: Учебное пособие / Калинингр. ун-т. - Калининград, 1998. - 68 с. - ISBN 5-88874-092-6.
5. А. А. Швырев ; под общ. ред. Р. Ф. Морозовой. — Изд. 8-е, стер. — Ростов-на-Дону : Феникс, 2015. — 411, [1] с. : ил. : 21 см — (Серия "Среднее медицинское образование"); ISBN 978-5-222-23982-7.
6. Kandel, Eric R, James H. (James Harris) Schwartz, and Thomas M Jassell. Principles of Neural Science. 4th ed. New York: McGraw-Hill, Health Professions Division, 2000. Print.
7. Navarro, X., Krueger, T. B., Lago, N., Micera, S., Stieglitz, T., & Dario, P. (2005). A critical review of interfaces with the peripheral nervous system for the control of neuroprostheses and hybrid bionic systems. Journal of the Peripheral Nervous System, 10(3), 229–258. <https://doi.org/https://doi.org/10.1111/j.1085-9489.2005.10303.x>
8. Biddiss, E. A., & Chau, T. T. (2007). Upper limb prosthesis use and abandonment: A survey of the last 25 years. Prosthetics and Orthotics International, 31(3), 236–257. <https://doi.org/10.1080/03093640600994581>
9. Vallabhaneni, T. Wang, B. He, Brain—Computer Interface, in Neural Engineering (Springer, Boston, MA, 2005), pp. 85–121 https://doi.org/10.1007/0-306-48610-5_3

10. Yildiz, K. A., Shin, A. Y., & Kaufman, K. R. (2020). Interfaces with the peripheral nervous system for the control of a neuroprosthetic limb: a review. *Journal of NeuroEngineering and Rehabilitation*, 17(1), 43. <https://doi.org/10.1186/s12984-020-00667-5>
11. Thompson, C. H., Zoratti, M. J., Langhals, N. B., & Purcell, E. K. (2015). Regenerative Electrode Interfaces for Neural Prostheses. *Tissue Engineering Part B: Reviews*, 22(2), 125–135. <https://doi.org/10.1089/ten.teb.2015.0279>
12. Collinger, J. L., Wodlinger, B., Downey, J. E., Wang, W., Tyler-Kabara, E. C C., Velliste, M., Boninger, M. L., & Schwartz, A. B. (2013). High-performance neuroprosthetic control by an individual with tetraplegia. *The Lancet*, 381(9866), 557–564. [https://doi.org/10.1016/S0140-6736\(12\)61816-9](https://doi.org/10.1016/S0140-6736(12)61816-9)
13. Lissandrello, C. A., Gillis, W. F., Shen, J., Pearre, B. W., Vitale, F., Pasquali, M., Holinski, B. J., Chew, D. J., White, A. E., & Gardner, T. J. (2017). A micro-scale printable nanoclip for electrical stimulation and recording in small nerves. *Journal of Neural Engineering*, 14(3), 36006. <https://doi.org/10.1088/1741-2552/aa5a5b>
14. Veltink, P. H., van Veen, B. K., Struijk, J. J., Holsheimer, J., & Boom, H. B. K. (1989). A modeling study of nerve fascicle stimulation. *IEEE Transactions on Biomedical Engineering*, 36(7), 683–692. <https://doi.org/10.1109/10.32100>
15. Russell, C., Roche, A. D., & Chakrabarty, S. (2019). Peripheral nerve bionic interface: a review of electrodes. *International Journal of Intelligent Robotics and Applications*, 3(1), 11–18. <https://doi.org/10.1007/s41315-019-00086-3>
16. Naples, Gregory G., et al. "A spiral nerve cuff electrode for peripheral nerve stimulation." *IEEE transactions on biomedical engineering* 35.11 (1988): 905-916.
17. Anderson JM, Rodriguez A, Chang DT. Foreign body reaction to biomaterials. *Semin Immunol.* 2008 Apr;20(2):86-100. doi: 10.1016/j.smim.2007.11.004. Epub 2007 Dec 26. PMID: 18162407; PMCID: PMC2327202.
18. Rijnbeek, E. H., Eleveld, N., & Olthuis, W. (2018). Update on Peripheral Nerve Electrodes for Closed-Loop Neuroprosthetics. *Frontiers in Neuroscience*, 12. <https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2018.00350>
19. Osborn, L. E., Betthausen, J. L., & Thakor, N. v. (2019). Neural Prostheses. In *Wiley Encyclopedia of Electrical and Electronics Engineering* (pp. 1–20). <https://doi.org/https://doi.org/10.1002/047134608X.W1424.pub2>
20. Jia, X., Koenig, M. A., Zhang, X., Zhang, J., Chen, T., & Chen, Z. (2007). Residual Motor Signal in Long-Term Human Severed Peripheral Nerves and Feasibility of Neural Signal-Controlled Artificial Limb. *Journal of Hand Surgery*, 32(5), 657–666. <https://doi.org/10.1016/j.jhsa.2007.02.021>
21. Osborn, L. E., Iskarous, M. M., & Thakor, N. v. (2020). Chapter 22 - Sensing and Control for Prosthetic Hands in Clinical and Research Applications. In J. Rosen & P. W. Ferguson (Eds.), *Wearable Robotics* (pp. 445–468). Academic Press. <https://doi.org/https://doi.org/10.1016/B978-0-12-814659-0.00022-9>
22. Velliste, M., Perel, S., Spalding, M. C., Whitford, A. S., & Schwartz, A. B. (2008). Cortical control of a prosthetic arm for self-feeding. *Nature*, 453(7198), 1098–1101. <https://doi.org/10.1038/nature06996>

23. Маркеева С.С., Сраилова Г.Т., Аскарова З.А. Руководство к лабораторным занятиям по физиологии человека и животных: учебное пособие. – Алматы: Қазақ университеті, 2012. – 151 с. ISBN 978-601-247-545-6
 24. Knierim, J., 2022. Motor Units and Muscle Receptors (Section 3, Chapter 1) Neuroscience Online: An Electronic Textbook for the Neurosciences | Department of Neurobiology and Anatomy - The University of Texas Medical School at Houston. [online] Nba.uth.tmc.edu. Available at: <https://nba.uth.tmc.edu/neuroscience/m/s3/chapter01.html>
 25. Есир П. М., Симонов А. Ю. «ВВЕДЕНИЕ В ПАРАЛЛЕЛЬНЫЕ GPGPU ВЫЧИСЛЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ ДИНАМИКИ СПАЙКОВЫХ НЕЙРОННЫХ СЕТЕЙ» Учебно-методическое пособие.: маг-р дис. Радиофизика: 011800. - Нижний Новгород, 2014. http://hpc-education.unn.ru/files/5-100-Materials/7.1.3_Publications/16/Esir_gpgpu_last.pdf
 26. Buchthal, F., & Schmalbruch, H. (1980). Motor unit of mammalian muscle. *Physiological Reviews*, 60(1), 90–142. <https://doi.org/10.1152/physrev.1980.60.1.90>
 27. Doherty TJ, Brown WF. The estimated numbers and relative sizes of thenar motor units as selected by multiple point stimulation in young and older adults. *Muscle Nerve*. 1993 Apr;16(4):355-66. doi: 10.1002/mus.880160404. PMID: 8455648.
 28. Lexell J, Henriksson-Larsén K, Winblad B, Sjöström M. Distribution of different fiber types in human skeletal muscles: effects of aging studied in whole muscle cross sections. *Muscle Nerve*. 1983 Oct;6(8):588-95. doi: 10.1002/mus.880060809. PMID: 6646161.
 29. Enoka RM. Morphological features and activation patterns of motor units. *J Clin Neurophysiol*. 1995 Nov;12(6):538-59. doi: 10.1097/00004691-199511000-00002. PMID: 8600170.
 30. Swanson, O. K., & Maffei, A. (2019). From Hiring to Firing: Activation of Inhibitory Neurons and Their Recruitment in Behavior. *Frontiers in Molecular Neuroscience*, 12. <https://doi.org/10.3389/fnmol.2019.00168>
 31. Ramírez-Jarquín, U. N., Lazo-Gómez, R., Tovar-y-Romo, L. B., & Tapia, R. (2014). Spinal inhibitory circuits and their role in motor neuron degeneration. *Neuropharmacology*, 82, 101–107. <https://doi.org/https://doi.org/10.1016/j.neuropharm.2013.10.003>
 32. Kiehn O. Decoding the organization of spinal circuits that control locomotion. *Nat Rev Neurosci*. 2016 Apr;17(4):224-38. doi: 10.1038/nrn.2016.9. Epub 2016 Mar 3. PMID: 26935168; PMCID: PMC4844028.
 33. Werner SL, Jones DG, Guido JA Jr, Brunet ME. Kinematics and kinetics of elite windmill softball pitching. *Am J Sports Med*. 2006 Apr;34(4):597-603. doi: 10.1177/0363546505281796. Epub 2005 Nov 10. PMID: 16282576.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИИ И КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ

Иванов Е.А., ¹Амелютин Е.В.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ¹ kmaw2@yandex.ru

В статье проведён анализ предметной области системы обнаружения вторжений (IDS) и определены ключевые характеристики угроз безопасности в информационно-аналитических системах. Рассмотрены методы автоматической идентификации и классификации сетевых угроз на основе анализа трафика и поведения системы.

Ключевые слова: Система обнаружения вторжений, автоматическая идентификация угроз, информационная безопасность, сетевой трафик, классификация угроз.

DEVELOPMENT OF A SYSTEM FOR AUTOMATIC IDENTIFICATION AND CLASSIFICATION OF SECURITY THREATS IN AN INFORMATION AND ANALYTICAL SYSTEM

Ivanov E.A., ¹Amelutin E.V.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹ kmaw2@yandex.ru

The article analyzes the subject area of the intrusion detection system (IDS) and defines key characteristics of security threats in information and analytical systems. Methods of automatic identification and classification of network threats based on traffic analysis and system behavior are considered.

Keywords: Intrusion detection system, automatic threat identification, information security, network traffic, threat classification.

В условиях цифровой трансформации информационно-аналитические системы становятся основой для хранения, обработки и анализа данных в организациях. Рост объёмов информации и увеличение числа подключённых устройств повышают риски возникновения угроз безопасности. Для эффективного противодействия этим угрозам необходимы автоматизированные системы, способные своевременно обнаруживать и классифицировать возможные атаки. В данном исследовании рассматривается разработка системы обнаружения вторжений (IDS), обеспечивающей автоматическую идентификацию и классификацию угроз в информационно-аналитической системе.

Разработка системы автоматической идентификации и классификации угроз, являющаяся предметом данной работы, направлена на повышение защищённости информационно-аналитических систем (ИАС) путем автоматизации ключевых процессов

анализа и управления угрозами. Это особенно важно в условиях постоянно меняющихся угроз информационной безопасности, когда вручную управлять рисками становится всё сложнее.

Системы обнаружения вторжений (IDS) представляют собой ключевые компоненты информационной безопасности, предназначенные для мониторинга сетевого трафика и активности пользователей с целью выявления потенциальных угроз. В настоящее время на рынке существует множество IDS-решений, как коммерческих, так и открытых. Эти системы могут различаться по методам обнаружения, подходам к обработке данных и возможностям интеграции. Изучим классификацию существующих решений IDS, их особенности, а также проблемы и ограничения, с которыми сталкиваются традиционные системы. Также будет рассмотрено, как эти системы применяются в различных сферах, включая корпоративные сети, критическую инфраструктуру и IoT-системы.

Системы обнаружения вторжений (IDS) классифицируются по различным признакам, и одним из ключевых является метод обнаружения угроз. В этом контексте можно выделить три основных подхода: сигнатурный, аномальный и гибридный [1].

Сигнатурные системы работают на основе заранее определенных шаблонов или сигнатур, которые представляют собой записи о типичных признаках уже известных угроз. Такие системы эффективно выявляют атаки, зафиксированные в базе данных, например, вирусы, трояны и другие виды вторжений. Однако их главный недостаток заключается в том, что они не способны распознавать новые и неизвестные угрозы, которых нет в базе сигнатур.

В отличие от них, аномальные системы используют базовый профиль нормального поведения сети или пользователя. Если наблюдаемая активность отклоняется от этого профиля, система рассматривает такое поведение как потенциальную угрозу. Этот метод позволяет обнаруживать ранее неизвестные атаки, однако он сопровождается повышенным риском ложных срабатываний, особенно в сложных и динамичных сетевых средах, где нормальное поведение постоянно меняется.

Гибридные системы сочетают в себе элементы сигнатурного и аномального анализа. Такой подход позволяет более эффективно выявлять как известные, так и новые угрозы, обеспечивая при этом снижение числа ложных срабатываний. Благодаря сочетанию методов гибридные IDS демонстрируют высокую гибкость и точность, что делает их универсальными для различных сценариев обеспечения безопасности.

Таким образом, выбор метода обнаружения в IDS зависит от требований к точности, скорости реакции и способности адаптироваться к новым видам угроз.

Системы обнаружения вторжений (IDS) также классифицируются по месту их внедрения. В зависимости от уровня, на котором осуществляется мониторинг, можно выделить сетевые, хостовые и гибридные решения [2].

Сетевые IDS (NIDS) устанавливаются на уровне сети и занимаются анализом сетевого трафика, проходящего через точки подключения. Такие системы особенно эффективны для мониторинга взаимодействий между различными узлами сети. Они позволяют оперативно выявлять угрозы и атаки, происходящие на уровне передачи данных, что делает их важным инструментом для защиты сетевой инфраструктуры.

Хостовые IDS (HIDS), в свою очередь, размещаются непосредственно на конечных устройствах, таких как серверы или рабочие станции. Эти системы анализируют журналы событий, выполняемые процессы и другие данные, связанные с активностью на конкретном

устройстве. Хостовые IDS способны обнаруживать подозрительные действия, например, изменения в файловой системе или попытки несанкционированного доступа к конфиденциальной информации. Они играют важную роль в дополнении к сетевым IDS, так как могут выявлять атаки, которые остаются незамеченными на уровне сети.

Гибридные IDS объединяют функции как сетевых, так и хостовых систем, предоставляя комплексный подход к обеспечению безопасности. Такое сочетание позволяет достигнуть более полного покрытия и обеспечивать защиту как на уровне сети, так и на уровне конечных устройств. Гибридные решения эффективно выявляют широкий спектр угроз и атак, благодаря чему обеспечивается повышенная надежность и точность системы безопасности.

На рынке информационной безопасности представлено множество коммерческих систем IDS, каждая из которых разрабатывается с учётом конкретных потребностей и масштабов применения. Одним из примеров является **Cisco Secure Network Analytics** (ранее известная как **Stealthwatch**). Эта система специализируется на анализе сетевого трафика и использует технологии машинного обучения и поведенческого анализа для выявления аномальных паттернов. Благодаря высокой степени автоматизации и интуитивно понятному интерфейсу, решения Cisco особенно эффективны для крупных корпоративных сетей и объектов критической инфраструктуры.

Ещё одним широко применяемым решением является **McAfee Network Security Platform (NSP)**. Эта система использует комбинацию сигнатурных и аномальных методов для анализа сетевого трафика и обнаружения угроз. NSP востребована в крупных организациях, где требуется защита как от известных, так и от новых, неизвестных атак.

Кроме того, **Intrusion Detection Systems от Symantec (Broadcom)** представляют собой комплексные решения для обнаружения и предотвращения вторжений в корпоративных и облачных сетях. Эти системы обеспечивают анализ и блокировку атак на различных уровнях, применяя как сигнатурный анализ, так и технологии машинного обучения. Такой подход позволяет эффективно защищать информационные ресурсы от широкого спектра угроз и атак [7].

Основными преимуществами коммерческих решений являются высокое качество поддержки, гарантии работы и предоставление множества функциональных возможностей, включая интеграцию с другими средствами безопасности. Однако они обладают рядом ограничений, таких как высокая стоимость, сложности с кастомизацией под специфические задачи и закрытый исходный код, что ограничивает возможности для индивидуальной настройки под уникальные требования.

В дополнение к коммерческим решениям, на рынке также доступны открытые IDS-системы, которые приобретают всё большую популярность благодаря своей доступности и гибкости для адаптации под различные потребности. Одной из самых известных и распространённых систем является **Snort**. Этот инструмент поддерживает как сигнатурный, так и аномальный методы обнаружения, предоставляя пользователям возможность модифицировать систему под конкретные задачи. Snort является бесплатным и имеет открытый исходный код, что облегчает интеграцию с различными средствами мониторинга и управления безопасностью.

Другой значимой системой является **Suricata** — высокопроизводительная IDS/IPS-система с открытым исходным кодом. Suricata поддерживает многозадачность и способна

обрабатывать значительные объёмы трафика в реальном времени. Благодаря сочетанию сигнатурного и аномального анализа, а также поддержке различных сетевых протоколов, Suricata является гибким инструментом для множества сценариев применения.

Также заслуживает внимания система **Zeek**, ранее известная как Bro. Эта IDS ориентирована на глубокий сетевой анализ и использует уникальные подходы к мониторингу трафика. Zeek выявляет угрозы, анализируя сетевые паттерны и поведение сети, что позволяет эффективно обнаруживать аномалии. Дополнительным преимуществом является возможность интеграции Zeek с другими системами безопасности, что расширяет её функциональные возможности и повышает эффективность защиты [14].

Открытые решения позволяют использовать широкий спектр инструментов для настройки и оптимизации системы под специфические нужды организации. Преимущества таких решений включают низкую стоимость, возможность кастомизации и активное сообщество разработчиков. Однако у них также есть свои ограничения, такие как высокая сложность настройки и недостаток официальной технической поддержки.

Системы обнаружения вторжений (IDS) должны быть способны выявлять широкий спектр угроз, как внешних, так и внутренних. Эти угрозы могут варьироваться от традиционных атак, таких как взлом и DDoS-атаки, до более сложных и скрытых угроз, таких как инсайдерские атаки. Важно понять, как различные типы угроз могут быть обнаружены с помощью различных методов анализа, включая сигнатурный, аномальный и поведенческий подходы [6].

Система IDS должна эффективно работать с различными видами угроз, обеспечивая комплексную защиту сети и информационных ресурсов. Среди наиболее распространённых внешних угроз выделяются DDoS-атаки [12], которые представляют собой массовые атаки на сеть с использованием множества скомпрометированных устройств для создания большого объема трафика, направленного на целевой сервер или сервис. Цель таких атак заключается в перегрузке ресурсов системы, что приводит к отказу в обслуживании и недоступности сервиса для легитимных пользователей.

Также распространены попытки несанкционированного доступа [3], которые могут включать эксплуатацию уязвимостей в программном обеспечении, подбор паролей, внедрение вредоносного кода и другие методы, направленные на получение доступа к защищённым ресурсам. Эти действия могут привести к компрометации данных и нарушению целостности системы.

Особую опасность представляют атаки с использованием фишинга и социальной инженерии. Такие угрозы нацелены на обман пользователей с целью получения конфиденциальной информации, например, логинов, паролей или данных банковских карт. Злоумышленники создают поддельные сайты и сообщения, имитирующие доверенные источники, чтобы вызвать у жертвы чувство доверия и заставить её раскрыть важные данные.

Ещё одной серьёзной угрозой являются вредоносные программы [8], такие как вирусы, трояны и шпионское ПО. Эти программы могут использоваться для создания скрытых каналов доступа (бэкдоров), кражи данных и нарушения нормального функционирования системы. Они наносят значительный ущерб безопасности, внедряясь в инфраструктуру и выполняя деструктивные действия. Эффективное выявление и нейтрализация таких угроз являются важными задачами IDS для обеспечения устойчивости системы безопасности.

Внутренние угрозы также представляют собой значительный риск для безопасности информационных систем. Одним из самых опасных типов внутренних угроз являются инсайдерские угрозы [10], которые исходят от сотрудников организации, имеющих доступ к защищенным данным и системам. Эти сотрудники могут злоупотреблять своими привилегиями для выполнения вредоносных действий, таких как кража данных, саботаж или несанкционированный доступ к критической информации. Инсайдеры могут быть мотивированы личными или финансовыми интересами, что делает их угрозой, которую сложно предсказать и предотвратить с помощью стандартных методов безопасности.

Еще одной внутренней угрозой являются ошибки конфигурации и недостаточная настройка систем [5]. Эти уязвимости могут возникать из-за человеческого фактора, неправильного управления системами или несоответствия безопасности установленным стандартам. Если настройки системы сделаны неаккуратно или с ошибками, они могут стать дверью для злоумышленников, которые смогут использовать эти уязвимости для проникновения в сеть или нарушения работы системы.

Для обнаружения внутренних угроз существует несколько методов, каждый из которых имеет свои особенности и ограничения. Сигнатурный метод обнаружения эффективно защищает от известных угроз, однако он не способен обнаружить новые, неизвестные атаки, что является его основным ограничением. Аномальный метод, в свою очередь, может привести к высокому количеству ложных срабатываний, так как любой отклоняющийся от нормы трафик может восприниматься как атака. Поведенческий метод требует постоянного мониторинга и анализа больших объемов данных, что может быть трудно реализуемо в реальном времени, особенно в сложных и динамичных средах. [13] Поэтому при проектировании системы IDS важно учитывать все эти ограничения и выбирать наиболее подходящие методы для эффективной защиты от как внешних, так и внутренних угроз.

Таким образом, сочетание этих методов в одной системе IDS позволяет более эффективно обнаруживать как известные, так и новые угрозы, а также минимизировать количество ложных срабатываний.

Хотя системы обнаружения вторжений играют ключевую роль в защите информационных систем, они не лишены ряда ограничений, которые могут затруднить их внедрение и эффективность: Высокие затраты на внедрение и поддержку — коммерческие решения, как правило, требуют значительных финансовых вложений, а их обслуживание может быть связано с дополнительными затратами на обновление и настройку. Сложность настройки и использования — многие решения требуют глубокой настройки и профессиональных навыков для правильной интеграции с существующими системами безопасности. Это может стать барьером для организаций с ограниченными ресурсами. Высокая частота ложных срабатываний — системы, использующие аномальный анализ, могут давать много ложных срабатываний, что требует дополнительной настройки и мониторинга, чтобы избежать перезагрузки команды безопасности. Закрытые исходные коды — коммерческие IDS часто имеют закрытый исходный код, что ограничивает возможности их модификации и адаптации под специфические нужды компании.

Эти ограничения подчеркивают необходимость разработки отечественных IDS, ориентированных на локальные условия, которые обеспечивают высокую гибкость в настройке и эффективное реагирование на угрозы в специфических условиях.

В рамках данного исследования рассмотрены современные методы и алгоритмы для анализа угроз, включая методы машинного обучения, анализ сетевого трафика и поведенческий анализ.

В рамках данного исследования рассмотрены современные методы и алгоритмы, используемые для анализа угроз в системах безопасности. Одним из ключевых подходов является применение методов машинного обучения для классификации угроз. В частности, используются алгоритмы, такие как деревья решений, случайный лес, методы опорных векторов (SVM) [11], а также глубокие нейронные сети. Эти методы позволяют создавать модели, которые могут обучаться на исторических данных, улучшая точность предсказаний и адаптируясь к новым, ранее не встречавшимся угрозам.

Также важным методом является анализ сетевого трафика, который включает использование заранее определенных правил для выявления аномалий на основе базового профиля сети. Этот подход позволяет отслеживать отклонения от нормального поведения, что помогает своевременно обнаруживать потенциальные угрозы и предотвращать атаки.

Поведенческий анализ, в свою очередь, ориентирован на изучение паттернов действий пользователей и процессов. Он помогает выявлять отклонения, которые могут свидетельствовать о том, что в системе происходят атаки или другие злонамеренные действия. Такой подход позволяет своевременно обнаружить угрозы, которые не могут быть выявлены с помощью традиционных методов, основанных на сигнатурах.

Для обеспечения высокой точности классификации угроз в разработанной системе используется комбинация перечисленных методов. Это позволяет учитывать и статистические, и поведенческие особенности угроз, что повышает надежность системы.

Архитектура системы, разработанная на основе UML-моделей, включает несколько ключевых компонентов, каждый из которых выполняет свою роль в обеспечении безопасности и анализа угроз. Данные для обучения модели берутся из файла logs.csv, который содержит набор метрик, собранных за определенный период времени, включая как нормальный трафик, так и потенциальные угрозы. Этот файл формируется на основе журналов сетевого трафика, которые могут быть выгружены из систем мониторинга, таких как IDS/IPS (Intrusion Detection/Prevention Systems) или файлы *.pcap, используемые для анализа сетевых пакетов. На этапе сбора данных система захватывает и агрегирует информацию из различных источников, таких как сетевой трафик, системные логи и события безопасности. Для реализации этого процесса были использованы специализированные библиотеки и фреймворки: **Flask**, **Pandas**, **Scikit-learn**, **Joblib**, **Matplotlib**, **SQLite** и инструменты, включая **libpcap** и **tcpdump** для мониторинга сетевого трафика, а также **Logstash** для обработки логов. Гибкость настройки позволяет системе работать как в режиме реального времени, отслеживая текущую активность, так и в пакетном режиме для обработки архивных данных.

На следующем этапе происходит обработка собранных данных. Этот процесс включает фильтрацию для удаления дублирующейся и нерелевантной информации, а также нормализацию, которая приводит данные к единому формату. Подготовленные данные проходят этап агрегации и выделения ключевых признаков, необходимых для дальнейшего анализа. Такой подход гарантирует высокое качество данных и повышает точность идентификации угроз на следующих этапах обработки.

На уровне анализа система применяет современные алгоритмы машинного обучения и методы детектирования аномалий. Были реализованы как классические алгоритмы классификации, такие как случайный лес, метод опорных векторов и k-ближайших соседей, так и нейронные сети для более сложных сценариев. Эти алгоритмы позволяют системе распознавать известные типы угроз и выявлять аномальное поведение, что помогает идентифицировать новые или модифицированные атаки. Благодаря возможности автоматического обучения на новых данных, система адаптируется к изменениям сетевого трафика и эволюции киберугроз.

Для удобного взаимодействия с системой был разработан интуитивно понятный веб-интерфейс. Он предоставляет пользователю визуализацию результатов анализа в форме интерактивных графиков, таблиц и дашбордов. Через интерфейс можно управлять параметрами системы, настраивать уровни критичности угроз и создавать отчеты на основе результатов анализа. Веб-приложение разработано с использованием современных технологий, таких как React и Bootstrap, что обеспечивает стабильность и адаптивность интерфейса для работы на различных устройствах.

Тестирование системы проводилось на реальных сценариях эксплуатации, включающих моделирование различных типов атак. В ходе испытаний были воспроизведены DDoS-атаки, попытки фишинга и эксплуатации уязвимостей. Результаты тестов подтвердили высокую точность классификации угроз и стабильность системы при обработке больших объемов данных. Система успешно распознает как известные угрозы, так и новые виды атак благодаря механизмам анализа аномалий. Гибкая и масштабируемая архитектура позволяет легко интегрировать разработку с существующими информационно-аналитическими платформами и расширять её функционал по мере необходимости.

В ближайшие годы можно ожидать развитие новых технологий в области ИТ-безопасности, таких как использование квантовых вычислений для усиленной защиты данных или внедрение систем защиты, основанных на блокчейн-технологиях. Это создаст новые возможности для улучшения существующих систем IDS и разработки более мощных и надежных инструментов защиты.

Внедрение системы автоматической идентификации и классификации угроз позволяет значительно снизить риски кибератак, что ведет к сокращению финансовых потерь и трудозатрат, связанных с устранением последствий инцидентов ИБ. Дополнительным преимуществом является снижение зависимости от внешних поставщиков и повышение информационной независимости компании. Экономические расчеты показали, что использование IDS помогает существенно сократить затраты на предотвращение угроз и повысить общую безопасность организации.

Созданная система представляет собой надежное и доступное решение для отечественных компаний, позволяя повысить уровень защиты информационно-аналитических систем, сократить время реакции на инциденты и минимизировать ущерб от кибератак.

После внедрения системы автоматической идентификации и классификации угроз значительное внимание стоит уделить ее поддержке и развитию, поскольку динамично изменяющиеся угрозы требуют постоянной адаптации системы к новым реалиям. Важнейшей частью является регулярное обновление базы данных угроз, совершенствование алгоритмов

машинного обучения и улучшение механизмов обнаружения аномалий. Это позволит системе оставаться эффективной и актуальной на протяжении длительного времени.

Кроме того, стоит отметить, что система IDS, как и любая другая компонент информационной безопасности, должна интегрироваться в общую экосистему защиты, что требует тесного взаимодействия с другими системами безопасности, такими как системы управления инцидентами (SIEM) [9], антивирусные решения и системы управления доступом. Эффективная интеграция IDS с этими системами позволит не только оперативно реагировать на инциденты, но и проводить глубокий анализ причин и последствий атак.

Важным аспектом является обучение персонала, работающего с системой. Даже самая продвинутая система IDS не будет эффективной без квалифицированного реагирования на предупреждения и инциденты. Специалисты, использующие систему, должны быть обучены правильной интерпретации результатов анализа и принятия своевременных мер для минимизации ущерба. Это также способствует повышению общей осведомленности сотрудников о текущих угрозах и улучшению процессов реагирования на инциденты.

Еще одной важной стороной внедрения системы является обеспечение ее масштабируемости. В современных организациях, работающих с большими объемами данных, необходимо гарантировать, что система будет справляться с увеличивающимся потоком информации, не теряя в эффективности. Масштабируемость должна учитывать не только количество данных, но и сложность анализа, которая будет возрастать по мере увеличения числа угроз и новых типов атак.

Для повышения устойчивости системы к современным угрозам и увеличения ее гибкости в будущем предполагается дальнейшая разработка и внедрение более сложных моделей на основе нейронных сетей, что позволит адаптироваться к новым типам атак без необходимости полной переработки алгоритмов. В частности, методики глубокого обучения (deep learning) [4] могут значительно улучшить точность обнаружения и классификации угроз, особенно в тех случаях, когда необходимо работать с большими объемами данных и сложно выявляемыми аномалиями.

Системы автоматической идентификации и классификации угроз могут также интегрироваться с различными облачными сервисами и платформами. В условиях быстро развивающихся технологий облачные решения становятся все более востребованными, и возможность интеграции IDS с облачной инфраструктурой будет играть важную роль в обеспечении безопасности гибридных и облачных ИАС. Это также обеспечит высокую доступность системы и минимизацию рисков, связанных с потерей данных или отказом оборудования.

Наконец, нельзя забывать о важности создания гибкой политики безопасности, которая будет учитывать особенности работы каждой отдельной организации. Успешная реализация системы IDS зависит от того, насколько она будет интегрирована в существующую инфраструктуру и насколько пользователи смогут адаптировать ее под свои специфические потребности. Это требует наличия функций кастомизации, включая настройку пороговых значений для тревог и настройку алгоритмов на основе специфики работы предприятия.

Заключение

В данной статье был проведен всесторонний анализ проблем безопасности информационно-аналитических систем и рассмотрены основные подходы к разработке системы автоматической идентификации и классификации угроз безопасности. Было показано, что угрозы информационной безопасности могут быть разнообразными, включая как внешние, так и внутренние атаки, а также ошибки конфигурации и человеческий фактор. Важно отметить, что традиционные методы обнаружения угроз, такие как сигнатурный анализ, не всегда способны эффективно противостоять новым, неизвестным угрозам, что подчеркивает необходимость в комплексных решениях, использующих аномальные и поведенческие методы.

Одной из ключевых задач в разработке системы IDS является способность эффективно классифицировать и анализировать угрозы, обнаруженные в информационной системе, чтобы предотвратить или минимизировать их последствия. В статье подробно рассмотрены различные методы анализа сетевого трафика, основанные на машинном обучении, а также применение нейросетевых технологий для прогнозирования угроз и выявления аномального поведения в реальном времени.

Для эффективной защиты информационных систем от внешних и внутренних угроз требуется не только использование специализированных программных решений, таких как IDS, но и внедрение организационных и правовых мер. Правильная настройка и постоянное совершенствование системы безопасности могут значительно повысить уровень защиты данных и предотвратить возможные инциденты.

Разработка системы автоматической идентификации и классификации угроз, как показано в статье, может значительно улучшить мониторинг и защиту информационно-аналитических систем, обеспечивая защиту как от традиционных, так и от более сложных атак. Внедрение таких решений требует глубокого анализа существующих угроз, использования современных технологий анализа данных и постоянного обновления системы для защиты от новых типов угроз.

Список литературы

1. Николаева М.О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации // Журнал: Мониторинг. Образование. Безопасность. – 2023. – С. 51-57.
2. Чапис М.А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере // Журнал: НАУКОСФЕРА – 2024. – С. 551-557
3. Добродеев А.Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности. // Журнал: Труды ЦНИИС. Санкт-петербургский филиал – 2020. – С. 50-78
4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. - 2nd Edition. - No Starch Press, 2013.
5. Kshetri, N. Cybersecurity and International Relations: An Introduction. – 2020. – Т. 8. – No. 3. – pp. 11-18.
6. Northcutt, S., & Novak, J. Network Intrusion Detection. – 3rd Edition. – New Riders, 2003.

7. Debar, H., Dacier, M., & Scuteri, M. A survey of intrusion detection systems. – Computer Networks. – 1999. – Т. 31. – No. 8. – pp. 1007-1021.
8. Sommer, R., & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. – 2010. – ACM Transactions on Information and System Security. – Т. 13. – No. 3. – p. 6.
9. Ziegler, K., & Huitema, C. "Application of Machine Learning in Intrusion Detection Systems." – IEEE Communications Surveys & Tutorials. – 2022. – Т. 24. – No. 1. – pp. 58-72.
10. Chabaud, F., & Ren, L. Behavioral Anomaly Detection for Intrusion Prevention Systems. – Springer, 2021.
11. Bace, R. Network Intrusion Detection. – 2nd Edition. – Sams Publishing, 2000.
12. Zhang, Z., & Zeng, X. A Survey of Intrusion Detection Systems Using Data Mining Techniques. – Journal of Network and Computer Applications. – 2022. – Т. 133. – pp. 118-126.
13. Li, X., & Wang, W. A Review of Signature-Based Intrusion Detection Systems. – Journal of Computer Science and Technology. – 2021. – Т. 36. – p. 101-113.
14. Breiman, L. Random Forests. – Machine Learning. – 2001. – Т. 45. – p. 5-32.

References

1. Nikolaeva M.O. Information security: a modern picture of the problem of information security and information protection // Journal: Monitoring. Education. Safety. – 2023. – pp. 51-57.
2. Chapis M.A. Information security of the state as a legal procedure for ensuring national security in the information sphere // Journal: NAUKOSPHERE – 2024. – pp. 551-557
3. Dobrodeev A.Yu. Information security indicators as a characteristic (measure) of the compliance of communication networks and organizations with information security requirements. // Journal: Proceedings of the Central Research Institute. St. Petersburg branch – 2020. – pp. 50-78
4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. - 2nd Edition. - No Starch Press, 2013.
5. Kshetri, N. Cybersecurity and International Relations: An Introduction. – 2020. – Т. 8. – No. 3. – pp. 11-18.
6. Northcutt, S., & Novak, J. Network Intrusion Detection. – 3rd Edition. – New Riders, 2003.
7. Debar, H., Dacier, M., & Scuteri, M. A survey of intrusion detection systems. – Computer Networks. – 1999. – Т. 31. – No. 8. – pp. 1007-1021.
8. Sommer, R., & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. – 2010. – ACM Transactions on Information and System Security. – Т. 13. – No. 3. – p. 6.
9. Ziegler, K., & Huitema, C. "Application of Machine Learning in Intrusion Detection Systems." – IEEE Communications Surveys & Tutorials. – 2022. – Т. 24. – No. 1. – pp. 58-72.
10. Chabaud, F., & Ren, L. Behavioral Anomaly Detection for Intrusion Prevention Systems. – Springer, 2021.
11. Bace, R. Network Intrusion Detection. – 2nd Edition. – Sams Publishing, 2000.

12. Zhang, Z., & Zeng, X. A Survey of Intrusion Detection Systems Using Data Mining Techniques. – Journal of Network and Computer Applications. – 2022. – Т. 133. – pp. 118-126.
 13. Li, X., & Wang, W. A Review of Signature-Based Intrusion Detection Systems. – Journal of Computer Science and Technology. – 2021. – Т. 36. – pp. 101-113.
 14. Breiman, L. Random Forests. – Machine Learning. – 2001. – Т. 45. – pp. 5-32.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738

ПОСТРОЕНИЕ СЕТИ ДЛЯ ИЗОЛЯЦИИ АТАКУЕМЫХ СЕРВИСОВ: ИСПОЛЬЗОВАНИЕ DMZ

Бютнер С.И.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
serafimkavasaki@gmail.com

Использование демилитаризованной зоны (DMZ) в архитектуре сетей позволяет изолировать атакуемые сервисы, минимизируя риск доступа злоумышленников к внутренним сетям. DMZ служит буфером между публичными ресурсами и внутренними сетями организации, защищая чувствительные данные. Статья объясняет принципы работы DMZ, её ключевые компоненты, преимущества и недостатки, а также даёт рекомендации по настройке для повышения уровня безопасности.

Ключевые слова: DMZ, изоляция сетей, защита сервисов, архитектура сети, безопасность данных, фаерволы, настройки сети.

BUILDING A NETWORK TO ISOLATE VULNERABLE SERVICES: USING A DMZ

Buetner S.I.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

Using a demilitarized zone (DMZ) in network architecture allows for isolating vulnerable services, minimizing the risk of attackers accessing internal networks. A DMZ acts as a buffer between public resources and an organization's internal networks, safeguarding sensitive data. The article explains the principles of DMZ operation, its key components, advantages and drawbacks, and provides recommendations for configuration to enhance security.

Keywords: DMZ, network isolation, service protection, network architecture, data security, firewalls, network configuration.

Введение

С ростом числа киберугроз и атак на сетевые ресурсы организации всё чаще сталкиваются с необходимостью изолировать свои критически важные сервисы от внешних угроз. Одним из эффективных способов достижения этой цели является использование демилитаризованной зоны (DMZ). DMZ — это специализированная сеть, которая размещает публично доступные сервисы, такие как веб-серверы, почтовые серверы или DNS-серверы, в изолированном пространстве между внешним интернетом и внутренней корпоративной сетью.

Идея DMZ заключается в том, чтобы создать буфер, который защитит внутренние системы от прямых атак, даже если публичный сервер будет скомпрометирован. Такой подход особенно актуален для организаций, работающих с конфиденциальными данными,

финансовыми транзакциями или предоставляющих услуги через интернет. Однако, несмотря на очевидные преимущества, эффективное построение и настройка DMZ требуют понимания её архитектуры и грамотного подхода к безопасности.

Построение сети для изоляции атакуемых сервисов

Демилитаризованная зона (DMZ) представляет собой отдельную подсеть, которая служит буфером между внешним интернетом и внутренней сетью компании. Её основное предназначение — размещение публично доступных сервисов, таких как веб-сайты, почтовые серверы, FTP-серверы и DNS. Эти ресурсы чаще всего подвергаются атакам со стороны злоумышленников, и их размещение в изолированной зоне помогает минимизировать риск для остальных компонентов инфраструктуры. Основной принцип работы DMZ базируется на использовании двух фаерволов: внешний фаервол ограничивает доступ из интернета в DMZ, а внутренний защищает корпоративную сеть, предотвращая передачу трафика из DMZ внутрь без строгой проверки. Такое разделение позволяет защитить внутренние данные и ресурсы даже в случае успешной компрометации одного из сервисов в демилитаризованной зоне[1].

Размещение сервисов в DMZ даёт множество преимуществ. Во-первых, это изоляция наиболее атакуемых ресурсов. Например, если веб-сервер в DMZ скомпрометирован, злоумышленники не смогут напрямую атаковать внутреннюю сеть, поскольку её доступ ограничен внутренним фаерволом. Во-вторых, это упрощает мониторинг: трафик, проходящий через DMZ, легче отслеживать на наличие аномалий, что повышает эффективность систем обнаружения и предотвращения вторжений (IDS/IPS). Ещё одним плюсом является удобство управления: все публичные сервисы находятся в одной изолированной зоне, что упрощает их настройку и контроль[2].

Однако реализация DMZ требует грамотного подхода. Неправильная настройка может свести на нет её защитные функции. Например, слишком широкие правила фаерволов могут позволить злоумышленникам обойти защиту и проникнуть во внутреннюю сеть. Кроме того, администрирование DMZ требует высокого уровня компетенции: регулярное обновление серверов, установка патчей и использование современных протоколов шифрования, таких как HTTPS и SFTP, являются обязательными мерами. Для повышения безопасности рекомендуется использовать сегментацию внутри самой DMZ, когда каждый сервер размещается в отдельной подсети. Это предотвращает распространение угрозы на другие ресурсы в случае компрометации одного из них[3].

При создании DMZ важно учитывать специфику работы организации. Например, если компания активно использует удалённые подключения, то DMZ должна быть настроена с учётом этих требований. Использование VPN для доступа к серверам в DMZ поможет дополнительно защитить данные от перехвата. Для мониторинга активности в DMZ стоит применять системы логирования и анализа трафика, которые позволят оперативно реагировать на попытки атак. Ещё одной важной мерой является ограничение доступа: подключение к серверам в DMZ должно быть разрешено только с конкретных IP-адресов или через определённые порты[4].

Несмотря на все преимущества, DMZ имеет свои ограничения. Она не является универсальным решением и не может защитить сеть от всех типов атак. Например, социальная инженерия или фишинг могут позволить злоумышленникам получить доступ к внутренней сети, минуя DMZ. Поэтому её использование должно быть частью комплексной стратегии

безопасности, включающей регулярные аудиты, обучение сотрудников и резервное копирование данных[5].

Заключение

Использование демилитаризованной зоны (DMZ) является одним из ключевых методов обеспечения сетевой безопасности, позволяя изолировать уязвимые сервисы от внутренних систем. Благодаря правильной настройке и использованию современных технологий, таких как IDS/IPS, фаерволов и шифрования, DMZ помогает организациям защищать свои ресурсы от киберугроз.

Однако для достижения максимального уровня безопасности важно не только внедрять DMZ, но и регулярно обновлять её компоненты, а также проводить аудит сетевой инфраструктуры. Современные угрозы требуют комплексного подхода к безопасности, в котором DMZ становится лишь одним, но крайне важным элементом общей стратегии.

В условиях увеличивающегося числа атак на публично доступные ресурсы создание DMZ — это не только эффективное, но и необходимое решение для защиты критически важных данных и систем.

Список литературы

1. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
2. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Current problems of infotelecommunications in science and education. - 2021. – pp. 409-414.
3. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.

4. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
 5. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruевич, 1996.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

ВАЛИДАЦИЯ СТРУКТУРИРОВАННОГО КОНТЕНТА И ЕЁ РОЛЬ В ЗАЩИТЕ ВЕБ-ПРИЛОЖЕНИЙ

Буйтвидас А.В.

ФГАОУ ВО «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА», Москва, Россия, (127055, город Москва, ул. Образцова, д.9 стр.9), e-mail: buytik13@gmail.com

В статье определены наиболее распространённые типы структурированных данных, использующиеся в веб-приложениях. Описаны примеры уязвимостей, которые можно эксплуатировать, опираясь на некорректную структуру передаваемых данных. Сформулированы правила составления схем валидации наиболее популярных структур данных XML и JSON, которые позволят защитить приложение от атак, использующих подобные уязвимости.

Ключевые слова: JSON. XML, валидация данных, кибербезопасность, защита информации.

VALIDATION OF STRUCTURED CONTENT AND IT'S ROLE IN WEB APPLICATION PROTECTION

Buitvydas A.V.

RUSSIAN UNIVERSITY OF TRANSPORT, Moscow, Russia, (127055, Moscow, Obraztsova str., 9, bldg. 9), e-mail: buytik13@gmail.com

The article identifies the most common types of structured data used in web applications. Examples of vulnerabilities that can be exploited based on the incorrect structure of the transmitted. The rules compiling validation schemes for the most popular XML and JSON data structures are formulated, which will protect the application from attacks using such vulnerabilities.

Keywords: JSON, XML, data validation, cybersecurity, data protection.

Согласно статистике, собранной посредством сканирования общедоступных веб-приложений работающих на REST архитектуре, на октябрь 2024 года наибольшее распространение среди типов данных, используемых в приложениях, получили такие форматы, как binary, pdf, xml, json.

Таблица 1. - Статистика используемых медиа-типов в приложениях [1]

Разведанный mimetype	Август 2024, %	Сентябрь 2024, %	Октябрь 2024, %
application/pdf	0.6007	1.0165	0.7784
application/atom+xml	0.1005	0.1106	0.0989
application/xml	0.0238	0.0265	0.0542
application/rss+xml	0.0497	0.0577	0.0525
application/octet-stream	0.0443	0.0544	0.0496
application/json	0.0259	0.0306	0.0321

Так как pdf [2] и тем более бинарные файлы(application/octet-stream) не являются структурированным контентом, рассмотрим более подробно валидацию популярных типов данных JSON[3] и XML[4].

Хотя спецификации XML и схем XML(XSD)[5] уже предоставляют инструменты, необходимые для защиты приложений использующих XML, они также содержат множество недостатков безопасности. Их можно использовать для выполнения нескольких типов атак, включая извлечение файлов, подделку запросов к серверу, сканирование портов и прочее. В этой статье рассмотрим, как злоумышленники могут эксплуатировать уязвимости приложений, основанных на XML в библиотеках и программном обеспечении, которые можно разделить на два направления атаки:

1. Некорректно сформированные XML-документы, использование уязвимостей, когда приложения обрабатывают XML-документы, которые сформированы не по спецификации.
2. Невалидные XML документы, использование уязвимостей, связанных с отправкой документов соответствующих спецификации, но с неверной структурой данных.

Обработка содержимого, не соответствующего спецификации, может привести к чрезмерной утилизации процессора. Если документ XML имеет неверный формат, анализатор XML обнаружит фатальную ошибку, он должен прекратить выполнение, документ не должен подвергаться какой-либо дополнительной обработке, а приложение должно отобразить сообщение об ошибке.

Одна из таких популярных атак - это отправка документа с большой вложенностью без соответствующих закрывающих тэгов:

Пример:

```
<S1>
<S2>
<S3>
...
<S10000>
```

Таким образом, даже если проверяется размер передаваемого сообщения, такая атака позволит передать как минимум вдвое больше тегов чем предполагается. Обработка одного такого документа займёт много процессорного времени.

Такая атака при отсутствии правильно настроенной схемы валидации приведёт к отказу сервиса (DOS), без необходимости со стороны злоумышленника задействовать большие вычислительные ресурсы для атаки на приложение.

Если отсутствует строгий контроль состава структуры данных, то существует много вариантов атак, которыми может воспользоваться злоумышленник.

Рассмотрим на примере интернет магазина.

Пусть некоторый магазин продаёт электронные книги и валидная структура на покупку выглядит так:

```
<purchase>
  <id>1</id>
  <price>100</price>
  <quantity>1</quantity>
</purchase>
```

Где, id – это номер/артикул товара, price – цена товара, quantity – количество товара

Злоумышленник может отправить, например, отрицательное количество товара или дублирующиеся теги в результате чего получится книгу бесплатно в случае если приложение обрабатывает только первый встретившийся id:

```
<purchase>
  <id>1</id><price>0</price><quantity>1</quantity><id></id>
  <price>100</price>
  <quantity>1</quantity>
</purchase>
```

Для того чтобы предотвратить такие проблемы, опишем схему валидации данных чтобы исключить возможность обработки негативных значений и дублирования тегов:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="purchase">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="id" type="xs:positiveInteger"/>
        <xs:element name="price" type="xs:decimal"/>
        <xs:element name="quantity" type="xs:positiveInteger"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Чтобы корректно обрабатывать такие исключения XSD схема и обработчик должны в точности следовать спецификации, принимать только корректно сформированные XML, следовать чёткой валидации:

1. Запрет передачи не декларированных в схеме тегов(отсутствуют параметры xs:any, xs:anyType, xs:anySimpleType)
2. Должны быть ограничения по длине для всех строковых тегов
3. Для числовых значений должны быть указаны ограничения по минимальным и максимальным значениям.

4. Отсутствие циклических ссылок, т.е. если у тега “А” определено свойство ref со ссылкой на некоторый тег “Б”, то необходимо убедиться что у этого тега “Б” нет свойства ref со ссылкой на тег “А”, должно выполняться для любого уровня вложенности.

Эксплуатация уязвимостей приложений, использующих структуры JSON во многом схожи с XML и делятся на некорректно сформированные JSON документы и невалидные JSON документы, поэтому далее описываются только правила защиты от подобных уязвимостей.

Изначально в спецификации JSON отсутствовало такое понятие как JSON Schema[6], однако в связи с необходимостью валидации данных по аналогии с XML был разработан этот стандарт. Для JSON схем требования к схемам частично схожи с XML, однако есть и отличия:

1. Должны быть ограничения по длине для всех строковых тегов
2. Для строковых тегов, по возможности, должны быть определены patternProperties
3. Для числовых значений должны быть указаны ограничения по минимальным и максимальным значениям.

4. Отсутствие циклических ссылок, т.е. если у тега “А” определено свойство ref со ссылкой на некоторый тег “Б”, то необходимо убедиться что у этого тега “Б” нет свойства ref со ссылкой на тег “А”, должно выполняться для любого уровня вложенности.

5. У всех тегов с типом object должно быть определено свойство запрета не описанных в схеме полей additionalProperties: false

6. У тегов с типом массив, должно быть должно быть определено свойство maxItems – максимальное число элементов массива.

Заключение

В статье определены наиболее распространённые типы структурированных данных, использующиеся в веб-приложениях. Описаны примеры уязвимостей, которые можно эксплуатировать, опираясь на некорректную структуру передаваемых данных. Сформулированы правила составления схем валидации наиболее популярных структур данных XML и JSON, которые позволят защитить приложение от атак, использующих подобные уязвимости. Валидация данных позволяет повысить надёжность и безопасность приложений.

Список литературы

1. Статистика ежемечного сканирования по медиатипам [Электронный ресурс] <https://commoncrawl.github.io/cc-crawl-statistics/plots/mimetypes> (дата обращения 24.11.2024)
2. RFC для PDF формата [Электронный ресурс] <https://datatracker.ietf.org/doc/html/rfc7995> (дата обращения 24.11.2024)
3. The application/json медиатип JavaScript Object Notation (JSON) [Электронный ресурс] <https://datatracker.ietf.org/doc/html/rfc4627.html> (дата обращения 24.11.2024)
4. Медиатип XML [Электронный ресурс] <https://www.rfc-editor.org/rfc/rfc7303> (дата обращения 24.11.2024)
5. [Электронный ресурс] Спецификация XSD <https://www.w3.org/TR/xmlschema11-1/> (дата обращения 24.11.2024)

6. Спецификация JSON Schema [Электронный ресурс] <https://json-schema.org/> (дата обращения 24.11.2024)

References

1. Statistics of Monthly Scanning by Media Types [Electronic resource] <https://commoncrawl.github.io/cc-crawl-statistics/plots/mimetypes> (accessed 24.11.2024)
 2. RFC for PDF format [Electronic resource] <https://datatracker.ietf.org/doc/html/rfc7995> (accessed 24.11.2024)
 3. The application/json media type JavaScript Object Notation (JSON) [Electronic resource] <https://datatracker.ietf.org/doc/html/rfc4627.html> (accessed 24.11.2024)
 4. Media type XML [Electronic resource] <https://www.rfc-editor.org/rfc/rfc7303> (accessed 24.11.2024)
 5. Specification of XSD <https://www.w3.org/TR/xmlschema11-1/> (accessed 24.11.2024)
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.67

ИНТЕГРАЦИЯ БОЛЬШИХ ДАННЫХ И ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ АНАЛИЗА ГОРОДСКИХ ЭКОСИСТЕМ

¹Полежаева М.В., ²Кенжина Д.С., ³Аксёнова К.В., ⁴Сафонова Т.В., ⁵Мокряк А.В.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: ¹kolezei21@gmail.com, ²diana.kenzhina@yandex.ru, ³kseniaaksenova@inbox.ru, ⁴tatyana.vsafonova@gmail.com
⁵ФГБОУ ВО "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", Санкт-Петербург, Россия (196105, г. Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

В статье рассматривается интеграция технологий больших данных и геоинформационных систем (ГИС) для анализа и мониторинга городских экосистем. Данное исследование подчеркивает важность использования пространственных и временных данных для устойчивого управления городами, решения проблем с загрязнением окружающей среды, оптимизации транспортной системы и улучшения качества жизни жителей. Анализируется, как объединение этих технологий способствует более точному и оперативному мониторингу, а также позволяет разрабатывать модели предсказательной аналитики для умных городов будущего. Особое внимание уделяется перспективам развития и вызовам, связанным с обработкой больших объемов данных и вопросами конфиденциальности.

Ключевые слова: Большие данные, геоинформационные системы, городские экосистемы, анализ данных, устойчивое развитие, умные города, мониторинг, предсказательная аналитика.

INTEGRATION OF BIG DATA AND GEOGRAPHIC INFORMATION SYSTEMS FOR THE ANALYSIS OF NATURAL ECOSYSTEMS

¹Polezhaeva M.V., ²Kenzhina D.S., ³Aksenova K.V., ⁴Safonova T.V., ⁵Mokryak A.V.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: ¹kolezei21@gmail.com, ²diana.kenzhina@yandex.ru, ³kseniaaksenova@inbox.ru, ⁴tatyana.vsafonova@gmail.com
⁵ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt, 149), e-mail: ¹mokryakanna@mail.ru

The article explores the integration of big data technologies and geographic information systems (GIS) for analyzing and monitoring urban ecosystems. This study highlights the importance of using spatial and temporal data for sustainable urban management, addressing environmental pollution issues, optimizing transportation systems, and improving residents' quality of life. The integration of these technologies is examined in terms of its contribution to more accurate and timely monitoring, as well as its potential for predictive analytics in the smart

Введение

Современные города сталкиваются с целым рядом вызовов, связанных с быстрыми темпами урбанизации, изменениями климата, ухудшением качества воздуха и ростом потребности в устойчивом развитии [1, 2]. В этом контексте интеграция технологий больших данных и геоинформационных систем (ГИС) открывает новые возможности для анализа, мониторинга и оптимизации городских экосистем. Большие данные, которые включают огромные объемы информации из различных источников (таких как датчики Интернета вещей (IoT), спутниковые изображения и социальные сети), позволяют более полно оценивать и предсказывать изменения в городской среде. ГИС, в свою очередь, предоставляют инструменты для визуализации и пространственного анализа, что помогает эффективно отслеживать и интерпретировать динамику различных процессов в городе.

Одной из главных задач, стоящих перед исследователями и городскими властями, является создание умных городов, которые способны адаптироваться к меняющимся условиям и обеспечивать высокий уровень жизни для своих жителей. Интеграция больших данных и ГИС позволяет анализировать городские процессы с высокой точностью, улучшать управление ресурсами, прогнозировать потребности города и принимать обоснованные решения на основе актуальных данных.

Однако, несмотря на очевидные преимущества, существуют и определенные трудности, связанные с использованием данных такого масштаба. В первую очередь, это проблемы конфиденциальности, стандартизации данных, а также необходимость обработки огромных объемов информации. Тем не менее, перспективы использования больших данных и ГИС в городских исследованиях выглядят многообещающе, и данная статья направлена на освещение возможностей и вызовов, связанных с применением этих технологий для анализа городских экосистем.

Роль больших данных в анализе городских экосистем

Большие данные играют ключевую роль в анализе и управлении городскими экосистемами, предоставляя новые возможности для комплексного понимания процессов, происходящих в городской среде [3-6]. Благодаря большим данным исследователи и городские власти могут получать детализированную информацию о состоянии города, выявлять закономерности и даже предсказывать развитие различных процессов. Важно отметить, что большие данные включают данные из различных источников, таких как датчики IoT, спутниковые снимки, социальные сети и мобильные приложения. Данные источники позволяют собирать и анализировать информацию в реальном времени, что значительно улучшает мониторинг и управление городскими процессами.

Источниками больших данных для городских исследований могут служить следующие инструменты (Рисунок 1.):

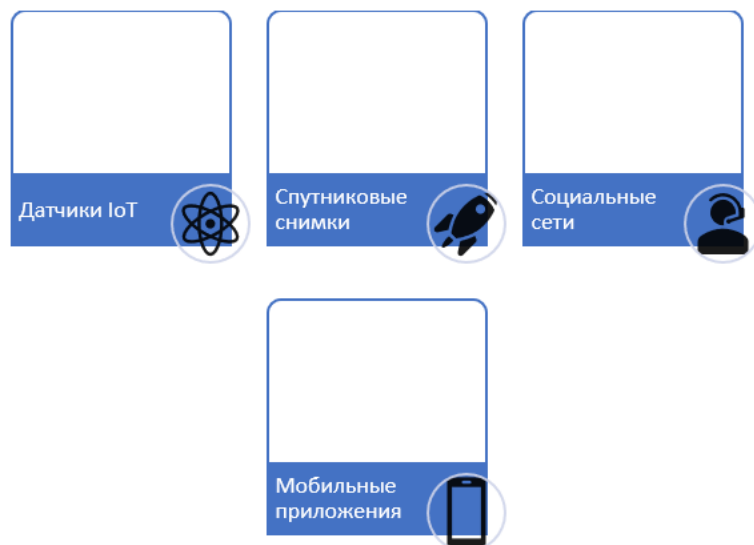


Рисунок 1 - Источниками больших данных для городских исследований

IoT широко используется в городской инфраструктуре, где установлены датчики на транспорте, уличных фонарях, зданиях и прочих объектах города. Эти сенсоры измеряют показатели качества воздуха, уровня шума, транспортного потока и передают информацию для последующего анализа в централизованные системы [3].

Спутниковые снимки и аэрофотосъемка предоставляют важную информацию о городских ландшафтах, изменениях инфраструктуры и состоянии окружающей среды. С их помощью отслеживаются зеленые зоны, строительство новых объектов, загрязнение водоемов и почв [4].

Данные социальных сетей тоже имеют значение для оценки восприятия городской среды горожанами. Геолокация и хештеги позволяют выявлять популярные места, события, а также инциденты, связанные с загрязнением или авариями [5, 6].

Мобильные приложения, среди которых навигационные сервисы, программы для заказа такси и погодные приложения, собирают сведения о перемещении людей, их предпочтениях и активности, что помогает анализировать транспортные потоки, загруженность общественного транспорта и совершенствовать городской сервис.

Типы данных для анализа городских экосистем

Различные типы данных, собираемые из этих источников, предоставляют всесторонний обзор на процессы в городской среде. Основные типы данных включают метеорологические, экологические, демографические сведения, включая данные о трафике.

Климатические данные включают информацию о температуре, влажности, скорости ветра и количестве осадков, что благополучно используется для анализа погодных условий и их воздействия на экологическое состояние города.

Сведения о трафике содержат данные о загруженности дорог, работе общественного транспорта и пробках, что дает возможность определять проблемные участки и улучшать организацию движения.

Экологические данные включают показатели загрязнённости воздуха, воды и почвы, а также уровни шумового загрязнения, что помогает контролировать состояние окружающей среды и предпринимать шаги для её улучшения.

Демографические данные содержат сведения о численности населения, возрастном составе и социальном статусе жителей, что способствует лучшему пониманию потребностей разных районов и планированию развития городской инфраструктуры.

Использование больших данных для получения детализированной информации

Применение больших данных способствует получению точных и актуальных сведений для принятия обоснованных решений. К примеру, благодаря информации, поступающей от датчиков IoT и мобильных приложений, города могут следить за текущей ситуацией на дорогах, уровнем загрязнения и другими показателями в реальном времени.

Большие данные позволяют разрабатывать модели предсказательной аналитики, прогнозирующие развитие тех или иных событий, например, ухудшение экологической обстановки при изменении погоды или увеличение транспортного потока в час пик, что помогает городам заранее планировать ресурсы и предотвращать негативные последствия.

Также данные о перемещениях и активности граждан позволяют глубже понять их потребности и адаптировать городское пространство к реальным запросам населения – будь то создание новых маршрутов общественного транспорта или улучшение качества воздуха в перенаселённых районах.

Функции и возможности ГИС

ГИС являются мощным инструментом для анализа, интерпретации и визуализации пространственных данных, что делает их незаменимыми в исследовании и управлении городскими экосистемами [7, 8]. ГИС позволяют объединять различные типы данных с географической привязкой, анализировать их и визуализировать в виде карт и графиков.

ГИС помогает преобразовывать сложные наборы пространственных данных в удобный и доступный для интерпретации формат, значительно упрощая анализ городских процессов. Также ГИС объединяет данные с точной географической привязкой, такие как демография, транспортная активность, уровень загрязнения воздуха и другие параметры, относящиеся к конкретным местам в городе. Таким образом, ГИС становится ценным инструментом для пространственного анализа, поскольку:

- позволяет отслеживать изменения в пространстве и времени;
- помогает обнаруживать закономерности и тенденции в городской среде;
- упрощает прогнозирование, например, увеличения плотности населения или ухудшения экологической ситуации в отдельных районах.

Примеры визуализации в ГИС для упрощения понимания сложных связей

Визуализация данных в ГИС делает сложные взаимосвязи и зависимости в городской экосистеме очевидными и простыми для понимания. Вот несколько примеров:

- тепловые карты дорожного трафика: ГИС может показывать загруженность дорог в разные периоды дня, что помогает выявить узкие места и моменты наибольшей нагрузки;
- карта загрязнения воздуха: данные о концентрации вредных веществ в воздухе можно нанести на карту города, чтобы наглядно увидеть районы с высоким уровнем загрязнения;

- зонирование зелёных насаждений: визуализация распределения зелёных зон и их плотности в городе помогает оценить доступность парков, скверов и других природных объектов для жителей, что играет ключевую роль в поддержании их здоровья и благополучия;
- интерактивные карты изменений в инфраструктуре: ГИС способна демонстрировать динамику изменений в городской инфраструктуре, показывая, как новые здания или дороги влияют на уже существующие районы и их население.

Интеграция больших данных и ГИС

Объединение технологий больших данных и ГИС позволяет значительно углубить и точнее анализировать процессы, происходящие в городской среде. В то время как большие данные предоставляют обширные объёмы информации из разных источников, таких как датчики IoT, спутники и социальные сети, ГИС предоставляет платформу для анализа и визуализации этих данных в пространственной плоскости. Совместное использование этих технологий помогает создать более полное представление о текущем состоянии города, что позволяет не только наблюдать за изменениями, но и предсказывать их. Например, на основе данных о трафике, погодных условиях и загрязнении воздуха можно разработать модели для прогнозирования пробок или ухудшения экологической ситуации в определённых районах [9].

Для интеграции больших данных и ГИС используют различные методы, среди которых важную роль играют API, облачные платформы и специализированные программы. API предоставляют разработчикам возможность легко передавать данные между системами, например, в ГИС можно передавать данные в реальном времени из внешних источников, таких как мобильные приложения или метеорологические датчики, что особенно полезно для оперативного обновления данных и создания динамических карт, отражающих текущую ситуацию. Облачные платформы поддерживают хранение и обработку больших объёмов данных, что важно для городов с интенсивными информационными потоками. Специализированные ГИС, такая как ArcGIS, предоставляет инструменты для сложной пространственной обработки данных и их визуализации. Они позволяют объединять данные из различных источников и применять аналитические модели, поддерживая широкий спектр функций, от создания карт до сложных пространственных расчетов.

Интеграция больших данных и ГИС также позволяет обновлять карты в реальном времени, предоставляя актуальную картину происходящего в городе, что достигается за счет использования данных от сенсоров, GPS-устройств и других источников, которые предоставляют информацию практически без задержек. Например, данные с транспортных датчиков и мобильных приложений о загруженности дорог можно обрабатывать и выводить на карту почти мгновенно, позволяя жителям и городским службам видеть актуальную ситуацию и корректировать свои действия. Точно так же данные о качестве воздуха, поступающие от датчиков, помогают городским экологам оперативно отслеживать экологическую обстановку и при необходимости принимать меры.

Примеры использования интеграции в анализе городских экосистем

Объединение больших данных и ГИС предоставляет значительные возможности для всестороннего анализа и улучшения городских экосистем в самых разнообразных сферах. Одним из ярких примеров этого является контроль качества воздуха. Информация, собранная множеством

датчиков, установленных по всей территории города, совместно с ГИС, позволяет точно отслеживать уровень загрязнений, включая содержание углекислого газа и диоксида азота. Пространственно-временной анализ этих данных помогает понять пути распространения загрязнений и выявить районы с повышенным риском, что имеет особое значение для оценки влияния на здоровье горожан, ведь длительное воздействие загрязненного воздуха связано с ростом числа респираторных и сердечно-сосудистых заболеваний. Используя эти данные, муниципальные органы могут принять меры по снижению вредного воздействия, например, ограничить движение автотранспорта в некоторых зонах или создать зелёные пространства, способствующие очистке воздуха.

Другим важным примером применения комбинации больших данных и ГИС является управление транспортными потоками. Данные о пробках, полученные из различных источников, таких как автомобильные GPS и мобильные приложения, поступают в ГИС, позволяя получить целостную картину загруженности дорог [10]. С использованием ГИС городские службы могут моделировать транспортные потоки и корректировать маршруты общественного транспорта, тем самым повышая эффективность транспортной системы и сокращая время простоев на дорогах.

Интеграция данных также играет значительную роль в изучении урбанизации и распределении зелёных зон. Данные спутниковой съёмки и аэрофото, вместе с ГИС, позволяют оценивать площади зелёных насаждений в каждом районе и их доступность для местных жителей. Известно, что зелёные зоны оказывают положительное влияние на микроклимат и здоровье горожан, понижают температуру и улучшают качество воздуха. С помощью ГИС можно не только отслеживать изменение площадей зелёных зон, но и планировать их оптимальное размещение, обеспечивая всем жителям доступ к паркам и скверам. Данные сведения помогают градостроителям принимать взвешенные решения для сохранения экологического равновесия и повышения качества жизни в условиях активного городского роста.

Ещё одно направление использования больших данных и ГИС — оптимизация энергопотребления и продвижение устойчивого развития. Данные об использовании электричества и других ресурсов, таких как вода или газ, интегрированы в ГИС для анализа на уровне районов или отдельных строений. ГИС также помогает отслеживать применение возобновляемых источников энергии, таких как солнечные панели, и планировать их установку там, где они окажутся наиболее эффективными. Всё это способствует переходу к более рациональному использованию энергии и снижению нагрузки на окружающую среду города.

Выводы

Совмещение больших данных и ГИС является мощным средством для устойчивого и интеллектуального развития современных мегаполисов. Эти технологии позволяют глубже проникнуть в суть городских процессов, оперативно отслеживать изменения и формировать действенные стратегии для решения вопросов, связанных с урбанизацией, экологическими проблемами, регулированием транспортных потоков и оптимальным использованием ресурсов. Комбинируя большие данные и ГИС, можно осуществлять мониторинг в реальном времени, применять методы предсказательного анализа и визуализировать сложные взаимодействия внутри городской среды, что, в конечном счете, помогает принимать продуманные и своевременные решения, нацеленные на улучшение качества жизни горожан [11, 12].

Перспективы дальнейшего развития этих технологий обещают ещё больший вклад в устойчивое управление городами. В условиях увеличивающейся численности населения и

возрастающих нагрузок на городскую инфраструктуру подобные инструменты могут стать фундаментом для создания «умных» городов, способных адаптироваться к изменяющимся условиям и нуждам общества. Будущее интеграции больших данных и ГИС связано с применением искусственного интеллекта, автоматизацией анализа и всё более точным прогнозированием процессов в городской среде. Расширение и внедрение этих технологий вселяют надежду на то, что города будущего станут более безопасными, экологически чистыми и комфортными для жизни, открывая новые перспективы для устойчивого городского развития и обеспечения высокого уровня жизни для всех жителей [12].

Список литературы

1. Гудчайлд М.Ф. Географическая информатика и системы для городского управления и планирования / Майкл Ф. Гудчайлд // Журнал городского планирования и развития. – 2018. – Т. 144, № 1. – С. 04017018.
2. Китчин Р. Город в реальном времени? Большие данные и интеллектуальный урбанизм / Роб Китчин // GeoJournal. – 2016. – Т. 81, № 1. – С. 147–160.
3. Сафонова Т.В. Анализ моделей данных в ГИС Информационные технологии и системы: управление, экономика, транспорт, право. 2022. № 3 (43). С. 4-11.
4. Бэтти М., Аксхаузен К.В., Джаннотти Ф. и др. Умные города будущего / Майкл Бэтти, Кей В. Аксхаузен, Фоска Джаннотти и др. // The European Physical Journal Special Topics. – 2021. – Т. 230, № 14. – С. 2685–2698.
5. Шахаби К., Уилсон Дж. П. Интеграция геопространственных данных для исследований в области городского здравоохранения и окружающей среды / Сайрус Шахаби, Джон П. Уилсон // Компьютеры, окружающая среда и городские системы. – 2019. – Том. 73. – С. 111–123.
6. Тикки Д.А., Сафонова Т.В., Матюхин Д.С. Технология применения растровых данных в ГИС Информационные технологии и системы: управление, экономика, транспорт, право. 2022. № 4 (44). С. 111-116.
7. Чжу С., Ли З. Применение больших данных и искусственного интеллекта в городской среде / Сяодун Чжу, Чжэнжун Ли // Журнал больших данных. – 2020. – Том. 7, № 1. – С. 103.
8. Майер-Шенбергер В., Кукье К. Большие данные: революция, которая изменяет тому, как мы живем, живем и думаем / Виктор Майер-Шенбергер, Кеннет Кукье; пер. с англ. Ю.И. Каптуревского. – Москва : Эксмо, 2014. – 240 с.
9. Трансформация глобальных городских данных, 2023-2029 гг. / ООН-Хабитат. – Найроби: Программа Организации Объединенных Наций по населенным пунктам, 2023. – 128 стр.
10. Франк А.У., Марк Д.М. Введение в геоинформационную науку и технологии / Эндрю У. Франк, Дэвид М. Марк; пер. с англ. А.Н. Сергеева. – Москва : Лаборатория знаний, 2021. – 368 с.
11. Краенер М., Филлипс Э. Пространственный анализ в ГИС: руководство по использованию ArcGIS / Мартин Краенер, Эрик Филлипс; пер. с англ. Л.П. Смирнова. – Санкт-Петербург: Питер, 2016. – 352 с.
12. Google Earth Engine. – URL: <https://earthengine.google.com> (дата обращения: 27.11.2024).

References

1. Goodchild M.F. Geographic informatics and systems for urban management and planning / Michael F. Goodchild // *Journal of Urban Planning and Development*. – 2018. – Vol. 144, No. 1. – p. 04017018.
2. Kitchin R. The city in real time? Big data and intelligent urbanism / Rob Kitchin // *GeoJournal*. – 2016. – Vol. 81, No. 1. – pp. 147-160.
3. Safonova T.V. Analysis of data models in GIS Information technologies and systems: management, economics, transport, law. 2022. No. 3 (43). pp. 4-11.
4. Betty M., Axhausen K.V., Giannotti F. and others . Smart cities of the future / Michael Batty, Kay V. Axhausen, Fosca Giannotti, et al. // *The European Physical Journal Special Topics*. – 2021. – Vol. 230, No. 14. – pp. 2685-2698.
5. Shahabi K., Wilson J. P. Integration of geospatial data for research in the field of urban health and the environment / Cyrus Shahabi, John P. Wilson // *Computers, environment and urban systems*. – 2019. – Tom. 73. – pp. 111-123.
6. Tikki D.A., Safonova T.V., Matyukhin D.S. Technology of application of raster data in GIS Information technologies and systems: management, economics, transport, law. 2022. No. 4 (44). pp. 111-116.
7. Zhu S., Li Z. Application of big data and artificial intelligence in an urban environment / Xiaodong Zhu, Zhengrong Li // *Journal of Big Data*. 2020. Vol. 7, No. 1. p. 103.
8. Mayer-Schoenberger V., Kukye K. Big Data: a revolution that changes the way we live, live and think / Victor Mayer-Schoenberger, Kenneth Kukye; translated from English by Yu.I. Kapturevsky. Moscow : Eksmo, 2014. p.240
9. Transformation of global urban data, 2023-2029 / UN-Habitat. – Nairobi: United Nations Human Settlements Programme, 2023. – p.128
10. Frank A.U., Mark D.M. Introduction to Geoinformation science and Technology / Andrew W. Frank, David M. Mark; translated from English by A.N. Sergeev. Moscow : Laboratory of Knowledge, 2021. p.368
11. Kraener M., Phillips E. Spatial analysis in GIS: a guide to using ArcGIS / Martin Kraener, Eric Phillips; translated from English by L.P. Smirnov. – St. Petersburg: Peter, 2016. – p.352
12. Google Earth Engine. – URL: <https://earthengine.google.com> (date of request: 11/27/2024).



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.81

КАК ИИ ПОМОЩНИКИ МЕНЯЮТ РАЗРАБОТКУ

Берников А.Д., Варфоломеева А.К., Шве́ц П.А., ¹Сафонова Т.В., ²Мокряк А.В.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: ¹tatyana.vsafonova@gmail.com

²ФГБОУ ВО "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", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

Статья посвящена исследованию влияния искусственного интеллекта на процессы разработки в различных сферах деятельности. Основная цель работы заключается в раскрытии понятия ИИ помощников и их возможностей, а также в анализе их использования в разработке продуктов как в прошлом, так и в современном контексте.

В статье также анализируется применение ИИ помощников в таких областях, как технологии, финансы и здравоохранение, подчеркивая их роль в автоматизации процессов, повышении эффективности и улучшении качества принимаемых решений.

Результаты исследования демонстрируют, что ИИ помощники становятся неотъемлемой частью разработки, открывая новые возможности и способствуя инновациям в различных отраслях.

Ключевые слова: ИИ помощники, разработка, искусственный интеллект, машинное обучение, Low-code, наука о земле.

HOW AI ASSISTANTS ARE CHANGING DEVELOPMENT

Bernikov A.D., Varfolomeeva A.K., Shvets P.A., ¹Safonova T.V., ²Mokryak A.V.

RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: ¹tatyana.vsafonova@gmail.com

²ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt, 149), e-mail: ²mokryakanna@mail.ru

The article is devoted to the study of the influence of artificial intelligence on development processes in various fields of activity. The main purpose of the work is to reveal the concept and assistants and their capabilities, as well as to analyze their use in product development both in the past and in the modern context.

The article also analyzes the use of assistants in areas such as technology, finance and healthcare, emphasizing their role in automating processes, increasing efficiency and improving the quality of decisions.

The results of the study demonstrate that AI assistants are becoming an integral part of development, opening up new opportunities and contributing to innovation in various industries.

Keywords: AI assistants, development, artificial intelligence, machine learning, Low-code, geoscience.

Введение

Мир сегодня быстро меняется. За последнее время появилось множество концепций, направленных на цифровизацию различных аспектов жизни. Одна из них — искусственный интеллект, который все чаще внедряется в различные сферы деятельности.

Искусственный интеллект — это способность компьютерных систем решать задачи, требующие человеческого ума. Он включает в себя обработку данных и обучение на основе накопленных знаний. Для этого используются методы машинного обучения, а также нейронные сети, способные к самостоятельному развитию [1].

Машинное обучение — это технология искусственного интеллекта, основанная на анализе больших объемов данных. Чем больше информации у него под рукой, тем точнее будут результаты [2].

Нейронные сети имитируют работу человеческого мозга, передавая сигналы между вычислительными элементами так же, как это делают нейроны в мозгу.

Сегодня о существовании искусственного интеллекта (ИИ) знают многие, хотя он начал использоваться еще со времен первых смартфонов. Например, голосовые помощники в мобильных устройствах работают благодаря технологиям ИИ, распознавая и понимая голосовые команды. Уведомления и рекомендации в смартфонах также формируются на основе анализа предпочтений пользователя.

Применение ИИ в low-code разработке

Low-code платформы для разработки достаточно популярны в мире, но не в России. Пока в мире рынок лоукод привлек \$26,9 млрд в 2023, то на hh.ru на 200 «low-code» вакансий приходится около 17,5 тысяч вакансий «разработчиков» [3]. Но рынок ИИ в России достаточно быстро и хорошо развивается и входит в топ-10 по миру [4]. Соединив эти две технологии, мы можем получить уникальный продукт, который расширит рынок IT и привлечет новых пользователей, а также изменит ситуацию на рынке low-code, особенно в России.

Для начала, что такое low-code? Low-code – это способ разработки IT-продуктов с минимальным написанием кода лишь у некоторых элементов. То есть платформа лоукод— это такая «золотая середина» между классическим программированием (когда весь код пишется с нуля) и no-code разработкой (когда код вообще не пишется) [5]. Это позволяет системе быть более гибкой, по сравнению с no-code, но не такой сложной и требующей сложных навыков, как классическое программирование. Используется low-code, в основном, при автоматизации бизнес-процессов, для разработки несложных сайтов, например, в Tilda, и для маленьких приложений и чат-ботов.

Чем ИИ может помочь low-code разработчикам? Во-первых, в пост-анализе уже написанного продукта. Человеческий фактор при написании кода еще никто не отменял, а так как low-code – это открытый исходный код, то важно, чтобы при обновлении системы все «встало» на свои места, иначе программа не запустится. Этим и занимается ИИ, проводя диагностику написанного решения и выявляя ошибки, которые уже человек потом исправляет. Во-вторых, искусственный интеллект на основе ключевых слов/идей может составить шаблон готового решения, который пользователю только останется заполнить. Благо low-code платформы это позволяют, так как основными инструментами разработки являются графические модели, например, стрелки и различные фигуры.

Где же можно уже увидеть «коллаборацию» искусственного интеллекта и low-code? Примеров много, один из них — ИИ-помощник в Tilda. Он помогает пользователю с текстовым наполнением разрабатываемого сайта [6] (Рисунок1).

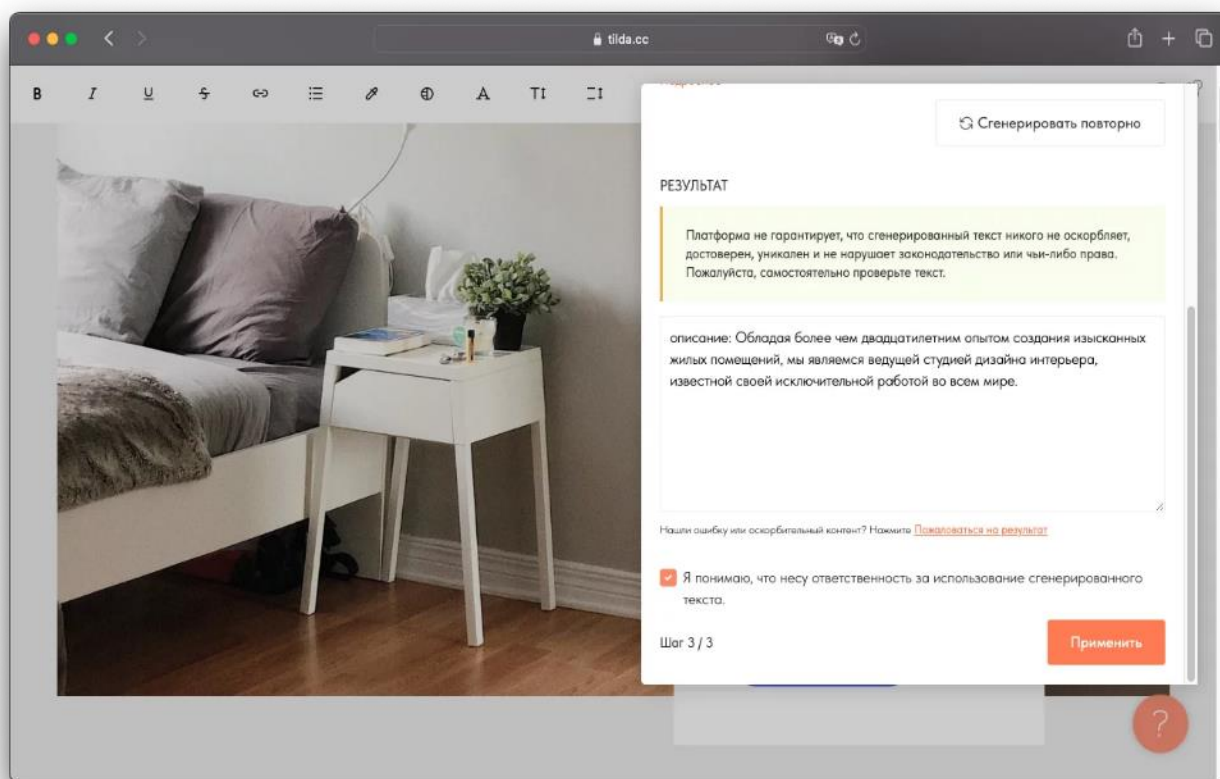


Рисунок 1 - ИИ-помощник в Tilda

Другой любопытный пример — это не столько внедрение ИИ в low-code платформу, сколько использование самой low-code платформы для работы с искусственным интеллектом. Поскольку процесс обучения ИИ часто требует выполнения однотипных задач, с помощью low-code платформ эти задачи можно запрограммировать всего один раз, после чего просто повторять их с новыми наборами данных [7] (Рисунок 2).

традиционная модель AI



Рисунок 2 – Low-code платформа для искусственного интеллекта

Применение ИИ и машинного обучения в сфере наук о Земле

В последнее время искусственный интеллект (ИИ) и машинное обучение (МО) стали весомыми инструментами в научных исследованиях, включая сферу наук о Земле. Эти технологии позволяют обрабатывать большие по объему данные, выявлять закономерности. Это все необходимо для понимания сложных процессов на нашей планете.

ИИ и МО в сфере наук о Земле открывает возможности для новых исследований в данном направлении:

1. Анализ больших массивов данных.

Одной из основных областей применения ИИ в науках о Земле является анализ больших данных. Например, алгоритмы машинного обучения могут быть использованы для обработки данных спутникового наблюдения, получая точные и временно актуальные данные о состоянии окружающей среды, не затрачивая для этого большое количество времени. Исследование, проведенное Б. М. Ирвином и др., демонстрирует, как машинное обучение позволяет эффективно извлекать информацию о змеиных миграциях и их корреляции с изменением климата, что может способствовать лучшему пониманию экосистем [8].

2. Моделирование климатических изменений.

ИИ и машинное обучение играют ключевую роль в моделировании климатических изменений. Алгоритмы могут использоваться для предсказания последствий различных сценариев изменения климата, включая повышение уровня моря и экстремальные погодные условия. Например, исследователи из [9] показали, что нейронные сети могут точно предсказывать сценарии изменения температуры и уровня осадков в различных регионах.

3. Мониторинг природных катастроф.

Машинное обучение также используется при мониторинге и предсказании природных катастроф, таких как землетрясения, наводнения и лесные пожары. Использование ИИ позволяет анализировать исторические данные и факторы риска, чтобы разработать более точные модели предсказания. Например, работа [10] продемонстрировала, как алгоритмы машинного обучения могут прогнозировать вероятность лесных пожаров, основанную на метеорологических данных и данных о растительности.

К основным достоинствам использования ИИ-помощников в разработке необходимо отнести (Рисунок 3.):



Рисунок 3 - Достоинства использования ИИ-помощников в разработке

Автоматизация рутинных задач. ИИ могут автоматизировать выполнение рутинных операций, таких как кодирование, тестирование и деплоймент.

Ускоренное прототипирование. С использованием ИИ разработчики могут быстрее создавать прототипы приложений и проверять их работоспособность, т.к. нейросети способны генерировать код на основе требований и спецификаций, что значительно сокращает время на разработку.

Оптимизация кода. ИИ помогает находить ошибки и оптимизировать существующий код, т.к. машинное обучение может предложить лучшие решения для улучшения производительности приложения, уменьшения потребления ресурсов и повышения безопасности.

Персонализация и кастомизация. Благодаря анализу пользовательских данных ИИ может предлагать персонализированные функции и интерфейсы, что улучшает взаимодействие с пользователем и повышает удовлетворенность продуктом.

Обучение и поддержка. ИИ-помощники становятся наставниками для начинающих разработчиков, предоставляя подсказки, примеры кода и помощь в решении проблем.

Безопасность и защита данных. ИИ активно применяется для обнаружения уязвимостей и предотвращения кибератак. Также может мониторить поведение системы в реальном времени и предупреждать о потенциальных угрозах.

Инновационные подходы к решению задач. ИИ открывает новые горизонты для творчества и инноваций. Разработчики могут использовать его для поиска нестандартных решений и создания уникальных продуктов, которые ранее казались невозможными.

Выводы

ИИ и машинное обучение открывают новые горизонты во всех сферах. Эти технологии в сочетании с традиционными методами исследования в науках о Земле создают множество возможностей для достижения более глубокого понимания процессов, происходящих в нашей планете, и разработки стратегий по ее защите.

ИИ-помощники существенно трансформируют процесс разработки, делая его более эффективным, безопасным и креативным. Они позволяют разработчикам тратить меньше времени на рутину и больше на создание качественных и инновационных продуктов.

Список литературы

1. Искусственный интеллект Российской Федерации - База знаний [Электронный ресурс]. - Режим доступа: https://ai.gov.ru/knowledgebase/vnedrenie-ii/2024_indeks_gotovnosti_prioritetnyh_otrasley_ekonomiki_rossiyskoy_federacii_k_vnedreniyu_iskusstvennogo_intellekta_ncrri/
2. Русскоязычный интернет-ресурс о компьютерных играх [Электронный ресурс]. - Режим доступа: <https://dtf.ru/deadlock/3051190-inzhener-valve-ispolzoval-chatgpt-chtoby-naity-novyi-algoritm-podbora-igrokov-dlya-deadlock-i-teper-on-v-igre>
3. Рынок безкодовой разработки [Электронный ресурс]. – Режим доступа: <https://решение-верное.рф/rynok-bezkodovoy-razrabotki-loukod-razrabotki-korporacii-vsyo-esche-verny-klassicheskomu>
4. ИИ в России. Есть ли шанс вырваться в лидеры? [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:ИИ_в_России:_есть_ли_шанс_вырваться_в_лидеры
5. No-code и low-code — что это и чем они отличаются? [Электронный ресурс]. – Режим доступа: <https://blog.tutortop.ru/no-code-i-low-code-chto-eto-i-chem-oni-otlichayutsya/>
6. Генерация текста с помощью искусственного интеллекта [Электронный ресурс]. – Режим доступа: <https://blog.tutortop.ru/no-code-i-low-code-chto-eto-i-chem-oni-otlichayutsya/>
7. Low-Code ускорит развитие искусственного интеллекта [Электронный ресурс]. – Режим доступа: <https://bercut.com/blog/technologies/low-code-uskorit-razvitie-iskusstvennogo-intellekta/>
8. Irwin, B. M., et al. (2020). "Machine Learning in Ecology and Conservation." *Ecology Letters*, 23(1), 3-14 [Электронный ресурс]. – Режим доступа: <https://doi.org/10.5751/ES-13696-280150>
9. Wi, S., & Steinschneider, S. (2022). Assessing the physical realism of deep learning hydrologic model projections under climate change. *Water Resources Research*, 58, e2022WR032123. [Электронный ресурс]. – Режим доступа: <https://doi.org/10.1029/2022WR032123>
10. Kondylatos, S., Prapas, I., Ronco, M., Papoutsis, I., Camps-Valls, G., Piles, M., et al. (2022). Wildfire danger prediction and understanding with Deep Learning. *Geophysical Research Letters*, 49, e2022GL099368.[Электронный ресурс]. – Режим доступа: <https://doi.org/10.1029/2022GL099368>

References

1. Artificial intelligence of the Russian Federation - Knowledge base [Electronic resource]. - Access mode: https://ai.gov.ru/knowledgebase/vnedrenie-ii/2024_indeks_gotovnosti_prioritetnyh_otrasley_ekonomiki_rossiyskoy_federacii_k_vnedreniyu_iskusstvennogo_intellekta_ncrri/
 2. Russian-language online resource about computer games [Electronic resource]. - Access mode: <https://dtf.ru/deadlock/3051190-inzhener-valve-ispolzoval-chatgpt-chtoby-naiti-novyi-algoritm-podbora-igrokov-dlya-deadlock-i-teper-on-v-igre>
 3. The market of codeless development [Electronic resource]. – Access mode: https://решение-верное.Russian_Federation/rynok-bezkodovoy-razrabotki-loukod-razrabotki-korporacii-vsyo-esche-verny-klassicheskomu
 4. AI in Russia. Is there a chance to break into the lead? [electronic resource]. – Access mode: https://www.tadviser.ru/index.php/Статья:II_b_Of_Russia:Are_there_any_chances_to_get_involved_with_the_leaders
 5. No-code and low-code — what is it and how do they differ? [electronic resource]. – Access mode: <https://blog.tutortop.ru/no-code-i-low-code-cto-eto-i-chem-oni-otlichayutsya/>
 6. Text generation using artificial intelligence [Electronic resource]. – Access mode: <https://blog.tutortop.ru/no-code-i-low-code-cto-eto-i-chem-oni-otlichayutsya/>
 7. Low-Code will accelerate the development of artificial intelligence [Electronic resource]. – Access mode: <https://bercut.com/blog/technologies/low-code-uskorit-razvitie-iskusstvennogo-intellekta/>
 8. Irwin, B. M., et al. (2020). "Machine Learning in Ecology and Conservation." Ecology Letters, 23(1), 3-14 [Electronic resource]. – Access mode: <https://doi.org/10.5751/ES-13696-280150>
 9. Wi, S., & Steinschneider, S. (2022). Assessing the physical realism of deep learning hydrologic model projections under climate change. Water Resources Research, 58, e2022WR032123. [electronic resource]. – Access mode: <https://doi.org/10.1029/2022WR032123>
 10. Kondylatos, S., Prapas, I., Ronco, M., Papoutsis, I., Camps-Valls, G., Piles, M., et al. (2022). Wildfire danger prediction and understanding with Deep Learning. Geophysical Research Letters, 49, e2022GL099368.[Electronic resource]. – Access mode: <https://doi.org/10.1029/2022GL099368>
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ЗЕМЕЛЬНЫМИ РЕСУРСАМИ И КАДАСТРАМИ

¹Полежаева М.В., ²Кенжина Д.С., ³Аксёнова К.В., ⁴Сафонова Т.В., ⁵Мокряк А.В.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская
ул., д. 79) e-mail: ¹kolezei21@gmail.com, ²diana.kenzhina@yandex.ru, ³kseniaaksenova@inbox.ru,
⁴tatyana.vsafonova@gmail.com

⁵ФГБОУ ВО "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", Санкт-Петербург, Россия (196105, г. Санкт-
Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

В статье рассматриваются возможности применения блокчейн-технологий в сфере управления земельными ресурсами и кадастрами. Описаны основные преимущества блокчейна, такие как прозрачность, безопасность, неизменность данных и повышение эффективности. Также обсуждаются практические примеры внедрения блокчейна в кадастровых системах различных стран и выделяются ключевые вызовы, связанные с интеграцией новых технологий в существующие системы. Делается вывод о том, что блокчейн может существенно улучшить процессы регистрации и управления земельной собственностью, сокращая бюрократические затраты и минимизируя риски ошибок и мошенничества.

Ключевые слова: Блокчейн, управление земельными ресурсами, кадастр, прозрачность, смарт-контракты, безопасность данных, автоматизация сделок, токенизация, цифровые активы.

APPLICATION OF HOUSING TECHNOLOGIES IN LAND MANAGEMENT AND CADASTRE

¹Polezhaeva M.V., ²Kenzhina D.S., ³Aksenova K.V., ⁴Safonova T.V., ⁵Mokryak A.V.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St.
Petersburg, Voronezhskaya str., 79), e-mail: ¹kolezei21@gmail.com, ²diana.kenzhina@yandex.ru,
³kseniaaksenova@inbox.ru, ⁴tatyana.vsafonova@gmail.com

⁵ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE
RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF
CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN
FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St.
Petersburg, Moskovsky prospekt, 149), e-mail: ¹mokryakanna@mail.ru

The article explores the potential of blockchain technology in the management of land resources and cadastral systems. It outlines the key benefits of blockchain, including transparency, security, data immutability, and improved efficiency. Practical examples of blockchain implementation in cadastral systems across various countries are discussed, along with the main challenges associated with integrating new technologies into existing systems. The article concludes that blockchain can significantly enhance the processes of land registration and management, reducing bureaucratic costs and minimizing risks of errors and fraud.

Введение

В эпоху быстрого развития цифровых технологий блокчейн стал признанной инновационной платформой для управления данными в разных сферах, включая государственное управление и земельный кадастр. Это распределенная база данных, отличающаяся децентрализованной структурой, позволяет надежно фиксировать и сохранять данные, делая их доступными всем участникам сети без участия посредников и снижая вероятность мошенничества [1, 2]. Первоначально созданный для защиты цифровых валют, таких как биткоин, блокчейн продемонстрировал свою способность создавать надежные и безопасные структуры данных, которые трудно подделать или изменить [1, 3]. Эти особенности делают его особенно полезным для земельных и кадастровых систем, где требуется надежная, доступная и защищенная информация о правах собственности [4, 5].

Традиционные кадастровые системы сталкиваются с множеством трудностей, среди которых трудности доступа к данным, высокая стоимость обновления информации, риски мошенничества и потери данных. Часто такие системы страдают недостатком прозрачности, что приводит к злоупотреблениям и юридическим спорам. Внедрение блокчейна может существенно улучшить эту ситуацию, создав надежную и прозрачную базу данных, содержащую историю изменения прав собственности на землю [3, 5]. Примеры Грузии и Швеции показывают, что использование блокчейна в кадастровых системах помогло снизить административные расходы и повысить доверие к системе регистрации прав собственности [6-10].

Одно из главных преимуществ блокчейна заключается в возможности автоматизации транзакций через смарт-контракты. Смарт-контракты, основанные на блокчейне, могут автоматизировать процесс передачи прав собственности, арендных соглашений и других сделок, упрощая процедуры и уменьшая операционные издержки [2, 6]. В сфере земельных ресурсов это ускоряет операции с недвижимостью и сокращает число посредников, повышая надежность и прозрачность каждого этапа передачи прав [4]. Подобные методы управления земельными ресурсами поддерживаются крупными международными организациями, такими как Всемирный банк, видящими в блокчейне средство для повышения прозрачности и эффективности в секторе недвижимости и землепользования [7].

Таким образом, важность изучения применения блокчейн-технологий в управлении земельными ресурсами и кадастрами объясняется их потенциалом увеличить надежность данных, минимизировать риски потери информации и создать более справедливую систему, основанную на принципе открытости и доступности информации для всех участников.

Преимущества блокчейн-технологий в управлении земельными ресурсами

Основные преимущества блокчейн-технологий в управлении земельными ресурсами основаны на таких ключевых качествах, как прозрачность, безопасность, неизменность данных, автоматизация сделок и возможности токенизации.

Прозрачность и доступность данных является одной из основных особенностей блокчейн-системы, что особенно важно для управления земельными ресурсами и кадастрами. В традиционных системах кадастра и регистрации собственности доступ к информации может быть ограничен, а процесс оформления прав собственности зачастую сопряжён с бюрократическими препятствиями. Блокчейн, благодаря своей децентрализованной

архитектуре, делает данные доступными для всех участников системы, что устраняет лишние административные барьеры и позволяет контролировать изменения на каждом этапе записи. Публичность блокчейна способствует более открытому процессу, повышая доверие к системе и защищая её от злоупотреблений и манипуляций [3, 4].

Безопасность данных, вторая ключевая характеристика блокчейна, обеспечивает защиту от подделок и мошенничества. В блокчейн-системе каждый новый блок данных защищён криптографией, что предотвращает несанкционированные изменения или удаления записей. Это особенно важно для земельных и кадастровых систем, где любые ошибки или манипуляции могут привести к серьёзным последствиям для владельцев собственности и других участников рынка. В то же время распределённая структура блокчейна означает, что данные хранятся на множестве независимых узлов сети, и даже в случае взлома одного из них общая целостность системы не будет нарушена. Этот уровень безопасности делает блокчейн надёжным выбором для управления данными о собственности, минимизируя возможность споров и сложностей, связанных с потерей или искажением информации [5, 6].

Неизменность данных, которая гарантирует, что информация в блокчейне не может быть изменена после внесения, также является важным фактором в кадастровых системах. С помощью блокчейна возможно создание долговременной истории владения земельными участками, что снижает риски споров и обеспечивает устойчивую базу данных для долгосрочных процессов управления. Такой подход к учёту прав собственности позволяет защитить владельцев от возможных изменений, введённых злоумышленниками или административными ошибками. Надёжность и неизменность записей служат залогом прозрачности и правовой защищённости собственности, что особенно актуально в случаях, где споры по поводу права собственности могут привести к длительным и сложным судебным разбирательствам [2, 4].

Автоматизация сделок через смарт-контракты является ещё одной значительной возможностью блокчейн-технологий в управлении земельными ресурсами. Смарт-контракты позволяют автоматизировать весь процесс передачи прав собственности, аренды и других сделок, выполняя заранее определённые условия без необходимости участия третьих лиц. Это не только сокращает временные затраты и упрощает процесс, но и уменьшает риск человеческой ошибки, делая процесс регистрации и передачи прав более эффективным и надёжным. Внедрение смарт-контрактов также сокращает потребность в нотариусах и других посредниках, что снижает издержки для участников рынка недвижимости и делает процесс более прозрачным и предсказуемым [2, 7].

Наконец, токенизация земельных участков, возможная с помощью блокчейна, открывает новые возможности для инвестирования. Токенизация позволяет представить земельные участки в виде цифровых активов или токенов, которые могут быть разделены на доли и проданы заинтересованным сторонам. данный процесс предоставляет доступ к земельным активам для более широкого круга инвесторов, что особенно полезно в странах с высокими барьерами входа на рынок недвижимости. Токенизация делает рынок земли более гибким, предоставляя возможность дробного владения, и стимулирует инвестиционную активность, что может способствовать экономическому росту в долгосрочной перспективе. Такие подходы к управлению земельными ресурсами позволяют обеспечить их доступность для более широкого круга участников, увеличивая ликвидность и прозрачность рынка [8, 9].

Таким образом, блокчейн-технологии открывают множество преимуществ для управления земельными ресурсами и кадастрами, создавая более прозрачную, безопасную и эффективную систему, которая способна изменить традиционные подходы к регистрации и защите прав собственности.

Практические примеры внедрения блокчейна в кадастровых системах разных стран

Практические примеры внедрения блокчейн-технологий в кадастровых системах демонстрируют, что потенциал блокчейна уже активно реализуется, улучшая процессы управления земельными ресурсами в различных странах. Одним из первых примеров успешного использования блокчейна в кадастровых системах стала Грузия. В 2016 году грузинское правительство в сотрудничестве с международной блокчейн-компанией внедрило систему для регистрации прав собственности на основе блокчейна. Этот шаг был направлен на повышение прозрачности и доверия к системе регистрации собственности, где ранее часто возникали споры из-за недостатка надёжных данных. С внедрением блокчейна регистрация сделок с недвижимостью стала проще и быстрее: процесс оформления прав собственности сократился по времени и теперь требует меньше бумажной работы, что позволяет экономить ресурсы и минимизировать риск ошибок [7, 8].

Швеция также стала одной из стран, активно интегрирующих блокчейн в свою систему регистрации собственности. Стремление к цифровизации сделок с недвижимостью привело к экспериментам с блокчейном в рамках государственной инициативы. В пилотном проекте, запущенном Шведским агентством по регистрации недвижимости, блокчейн используется для регистрации и верификации сделок с недвижимостью, что позволило значительно сократить время их проведения и исключить необходимость использования бумажных документов. Данная инициатива была нацелена на создание более оперативной и доступной системы, которая могла бы обеспечить прозрачность и надёжность данных о праве собственности. Пилотный проект уже доказал свою эффективность, и его планируют внедрять на более широком уровне, что может существенно модернизировать рынок недвижимости в стране [9, 10].

Другим значительным примером использования блокчейн-технологий является инициатива «Smart Dubai». В рамках этой амбициозной программы власти Дубая стремятся сделать город полностью цифровым к 2025 году, внедряя блокчейн в различные государственные процессы, включая кадастровый учёт. Использование блокчейна позволяет создавать безопасные цифровые записи сделок с недвижимостью, что повышает доверие к системе и снижает операционные издержки. Внедрение блокчейна в систему регистрации недвижимости Дубая направлено на создание полностью автоматизированной платформы, где процесс передачи прав собственности и другие операции выполняются без участия третьих лиц, что делает систему более прозрачной и устойчивой к манипуляциям. «Smart Dubai» продвигает блокчейн как основу для цифрового управления, стремясь привлечь как местные, так и международные инвестиции за счёт повышения эффективности работы государственных служб [6, 7].

Опыт этих стран подчёркивает как успехи, так и сложности внедрения блокчейна в системы регистрации собственности. Пример Грузии показал, что блокчейн может успешно сократить бюрократические затраты и повысить уровень доверия к кадастровой системе,

однако внедрение технологии требует тщательной юридической подготовки и координации с существующим законодательством, чтобы обеспечить её юридическую силу. В Швеции блокчейн продемонстрировал высокую эффективность в ускорении процесса оформления сделок, но проект требует значительных ресурсов и цифровой адаптации как со стороны властей, так и со стороны населения. Пример Дубая показывает, что блокчейн может стать частью долгосрочной стратегии цифровизации, однако требует значительных финансовых вложений и создания надёжной цифровой инфраструктуры. Внедрение блокчейн-технологий в государственные системы предполагает необходимость серьёзных изменений на всех уровнях — от технического до законодательного, что зачастую является сложным и длительным процессом [6-8].

Представленные примеры подтверждают, что блокчейн может значительно улучшить процесс управления земельными ресурсами, обеспечивая прозрачность, безопасность и доступность данных, однако успешная интеграция технологии требует не только технических, но и институциональных и правовых преобразований.

Вызовы и ограничения внедрения блокчейна в кадастровых системах

Основные вызовы и ограничения внедрения блокчейна в кадастровых системах охватывают как юридические, так и технические, социальные и этические аспекты, что требует комплексного подхода к их преодолению. Одним из наиболее значительных барьеров является юридическая и регуляторная неопределенность. Поскольку блокчейн представляет собой относительно новую технологию, в законодательной системе многих стран отсутствуют чёткие правила и нормы, регулирующие его использование в сфере земельного кадастра и управления собственностью. Чтобы блокчейн-системы могли получить юридическую силу, необходимо адаптировать существующее законодательство к новым требованиям и обеспечить, чтобы записи в блокчейне признавались юридически значимыми. Это включает не только признание правовой силы цифровых записей, но и разработку механизмов защиты прав собственности, предусмотренных в блокчейн-реестрах, что требует времени и значительных усилий со стороны законодателей [6,8].

Второй крупный вызов — технические сложности, связанные с интеграцией блокчейна в уже существующие кадастровые системы. Внедрение блокчейна требует значительных технических ресурсов и профессиональных знаний, так как необходимо не только создать новую инфраструктуру, но и обеспечить её совместимость с действующими базами данных. Традиционные кадастровые системы часто построены на устаревших технологиях, и миграция данных в блокчейн-систему может оказаться трудоёмким процессом. Кроме того, необходимо решить проблему масштабируемости блокчейна, так как количество операций и объём данных в земельно-кадастровых системах может оказаться значительным, что потребует высоких вычислительных мощностей и устойчивых технических решений. Эти технические сложности включают и необходимость защиты системы от кибератак, что усложняет задачу её внедрения и требует дополнительных вложений в безопасность [5,7].

Серьёзное ограничение для внедрения блокчейна в кадастровые системы представляет уровень цифровой грамотности среди населения и государственных служащих. Блокчейн требует базового понимания принципов работы распределённых систем и умения работать с цифровыми технологиями, что для многих граждан может стать преградой. Внедрение новой системы требует обучения и повышения квалификации сотрудников, работающих с

кадастровыми данными, а также разработки доступных инструкций для пользователей. Без должного уровня цифровой грамотности как со стороны государственных органов, так и со стороны населения, внедрение блокчейна может быть воспринято с недоверием и вызвать сложности на этапе эксплуатации системы. Этот аспект требует инвестиций в образовательные программы и подготовки кадров, что может увеличить общую стоимость внедрения блокчейн-технологий в государственное управление [9, 10].

Ещё одним важным вызовом при внедрении блокчейна в кадастровые системы является защита конфиденциальности данных. Несмотря на то, что блокчейн обеспечивает высокий уровень безопасности, децентрализованная система хранения данных создаёт трудности для соблюдения конфиденциальности. Земельные кадастры содержат личные данные владельцев, и при использовании блокчейна возникает вопрос о необходимости их защиты от несанкционированного доступа. Современные блокчейн-системы всё ещё ограничены в возможностях создания конфиденциальных записей, поэтому для обеспечения безопасности персональных данных требуются дополнительные меры, такие как внедрение приватных блокчейнов или технологий, обеспечивающих конфиденциальность, что увеличивает техническую сложность и стоимость системы [3, 7].

Представленные вызовы и ограничения подчёркивают, что, несмотря на огромный потенциал блокчейн-технологий, для их успешного внедрения в кадастровые системы требуется комплексное решение, что включает модернизацию законодательства, разработку технической инфраструктуры, повышение уровня цифровой грамотности и создание механизмов защиты конфиденциальных данных. Успешное преодоление этих барьеров станет важным шагом к созданию надёжной, прозрачной и доступной системы управления земельными ресурсами на основе блокчейна.

Перспективы использования блокчейн-технологий в управлении земельными ресурсами

Перспективы и будущее блокчейн-технологий в управлении земельными ресурсами представляют собой многообещающее направление, где технологии способны решить давно существующие проблемы и создать совершенно новую модель управления. Возможные пути решения существующих проблем, связанных с блокчейном, прежде всего заключаются в развитии правовой базы. Необходимость юридического признания блокчейн-записей как легитимных и юридически значимых требует серьёзной работы над законодательством. Введение изменений может включать юридическую квалификацию смарт-контрактов, признание их равнозначности традиционным договорам, а также разработку стандартов, регулирующих защиту данных и обеспечение безопасности при работе с персональной информацией в блокчейн-системах [5-7, 12]. Некоторые страны, такие как Швеция и Эстония, уже активно работают в этом направлении, экспериментируя с юридическими рамками и создавая условия для признания блокчейн-реестров [8, 9].

Роль частного сектора в развитии блокчейна также сложно переоценить. Компании, специализирующиеся на блокчейн-решениях, уже предлагают платформы для создания цифровых кадастровых систем, и их участие в формировании технологической инфраструктуры крайне важно. Частный сектор может способствовать распространению блокчейн-технологий, предлагая решения для автоматизации сделок, токенизации земельных активов и разработки индивидуальных цифровых продуктов для различных нужд, от аренды

до долевого владения. Государственные инициативы также играют ключевую роль в продвижении блокчейна, так как именно государственные органы способны обеспечить надёжную правовую поддержку, финансирование и стратегическое руководство внедрением технологии. Программы вроде "Smart Dubai" показывают, что инициатива государства способна вдохновить на масштабные изменения и создать условия для интеграции блокчейна в национальные системы управления собственностью [6, 7].

Потенциал блокчейна как основного элемента цифровизации земельного кадастра лежит в его способности преобразовать традиционные процессы и обеспечить более высокую степень доверия, безопасности и доступности данных. В будущем блокчейн может стать неотъемлемой частью цифровых государственных систем, где каждый участок земли будет зарегистрирован в цифровом формате, а все сделки — происходить через автоматизированные смарт-контракты. Это не только ускорит процесс регистрации прав собственности, но и повысит доверие к системе как со стороны граждан, так и со стороны международных инвесторов. Внедрение блокчейна позволяет рассчитывать на создание глобальных сетей обмена информацией о недвижимости, где данные будут надёжно защищены и доступны для всех заинтересованных сторон, что в перспективе может ускорить цифровизацию не только национальных, но и трансграничных кадастровых систем [4, 7, 12].

Таким образом, будущее блокчейн-технологий в управлении земельными ресурсами напрямую зависит от способности государств и частного сектора работать вместе над преодолением юридических и технических барьеров. Благодаря своим характеристикам блокчейн может обеспечить прозрачность, безопасность и надёжность земельного кадастра, что станет важным шагом к созданию глобальной цифровой инфраструктуры для управления земельными ресурсами.

Выводы

Внедрение блокчейн-технологий в управление земельными ресурсами и кадастрами представляет собой значительный шаг вперёд в модернизации государственных систем учёта собственности. Прозрачность, безопасность и неизменность данных, которые предоставляет блокчейн, способны устранить основные проблемы, присущие традиционным кадастровым системам. Примеры таких стран, как Грузия, Швеция и Дубай, демонстрируют реальные достижения в создании цифровых платформ, основанных на блокчейне, которые уже сегодня повышают доверие и упрощают процессы регистрации и передачи прав собственности.

Преимущества блокчейна включают не только устранение бюрократических барьеров и снижение риска мошенничества, но и возможность автоматизации сделок с использованием смарт-контрактов. Токенизация земельных участков открывает новые перспективы для инвестирования и делает рынок недвижимости более доступным и гибким. Тем не менее, успешная интеграция блокчейна требует преодоления значительных вызовов, включая необходимость в развитии правовой базы, технические сложности и важность повышения цифровой грамотности среди населения и государственных служащих. Защита конфиденциальности данных также остаётся важной задачей для того, чтобы блокчейн-системы могли надёжно хранить персональные сведения.

Перспективы использования блокчейна в этой сфере зависят от взаимодействия частного сектора и государственных инициатив, которые должны не только создать необходимую инфраструктуру, но и внести изменения в законодательство для поддержки цифровых записей

и смарт-контрактов. В конечном итоге блокчейн может стать основой новой системы управления земельными ресурсами, обеспечивающей справедливость, безопасность и доступность информации для всех заинтересованных сторон. Успешное внедрение блокчейна в земельный кадастр не только улучшит государственные процессы, но и станет важным шагом к созданию глобальной цифровой сети управления собственностью, что открывает большие перспективы для будущего рынка недвижимости и государственного управления.

Список литературы

1. Накамото С. Биткоин: одноранговая электронная денежная система / Сатоши Накамото // URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения: 20.11.2024).
2. Тапскотт Д., Тапскотт А. Революция блокчейна: как технология, стоящая за биткоином и другими криптовалютами, меняет мир. - Нью-Йорк: Penguin Random House, 2016. - 320 стр.
3. Гюркайнак Г., Йылмаз И., Йесилюрт М. Интеллектуальная собственность и блокчейн / Гёкчен Гюркайнак, Илкер Йылмаз, Мехмет Йесилюрт // Computer Law and Security Review. - 2018. - № 34 (4). - С. 847-862.
4. Лемье В.Л. Доверие к записям: технология блокчейн – это ответ? / Виктория Л. Лемье // Журнал управления записями. – 2016. – Т. 26, № 2. – С. 110–139.
5. Чжан П., Уайт Дж., Шмидт Д.К., Ленц Г. Применение технологии блокчейн для управления земельной собственностью / Питер Чжан, Джеймс Уайт, Дуглас К. Шмидт, Грегор Ленц // Цифровое правительство: исследования и практика. – 2018. – Т. 19, № 1. – С. 1–15.
6. Субботина В.В., Назаренко М.Д., Максимов В.В., Сафонова Т.В., Мокряк А.В. Блокчейн в бизнесе: возможности и ограничения // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 2 (40). С. 42-49.
7. Талапина Е.В. Правовые аспекты использования технологии блокчейн в государственном управлении // Вестник Университета имени О.Е. Кутафина. – 2020. – № 9(57). – С. 98–112. URL:<https://vgmu.hse.ru/data/2020/09/30/1369439908/%D0%A2%D0%B0%D0%BB%D0%B0%D0%BF%D0%B8%D0%BD%D0%B0.pdf> (дата обращения: 25.11.2024).
8. Всемирный банк. Блокчейн и новые цифровые технологии для повышения прозрачности сектора недвижимости и земельных ресурсов / Всемирный банк. – Вашингтон, округ Колумбия: Группа Всемирного банка, 2018. – 48 с.
9. Применение блокчейна в различных секторах экономики / Хабр // URL: <https://habr.com/ru/companies/lenovo/articles/462047/> (дата обращения: 05.11.2024).
10. Deloitte. Токенизация активов: от недвижимости до земельного кадастра / Deloitte // URL: <https://www2.deloitte.com> (дата обращения: 03.11.2024).
11. Шипилов А.А. Проблемы правового регулирования цифровых технологий в Российской Федерации / Андрей Александрович Шипилов // Научный вестник Института экономики и права. - 2018. - № 8. - С. 45-52. - URL: https://www.iep.ru/files/Nauchniy_vestnik.ru/8-2018/8-2018.pdf (дата обращения: 17.11.2024).
12. Сафонова Т.В., Русскин В.Д., Макаров П.М., Пашенцев А.А., Мокряк А.В. Смарт-контракты: технологический анализ, применение и перспективы // Наукосфера. 2023. № 9-2. С. 142-147.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic monetary system / Satoshi Nakamoto // URL: <https://bitcoin.org/bitcoin.pdf> (accessed: 11/20/2024).
2. Tapscott D., Tapscott A. The Blockchain Revolution: how the Technology behind Bitcoin and other cryptocurrencies is changing the world. - New York: Penguin Random House, 2016. - 320 pages .
3. Gurkainak G., Yilmaz I., Yesilyurt M. Intellectual Property and Blockchain / Gokcen Gyurkainak, Ilker Yilmaz, Mehmet Yesilyurt // Computer Law and Security Review. - 2018. - № 34 (4). - Pp. 847-862.
4. Lemieux V.L. Trust in records: is blockchain technology the answer? / Victoria L. Lemieux // Journal of Records Management. 2016. Vol. 26, No. 2. pp. 110-139.
5. Zhang P., White J., Schmidt D.K., Lenz G. Application of blockchain technology for land property management / Peter Zhang, James White, Douglas K. Schmidt, Gregor Lenz // Digital government: Research and practice. – 2018. – Vol. 19, No. 1. – pp. 1-15.
6. Subbotina V.V., Nazarenko M.D., Maksimov V.V., Safonova T.V., Mokryak A.V. Blockchain in business: opportunities and limitations International Journal of Information Technology and Energy Efficiency. 2024. Vol. 9. No. 2 (40). pp. 42-49.
7. Talapina E.V. Legal aspects of the use of blockchain technology in public administration // Bulletin of the O.E. Kutafin University. – 2020. – № 9(57). – Pp. 98-112. URL:<https://vgmu.hse.ru/data/2020/09/30/1369439908/%D0%A2%D0%B0%D0%BB%D0%B0%D0%BF%D0%B8%D0%BD%D0%B0.pdf> (date of request: 11/25/2024).
8. The World Bank. Blockchain and new digital technologies to increase the transparency of the real estate and land resources sector / World Bank. – Washington, DC: World Bank Group, 2018. – 48 p
9. The use of blockchain in various sectors of the economy / Habr // URL: <https://habr.com/ru/companies/lenovo/articles/462047/> / (date of access: 05.11.2024).
10. Deloitte. Tokenization of assets: from real estate to the land registry / Deloitte // URL: <https://www2.deloitte.com> (date of request: 03.11.2024).
11. Shipilov A.A. Problems of legal regulation of digital technologies in the Russian Federation / Andrey Aleksandrovich Shipilov // Scientific Bulletin of the Institute of Economics and Law. - 2018. - No. 8. - pp. 45-52. - URL: https://www.iep.ru/files/Nauchniy_vestnik.ru/8-2018/8-2018.pdf (date of request: 11/17/2024).
12. Safonova T.V., Russkin V.D., Makarov P.M., Pashentsev A.A., Mokryak A.V. Smart contracts: technological analysis, application and prospects The science sphere. 2023. No. 9-2. pp. 142-147.



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

АНАЛИТИКА ДАННЫХ: ВИДЫ И ЕЁ РОЛЬ В ЗДРАВООХРАНЕНИИ

Спиридонова О.И.

ФГАОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ", Санкт-Петербург, Россия (190000, город Санкт-Петербург, Большая Морская ул., д.67 лит. а), e-mail: spiridonov-ig@mail.ru

В статье рассматривается аналитика данных как процесс обработки и интерпретации больших объемов информации, направленный на извлечение значимой информации и поддержку принятия решений в здравоохранении. Описываются основные виды аналитики данных: описательная, диагностическая, предиктивная и предписывающая. Для каждого вида анализа приводятся используемые модели, такие как модель визуализации данных, статистического анализа, причинно-следственного анализа и т.д. Подчеркивается важность аналитики данных для выявления скрытых закономерностей и улучшения качества медицинских услуг, а также оптимизации работы системы здравоохранения.

Ключевые слова: Аналитика данных, здравоохранение, описательная аналитика, диагностическая аналитика, предиктивная аналитика, предписывающая аналитика, модели анализа.

DATA ANALYTICS: TYPES AND ITS ROLE IN HEALTHCARE

Spiridonova O.I.

ST. PETERSBURG STATE UNIVERSITY OF AEROSPACE INSTRUMENTATION, St. Petersburg, Russia (190000, St. Petersburg, Bolshaya Morskaya str., 67 lit. a), e-mail: spiridonov-ig@mail.ru

The article discusses data analytics as a process of processing and interpreting large amounts of information aimed at extracting meaningful information and supporting decision-making in healthcare. The main types of data analytics are described: descriptive, diagnostic, predictive and prescriptive. For each type of analysis, the models used are given, such as a data visualization model, statistical analysis, cause-and-effect analysis, etc. The importance of data analytics for identifying hidden patterns and improving the quality of medical services, as well as optimizing the work of the healthcare system, is emphasized.

Keywords: Data analytics, healthcare, descriptive analytics, diagnostic analytics, predictive analytics, prescriptive analytics, analysis models.

Введение

Аналитика данных — это процесс обработки и интерпретации данных для извлечения значимой информации, формирования выводов и поддержки принятия решений. Аналитика больших данных включает в себя четыре вида аналитики, а именно, описательную, диагностическую, предиктивную и предписывающую (Рисунок 1).

Чаще всего аналитика данных применяется в сферах, где обрабатываются большие объёмы информации, которые невозможно обработать вручную [1]. Одной из таких сфер является сфера здравоохранения.



Рисунок 1 – Виды аналитики данных

В здравоохранении аналитика данных подразумевает под собой просмотр огромных объемов медицинских данных, который позволяет находить скрытые закономерности и нераспознанные связи [2], помогающие улучшить качество медицинских услуг и повысить эффективность работы системы здравоохранения.

Описательная аналитика подразумевает под собой процесс анализа исторических данных для выявления ключевых метрик и показателей [3]. Одна из основных моделей описательной аналитики - модель агрегирования данных, позволяющая формировать отчеты о состоянии здоровья населения и результатах лечения. Кроме того, в описательной аналитике используется модель визуализации данных, благодаря которой медицинские учреждения могут отслеживать эпидемиологические тенденции, анализировать результаты лечения и оценивать эффективность вмешательств. А вот использование модели статистического анализа позволяет оценить факторы риска заболеваний и эффективности лечения.

Диагностическая аналитика выявляет причины прошедших событий или явлений, позволяя определить факторы, которые влияли на результат [3]. Использование моделей диагностической аналитики, а именно, модели причинно-следственного, регрессионного и кластерного анализ, дает возможность выявить факторы, влияющих на здоровье населения, спрогнозировать вероятность госпитализации пациента с определенным диагнозом, и сегментировать пациентов по группам риска.

Предиктивная аналитика использует статистические модели и алгоритмы машинного обучения для прогнозирования будущих событий на основе исторических данных. Данный вид аналитики помогает предсказать, что может произойти в будущем, и подготовиться к этому [3]. За счет использования машинного обучения представляется возможным разработка индивидуальных планов лечения на основе анализа генетических данных пациента и его медицинской истории, прогнозирование вероятности возникновения какого-либо класса

заболеваний (например, сердечно-сосудистых) на основе факторов риска. В то время как машинное обучение позволяет изучить зависимость возникновения заболевания от факторов риска, благодаря временным рядам становится осуществимым предсказание всплесков заболеваний в определенные сезоны, опираясь на анализ заболеваемости по месяцам. Еще один немаловажный метод предиктивной аналитики - нейронные сети, имитирующие работу человеческого мозга. Они применяются для диагностики заболеваний на основе изображений (например, рентгеновских снимков) и для прогнозирования исходов лечения [4].

Предписывающая аналитика предлагает оптимальные решения для достижения определенных целей на основе анализа данных. Для нахождения наилучшего варианта действий в предписывающей аналитике используются оптимизационные модели и системы поддержки принятия решений. Это не все модели, используемые в предписывающей аналитике, но они являются одними из основных. Благодаря оптимизационным моделям становится возможным распределение медицинского персонала между пациентами. В свою очередь системы поддержки принятия решений могут предоставлять врачам рекомендации по лечению на основе анализа истории болезни пациента, его текущего состояния и клинических протоколов, что в свою очередь позволит улучшить качество диагностики и лечения [5].

Заключение

Различные виды аналитики данных в сфере здравоохранения играют важную роль в повышении качества медицинского обслуживания, оптимизации процессов и улучшении результатов лечения пациентов. Использование современных аналитических инструментов позволяет преобразовывать большие объемы необработанных данных в значимые знания, что способствует более эффективному принятию решений.

Список литературы

1. Основы анализа данных. URL: <https://skillbox.ru/media/code/osnovy-analiza-dannykh-dlya-nachinayushchikh/>
2. Role of Big Data Analytics in Healthcare. URL: https://translated.turbopages.org/proxy_u/en-ru.
3. Виды аналитики данных. URL: <https://sky.pro/media/kakie-vidy-analitiki-dannyh-sushhestvuyut/>
4. Прогнозная аналитика в системе здравоохранения. URL: <https://evercare.ru/sites/default/files/Prognoznaya-analitika.pdf>
5. Опыт разработки клинических сценариев для оценки специалистов здравоохранения. URL: <https://cyberleninka.ru>

References

1. Fundamentals of data analysis. URL: <https://skillbox.ru/media/code/osnovy-analiza-dannykh-dlya-nachinayushchikh/>
2. Role of Big Data Analytics in Healthcare. URL: https://translated.turbopages.org/proxy_u/en-ru.
3. Types of data analytics. URL: <https://sky.pro/media/kakie-vidy-analitiki-dannyh-sushhestvuyut/>
4. Predictive analytics in the healthcare system. URL: <https://evercare.ru/sites/default/files/Prognoznaya-analitika.pdf>

5. Experience in developing clinical scenarios for assessing healthcare specialists. URL: <https://cyberleninka.ru>
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.81

ПРЕДСКАЗАНИЕ ОШИБОК В ПРОИЗВОДСТВЕННОМ ОБОРУДОВАНИИ ИСПОЛЬЗУЯ МАШИННОЕ ОБУЧЕНИЕ

Уманский Д.М.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

"МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ", Москва, Россия, (124498, город Москва, город Зеленоград, пл. Шокина, д. 1), e-mail: umanskiy.dan@gmail.com

Контроль производительности и предсказание ошибок у промышленного оборудования являются крайне важными процессами не только для качества производимого материала, но также и для количества затрачиваемых денег и времени, сохраненных на проведении технического обслуживания. Целью данной статьи является проследить эволюцию искусственного интеллекта и машинного обучения для прогнозирования ошибок в производстве. Тематику, покрытую в данной статье включают алгоритмы машинного обучения, используемые случаи, принципы, связанные с применением подобной технологии в различных отраслях в том числе программном и аппаратном обеспечении. В данном обзоре рассматриваются исследования с конца 1980-х годов по начало 2000 годов, а также недавние исследования с 2000 по 2023 год. Данная статья предлагает детальный обзор различных подходов к машинному обучению и искусственному интеллекту используемых в различных Производствах. LSTM считается одним из наиболее широко используемых процессов.

Ключевые слова. Автоматизация производства, алгоритм предсказания, предсказание ошибок машинное обучение, длинная краткосрочная память.

PREDICTING ERRORS IN PRODUCTION EQUIPMENT USING MACHINE LEARNING

Umansky D.M.

"NATIONAL RESEARCH UNIVERSITY "MOSCOW INSTITUTE OF ELECTRONIC TECHNOLOGY", Moscow, Russia, (124498, Moscow, Zelenograd, Shokina Square, 1), e-mail: umanskiy.dan@gmail.com

Performance monitoring and error prediction for industrial equipment are extremely important processes not only for the quality of the material produced, but also for the amount of money spent and time saved on maintenance. The purpose of this article is to trace the evolution of artificial intelligence and machine learning to predict manufacturing errors. The topics covered in this article include machine learning algorithms, the cases used, and the principles associated with the use of such technology in various industries, including software and hardware. This review examines research from the late 1980s to the early 2000s, as well as recent research from 2000 to 2023. This article provides a detailed overview of the various approaches to machine learning and artificial intelligence used in various Industries. LSTM is considered one of the most widely used processes.

Keywords: Production automation, prediction algorithm, error prediction machine learning, long short-term memory.

Введение

Качество программ, использующих Интернета Вещей, существенно повысилось в последние годы, и связанные проблемы стали иметь большее значение в создании программного обеспечения. Это включает обеспечение возможности оценки шанса возникновения ошибки и способности программного модуля к её обработке, и дальнейшее тестирование модуля на готовность. Тестирование помогает разработчикам понизить

стоимость, а предсказание ошибок дает информацию для поддержания технического обслуживания. В процессе написания программного обеспечения слабости программы являются сложно-оценимыми. Однако поиск отношений между поддающимися оценке программными свойствами и неполадками поможет обнаружение неисправностей. Типовые методы, такие как тестирование или симуляция не отражают полную действительность предъявляемым к предсказанию ошибок в промышленном оборудовании.

Высокая стоимость и время затрат являются крайне значимыми свойствами для предсказания ошибок. Симуляция также не является пригодным методом проверки, так как она не учитывает все возможные состояния, в которых может находиться программное обеспечение. Формальным методом может быть использован для решения этих проблем. Математическая логика является основой формального метода. Формальные методы разделены на две категории:

- формальная спецификация – описывает взаимодействие между подверженностью к сбоям и формальным подтверждением;
- формальное подтверждение – подтверждает способность кода к выполнению без совершения ошибок.

Большинство существующего материала по данной теме используют симуляцию и эксперимент для проверки предложенных систем. Модульное тестирование – иной метод подтверждения в интернет-приложениях.

В данной статье исследование предсказания неполадок в программном обеспечении имеет две задачи:

- уменьшение количества измерений;
- увеличение шанса предсказания ошибки.

Данные характеристики могут быть отображены на модели поведения. Глубокое обучение было выбрано для продолжающегося развития машинного обучения. Глубокое обучение использует многослойную обработку информации и извлечение признаков, для оценки сложных нелинейных функций с малым количеством ошибок.

В области глубокого обучения свёрточные нейронные сети и рекуррентные нейронные сети являются часто используемым практичным решением. При проверке временных рядов рекуррентные нейронные сети считаются более точными. Глубокая тренировка, с другой стороны, приведет к исчезновению градиента нейронной сети. На основе рекуррентной нейронной сети сеть длинной кратковременной памяти добавляет три структуры «Врат» и имеет улучшенное предсказание временных рядов с достаточно высокой точностью. На оценку производительности оборудования часто влияет огромное количество многомерных переменных. Для обработки большого числа многомерных переменных длинная кратковременная память является малоэффективным методом проведения оценки, который не дает высокой точности результата. В то время как свёрточные нейронные сети способны поддерживать многомерные данные, сроки сбора данных не обладают высоким показателем качества. Традиционный метод роя частиц, метод внимания и другие алгоритмы могут использоваться для обработки многомерных данных, что позволит уменьшить количество излишней информации.

Данные методы также не учитывают отношение между входными данными, вызывая избыточность или потерю информации. В данной статье рассматривается модель обработки

данных основанной на CNN-LSTM – свёрточной долгой краткосрочной памяти, примененной к предсказанию ошибок у промышленного оборудования, для поиска подходящего решения. Компонент свёрточных нейронных сетей особенно эффективен для обработки данных благодаря его способности к уменьшению количества данных для проведения проверки, без ущерба для связи с данными. Извлеченный вектор признаков подается в сеть долгосрочной кратковременной памяти, которая превосходно справляется с прогнозированием данных временных рядов. При использовании данной модели обеспечивается не только свойства входных данных и их отношений, а также сроки вывода данных. Также при подготовке данной статьи сравнивались: функциональное значение, значение интерполяции модели и значение интерполяции сети долгой кратковременной памяти. Приведенный ниже пример используется для демонстрации логики и эффективности метода. Также показано, что этот подход оказывает большее влияние на улучшение, чем прогнозирование сети долгой краткосрочной памяти.

1. Обзор методов

Нахождение ошибок и их отправка к соответствующему разработчику для исправления является крайне важным для приложений Интернета Вещей, которых становится больше с каждым днем. Три ключевых направления, в которых развиваются приложения Интернета Вещей:

1. определения и уточнение измерения для вычисления сложности программного обеспечения;
2. подтверждение точности и тщательности программного обеспечения;
3. определение и исследование моделей предсказания ошибок, основанных на уточненной сложности программного обеспечения.

Программные метрики служат важным инструментом для качественной оценки свойств программного обеспечения и предсказания возникновения ошибок. Исследования подтверждают, что существует тесная связь между программными метриками и подверженностью программного кода к ошибкам. Для создания предсказательных моделей применяются различные методы, включая статистические подходы и алгоритмы машинного обучения.

Особое внимание уделяется выбору наиболее эффективных метрик, которые позволяют точно определить склонность программы к ошибкам в различных условиях. Метрики качества программного обеспечения исследуются как в статических, так и в динамических платформах. В статическом анализе основное внимание уделяется структуре кода, например, количеству контроллеров или ветвлений. Динамические платформы, напротив, измеряют такие характеристики, как тестовый перфекционизм, связанный с информационными потоками и спектром дополнений.

Определение зависимости между количественными характеристиками программного кода и вероятностью возникновения ошибок имеет практическую ценность. Это позволяет эффективно распределять ресурсы, выявляя модули, требующие приоритетного тестирования и оптимизации. Современные подходы, включая техники машинного обучения, такие как метод опорных векторов, активно применяются для повышения точности алгоритмов предсказания.

Эти методы играют ключевую роль в обеспечении надежности и качества программного обеспечения, способствуя выявлению потенциальных ошибок на ранних стадиях разработки. Многослойное восприятие является широко-используемым надзорным алгоритмом машинного обучения. Алгоритм Оптимизации Роя Частиц является алгоритмом оптимизации, что использует эволюционный алгоритм. Множественные источники предлагают систему поиска ошибок для мощных устройств применяющих Интернет Вещей.

Через глубокое обучение рассматривался многоспектральный подход к объединению изображений. Предложенный метод повышает точность и скорость локации точек ошибки. Предлагаемое гибридное решение включает Экстремальный процесс обучения и Генетический алгоритм. С изъятием полезной информации из отчетов об ошибке вектор пространственной модели строится на основе данной информации и минимальном наборе свойств. Эти свойства обрабатываются ансамблевым классификатор, представляющий собой Экстремальный алгоритм обучения на основе Генетического алгоритма. Предложенный алгоритм превзошел метод k-ближайших соседей, наивный метод Байеса и метод опорных векторов. Другая проблема в средах приложений Интернета Вещей – это возникновение компьютерных дефектов, появляющихся в результате старения инструмента. Для предсказания старения программного обеспечения был предложен метод Лиу Менга [1]. Подход основан на Метод обратного распространения ошибки нейронной сети. Алгоритм пчелиной колонии используется для определения весов и порогов. Иными словами, Алгоритм пчелиной колонии используется для улучшения метода обратного распространения ошибки. Это демонстрируется на сравнении типовых методов обратного распространения ошибки и предложенной ими модели, сходящейся с большей точностью и скоростью.

В системной инженерии, информационных системах и разработке программного обеспечения жизненный цикл программного обеспечения (SDLC) — это процесс разработки или изменения систем, а также моделей и методов используемых для построения этих систем. Определение SDLC лежит в основе ряда методологий разработки программного обеспечения в программной инженерии [2].

2.1. Существующие системы

Основных пути, которые изучаются для приложений Интернета Вещей это:

1. выявление и определение показателей для определения сложности приложения;
2. подтверждение корректности и полноты показателей.

Некоторые показатели, описывающие качество программного обеспечения в статических и динамических платформах, были рассмотрены. Свойства структуры кода вычисляются в виде показателей в статических платформах, таких как число контроллеров и число веток используется для статических вычислений. Тестируемая исполнительность измеряется в динамических платформах, таких как измерение базовых элементов основанных на объеме вспомогательных и информационных источников. Многие исследования показывают связь измерениями продукта и склонности к возникновению ошибок, а также множество оцениваемых программных характеристик [3].

Основные недостатки существующих систем заключается в использовании существующих подходов, сосредоточенных на протоколах исследования, которые не могут предсказать резкие изменения данных.

Предложенная система обнаруживает возможные ошибки программного обеспечения заранее и предупреждает устройство. Подход заключается в использовании модели Глубокого Обучения Долгой краткосрочной памяти, чтобы заранее прогнозировать значения временного ряда, а затем использовать классификатор для оценки необходимости выдачи оповещения [4].

В этой предлагаемой схеме алгоритм LSTM используется для создания модели из набора данных оборудования. Значения обучаются с использованием модели машинного обучения, которая затем используется для отслеживания обнаружения неисправностей и генерации предупреждений.

Преимущества предложенной системы заключается в использовании методов машинного обучения для обнаружения ошибок в процессах автоматического производства, что ограничивает необходимость ручного вмешательства и проверок. Также предложенная система снижает на половину время, требуемое для обработки данных[5].

2.2. Системный модуль

Набор данных:

Набор машинных данных о связи одного из свойств с одним из показателей используется в наборе данных. Функция с памятью и метка с 0 и 1 используются в качестве набора данных в этом проекте.

Предобработка:

На данном этапе набор машинных данных взят в качестве входных значений и вычисляется разница в данных временных рядов и создается новый набор данных, который имеет значения разницы с предыдущими значениями. Этот набор данных используется для прогнозирования следующих значений на основе разницы в качестве признака и следующего значения в качестве метки.

Модель предсказания:

Модель долгой краткосрочной памяти инициализируется для тренировки временных рядов. С помощью функции аппроксимации в качестве входных данных задаются признаки и метки, а модель алгоритма обучается для прогнозирования будущих значений.

Регрессионная модель:

На данном этапе набор данных со значениями памяти используются в качестве признаков, а предупреждение или отсутствие оповещения используется в качестве метки. Модель обучается и используется для прогнозирования условий возникновения ошибки.

Предсказание:

Для предсказания набор на вход подается предсказательная функция из 100 значений памяти в качестве метки в длинную краткосрочную модель и модель линейной регрессии для нахождения следующего значения и шанс ошибки вычисляется.

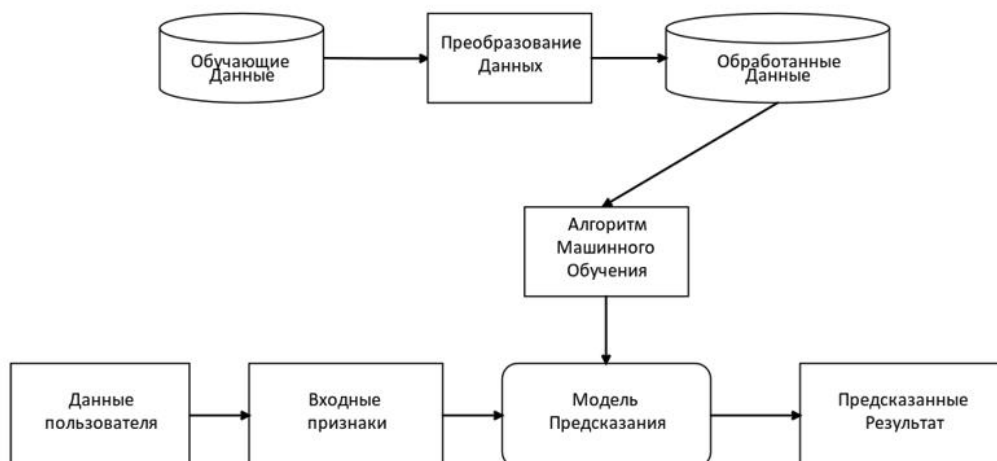


Рисунок 1 - Архитектура программы

Источник: анализ автора

Выводы

Быстродействующая модель предсказания, основанная на модели Длинной краткосрочной памяти предложен в данной статье, основываясь на существующих методах предсказания ошибок в автоматизированных системах. Данный подход повышает точность обнаружения ошибок в сравнении со Сверточной Нейронной Сетью. Преимущество данного подхода в точной и быстрой возможности предсказания следующего значения. Ошибки системы предсказываются и выдают предупреждение, сравнивая предыдущие значения наборов данных и основываясь на следующих данных используя Логистическую Регрессию.

Список литературы

1. Topological structure of complex predictions, авторы Менг Лиу, Тамал К. Дей, Девид Ф. Глейф, журнал Nature of Machine Intelligence 5, 1382-1389 (2023)
2. А.В. Кугаевских, Д.И. Муромцев, О.В. Кирсанова. Классические методы машинного обучения. – СПб: Университет ИТМО, 2022.
3. Основы машинного обучения: учебное пособие / О.В. Лимановская, Т.И. Алферьева; Мин-во науки и высш. образования РФ. Екатеринбург: Изд-во Урал. ун-та, 2020.
4. Бурков Андрей, Машинное обучение без лишних слов. — СПб.: Питер, 2020. — 192 с.: ил. — (Серия «Библиотека программиста»).
5. Мухамедиев Р.И., Амиргалиев Е.Н. Введение в машинное обучение: Учебник. – Алматы, 2022.

References

1. Topological structure of complex predictions, authors MengLi u, Tamal K. Day, David F. Plume, journal Nature of Machine Intelligence 5, 1382-1389 (2023)
2. A.V. Kugaevskikh, D.I. Muromtsev, O.V. Kirsanova. Classical machine learning methods. – St. Petersburg: ITMO University, 2022.
3. Fundamentals of machine learning: a textbook / O.V. Limanovskaya, T.I. Alferyeva; Ministry of Science and Higher Education. education of the Russian Federation. Yekaterinburg: Ural Publishing House. University, 2020.

4. Burkov Andrey, Machine learning without unnecessary words. — St. Petersburg: St. Petersburg, 2020. — p.192 ill. — (Series "Programmer's Library").
 5. Mukhamediev R.I., Amirgaliev E.N. Introduction to machine learning: Textbook. – Almaty, 2022.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.396

ТЕХНОЛОГИИ 3D-ПЕЧАТИ ДЛЯ ИЗГОТОВЛЕНИЯ ПЕЧАТНЫХ ПЛАТ: МЕТОДЫ, ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

¹ Соловьев В.А., ²Канюков А.Р., ³Сапунов Д.М., ⁴Булыгин И.В.

ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail:

¹volodimer@bmstu.ru, ²kanyukovar@student.bmstu.ru, ³kolegovdm@student.bmstu.ru, ⁴bulyyginiv@student.bmstu.ru

В данной статье представлен обзор и анализ методов для 3D-печати печатных плат. Было проведено исследование ряда научных трудов и статей на эту тему. Выявлено отсутствие всестороннего сравнения технологий 3D-печати печатных плат. В связи с этим основной целью данной статьи является анализ и сравнение широкого спектра возможностей в этой области. В ней рассматриваются различные технологии, на основе которых создаются современные печатные платы, широко используемые во многих областях деятельности человека. Была реализована классификация методов изготовления печатных плат по принципу их работы и отличительным характеристикам. Подробно описан механизм работы каждой рассматриваемой технологии, выявлены общие преимущества и недостатки. В статье описаны пять технологий для изготовления печатных плат: аэрозольное нанесение материала, капельное нанесение материала, непрерывное нанесение материала, послойное нанесение материала, многофункциональное нанесение материала. Рассмотренные в статье технологии являются наиболее популярными и распространенными на современном рынке. В рамках статьи обсуждается потенциал масштабирования такого типа производства.

Ключевые слова: аддитивные технологии, печатная плата, 3D-печать, 3D-принтер, прототипирование.

TECHNOLOGIES OF 3D-PRINTING FOR MANUFACTURING PRINTED CIRCUIT BOARDS: METHODS, ADVANTAGES AND DISADVANTAGES

¹ Solovyov V.A., ²Kanyukov A.R., ³Sapunov D.M., ⁴Bulygin I.V.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (105005, Moscow, 2nd Baumanskaya ul, 5 bld. 1), e-mail: ¹volodimer@bmstu.ru, ²kanyukovar@student.bmstu.ru, ³kolegovdm@student.bmstu.ru, ⁴bulyyginiv@student.bmstu.ru

This article provides an overview and analysis of methods for 3D-printing printed circuit boards. A study of a number of scientific papers and articles on this topic was realized. The absence of a comprehensive comparison of technologies for the 3D-printing printed circuit boards is revealed. In this regard, the main objective of this article is to analyze and compare a wide range of solutions in this area. It considers various technologies on the basis of which modern printed circuit boards that are widely used in many areas of human activity are being created. The classification of technologies of making printed circuit boards by the principle of their work has been realized. The mechanism of working of each technology under consideration is described in detail, the general advantages and disadvantages are identified. The article describes five technologies for making printed circuit boards: aerosol jet printing, drop on demand, continuous inkjet, fused deposition modeling, multi-functional additive manufacturing. The technologies considered in the article are the most popular and common in the current market. The article discusses the potential of scaling such a type of production.

Keywords: Additive technologies, printed circuit boards, 3D-printing, 3D-printer, prototyping.

Введение.

Аддитивные технологии в изготовлении печатных плат имеют преимущество перед субтрактивными: снижение отходов при производстве, в том числе вредных для человека и природы, уменьшение числа производственных этапов – нет необходимости в нанесении масок. А в случае с 3D-печатью печатную плату возможно полностью изготовить на одной установке. В целях прототипирования, а, возможно, в недалеком будущем – изготовления мелкосерийных партий, такие технологии позволяют обеспечить быстрое, недорогое и конфиденциальное производство печатных плат, что обуславливает актуальность изучения современных аддитивных технологий. Суть использования 3D технологий в изготовлении ПП заключается в формировании ПП либо с нуля, либо с использованием диэлектрического основания и нанесения на него проводящего рисунка.

Целью настоящего исследования является сбор и обобщение знаний о современных возможностях технологии 3D-печати печатных плат и представление сравнительного анализа методов на основе общих характеристик данной технологии.

Методы исследований.

В работе были формализованы и обобщены современные знания о технологиях 3D-печати печатных плат, был выполнен их качественный сравнительный анализ для выявления ключевых преимуществ и недостатков, что позволяет говорить об эффективности технологий в производстве.

Предметом исследования является сравнение технологий 3D-печати печатных плат на основе современных научных исследований.

Объектом исследования является повышение применимости технологий 3D-печати для эффективного серийного производства печатных плат.

Перед непосредственным переходом к методам, необходимо рассмотреть ряд важных вопросов. Одна из особенностей ПП, полученных 3D-печатью, заключается в возможности получения “3D-структуры” печатной платы. В случае пересечения соединений не требуется наносить полноценный диэлектрический слой поверх уже сформированных проводников, достаточно изолировать участок пересечения диэлектриком (Рисунок 1). Переходные отверстия могут быть исполнены как классически, так и по-новому: диэлектрический слой в местах соединения слоев не наносится, тем самым формируется контакт между различными слоями [1].

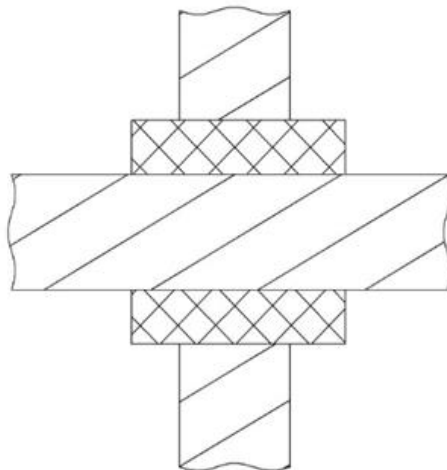


Рисунок 1 - 3D-структура взаимного расположения проводников

Ещё один важный аспект - монтаж компонентов, монтируемых поверхностно на ПП 3D-производства, схож с печатными платами, произведенными конвенциональными методами: во время печати проводников формируются контактные площадки, затем на них наносится дополнительный слой проводящих чернил, компонент устанавливается, чернила отверждаются. Дополнительно поверх установленного компонента может быть нанесен диэлектрический защитный слой, обеспечивающий большую адгезию к поверхности и защиту от окружающей среды. Возможно и использование низкотемпературных паяльных паст [2].

Одна из полезнейших апробированных возможностей рассмотренных методов - получение встроенных в коммутационную систему пассивных компонентов за счет различных чернил и геометрических форм. Например, при помощи метода АНМ были получены полимерные тонкопленочные резисторы номиналом от 100 Ом до 10 кОм с точностью до 10 % и установочной площадью 0,05 мм² [3]. В то же время напечатанные углеродистые резисторы имеют диапазон от 50 Ом до 1 МОм. Конденсаторы имеют емкость от 1 пФ до 1 нФ. Возможна печать катушек индуктивности, антенн [4]. Доступнее становится установка микросхемы «прямо на плату» (chip on board). Были получены и активные компоненты – транзисторы, светодиоды, батареи, фотоэлементы, однако в настоящее время их изготовление осуществимо только гибридным методом – сочетанием аддитивных и субтрактивных технологических операций [5].

Моделирование методом плавленого осаждения (Fused Deposition Modeling).

Метод плавленого осаждения (МПО) — это процесс аддитивного производства, при котором печатные платы изготавливаются путем нанесения материала слой за слоем. Это один из нескольких аддитивных процессов, включая стереолитографию (SL) и селективное лазерное спекание (SLS). Разработанный С. Скоттом Крапом в конце 1980-х годов и коммерциализированный в 1990 году компанией Stratasys, МПО широко используется для моделирования, создания прототипов и производственных приложений.

Принцип работы. В процессе МПО используется порталый робот, оснащенный экструдированной головкой, которая перемещается в направлениях X, Y и Z, в то время как рабочий стол перемещается вдоль осей Y и Z. Слои наносятся последовательно, при этом экструдер поднимается в соответствии с толщиной слоя.

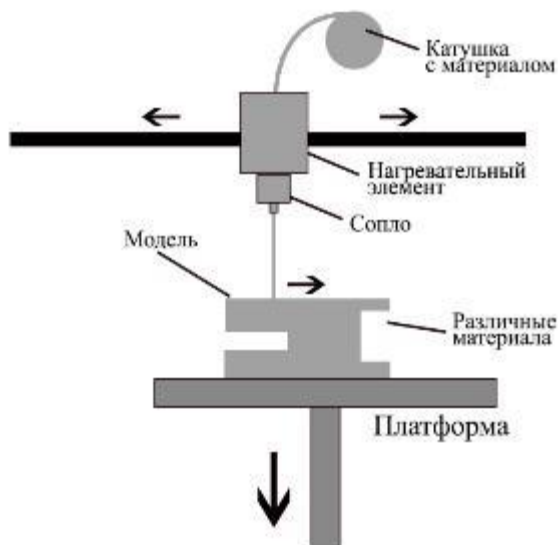


Рисунок 2 - Принцип работы МПО [6]

Используемые материалы. Для изготовления печатной платы в качестве изоляционных материалов используются полиамиды, керамика, высокотемпературные полимеры, термопластичный полиуретан, в то время как токопроводящим материалом является композитное углеродное волокно. Эти материалы выпускаются в виде нитей.

Этапы создания модели. Первоначально требуется CAD-модель печатной платы, которая сохраняется в формате Stereolithography (STL). Далее файл поступает в специальную программу для дальнейшего нарезания, а затем отправляется в МПО-станок. Дальнейшие параметры печати устанавливаются оператором станка, а по завершении деталь отсоединяется от стола сборки для последующих обработок.

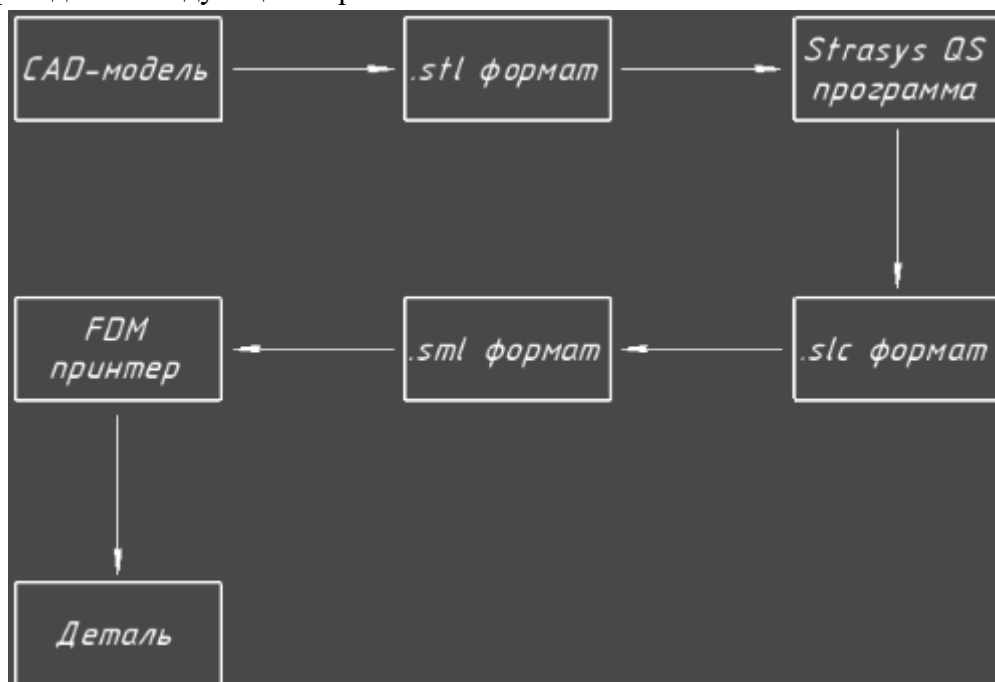


Рисунок 3 - Этапы по созданию физической модели методом МПО

Основные параметры, влияющие на качество МПО [7]. Ориентация: угол наклона детали по отношению к рабочей платформе влияет на точность размеров и использование материала. Толщина слоя: более толстые слои могут увеличить шероховатость поверхности. Угол раstra: направление раstra относительно оси X влияет на прочность и качество детали. Скорость нанесения: скорость, с которой материал наносится на сопло, может повлиять на общее качество детали.

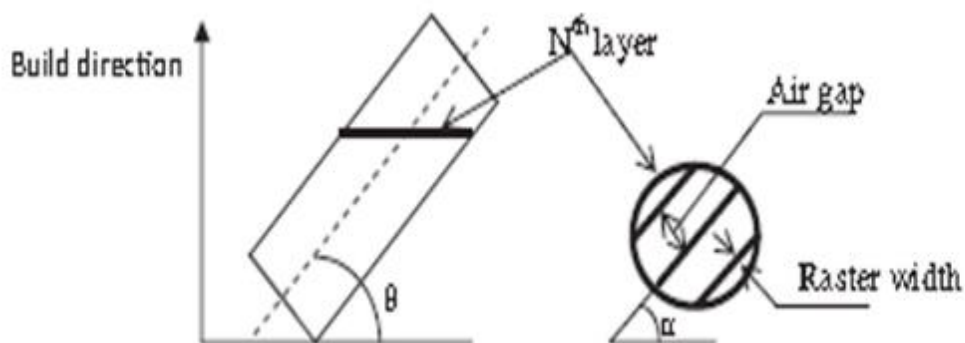


Рисунок 4 - Представление параметров процесса [7]

Характеристики деталей из МПО-материала. Точность размеров: степень соответствия между фактическими размерами и идеальными размерами изделия.

Шероховатость поверхности зависит от толщины слоя и эффекта лестницы, который возникает в результате послойного наращивания [8].

Механическая прочность зависит от сцепления между отдельными растрами и плотности используемого наполнителя.

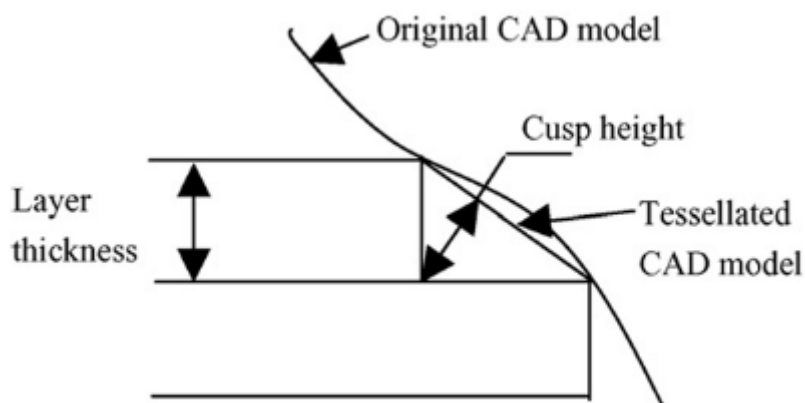


Рисунок 5 - Представление высоты острия в эффекте лестницы [8]

Аэрозольное нанесение материала (АНМ) (Aerosol Jet Printing).

Установки аэрозольного нанесения материала используют поток аэрозоля для фокусирования струи материала и его осаждения на подложку, затем следует спекание осажденного материала, либо его отверждение ультрафиолетом.

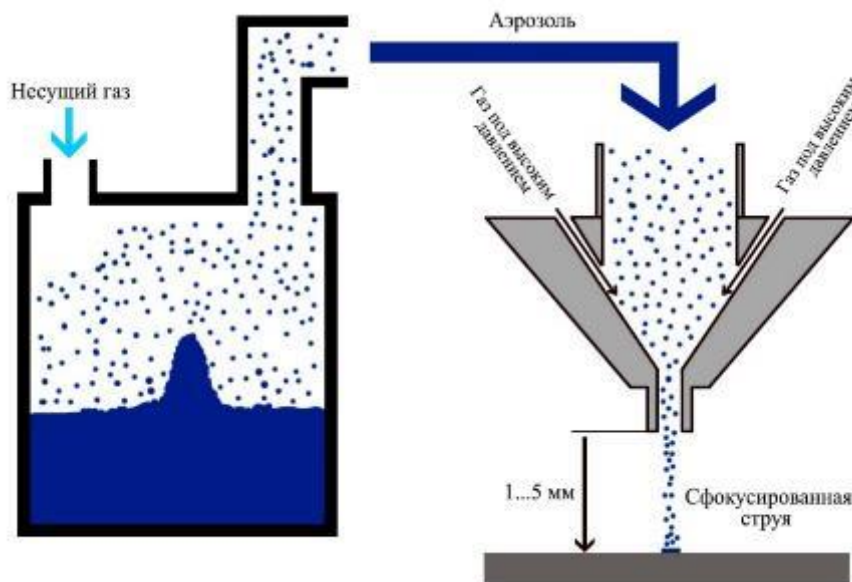


Рисунок 6 - Схема метода АНМ

Принцип печати. Жидкие чернила испаряют до частиц размером порядка 1–5 мкм, далее с помощью подачи несущего газа, например азота, формируется аэрозоль, который транспортируется в печатающую головку. Для наиболее точной печати необходимо обеспечить направленную струю аэрозоля диаметром менее 10 мкм через сопло, что достигается дополнительной подачей газа под высоким давлением. Это позволяет печатать мельчайшие структуры. Расстояние между соплом и подложкой составляет 1–5 мм - преимущество по сравнению с другими методами, так как позволяет наносить материал в канавки, печатать сложные объемные контуры, использовать основания различных форм, что было показано в работе [9], путем печати проводящего рисунка на сложных, изогнутых поверхностях из резины, отверждаемой ультрафиолетом – сформированных на том же принтере. Процесс проходит под контролем ЧПУ – CAD/CAM систем. Таким образом достигается стабильное и равномерное осаждение материала.

Напечатанные структуры находятся в размерном диапазоне от 10 мкм до нескольких миллиметров. Скорость подачи материала составляет до 10 мг/мин [10].

Взаимодействие между частицей и несущим газом описывается с помощью семи принципов: закона Стокса, описывающего силу трения на частицу в жидкости, Бассетова сила, которая описывает нестационарную силу вязкого сопротивления при ускорении частицы в жидкости, виртуальная масса, которая позволяет учесть инерцию жидкости вокруг частицы, градиент давления жидкости, сила тяжести, эффект Магнуса, который описывает силу, возникающую при обтекании жидкостью вращающейся частицы, сила Саффмана, которая описывает подъемную силу, возникающую из-за сдвигов в потоке жидкости. Сила Стокса и

Саффмана имеют наиболее значительный эффект на «прицельность» струи аэрозоля, обуславливают скорость выхода из сопла в 100 м/с [11].

Чернила. Теоретически, любой материал, взвешенный в газовой среде, подходит для метода АНМ. Это могут различные растворы, суспензии с наночастицами, содержащие металлы и их сплавы, полимеры, или даже биоматериалы. Современные коммерческие установки используют ультразвуковое или пневматическое дробление для получения жидкости вязкостью от 0,7 мПа·С до 2500 мПа·С [9]. Свойства полученных структур сильно зависят от размера частиц. Проводник, полученный спеканием при 200°C на 60 минут из чернил с содержанием наночастиц серебра 57-62% со средним их размером менее 50 нм, обладает сопротивлением 9,2 мОм/см, в то время как литой серебряный проводник имеет сопротивление 1,6 мОм/см [5]. Для печати методом АНМ на коммерческих принтерах используется дробление частиц до 1-5 мкм [12].

Для получения токопроводящих дорожек используются наночастицы серебра, меди, для диэлектрических слоев - акрилаты, фенольные, эпоксидные, полиуретановые, силиконовые смолы, резистивные чернила на основе углерода. После нанесения проводящего рисунка проводится спекание при температурах 120°C – 300°C на время от 30 до 60 минут, что предъявляет требования температурной устойчивости ко всем используемым материалам [10]. Возможно отверждение чернил ультрафиолетом, а также спекание лазером.

Диэлектрическое основание. В качестве ядра и препрегов печатной платы может использоваться как готовая подложка (стекло, стеклотекстолит, керамика), так и напечатанные диэлектрическими чернилами слои.

Метод АНМ позволяет изготавливать многослойные печатные платы с переходными отверстиями, достичь ширины печатного проводника в 10 мкм [13]. В работе [1] была продемонстрирована работоспособность двухслойной ПП, изготовленной исключительно методом АНМ, проведены успешные испытания на температурную устойчивость в диапазоне 10°– 80°.

Струйная печать. Капельное и непрерывное нанесение материала (drop on demand и continuous inkjet).

Два основных режима струйной печати — это режим непрерывной струйной печати (ННМ) и режим струйной печати по требованию, или же капельного нанесения материала (КНМ). В обоих методах жидкость проходит через отверстие или сопло.

В случае КНМ используется массив сопел, к каждому из которых поступает команда (с помощью пульсирующего давления) о выдавливании капли чернил. Затем капли падают по прямой линии [11].

Системы ННМ могут использовать как одно сопло, так и несколько. В режиме ННМ, как следует из его названия, жидкость непрерывно проталкивается через сопло. Затем струя распадается на поток капель в результате капиллярной неустойчивости Рэлея-Плато. Капельки заряжаются и отклоняются с помощью полевых пластин на подложку во время печати, в то время как остальные собираются улавливателем для переработки. ННМ обычно обеспечивает высокую скорость капли (> 10 м/с) [14] и, таким образом, обеспечивает быструю обработку для таких приложений, как маркировка и штрихкодирование. Благодаря непрерывному струйному действию сопло с меньшей вероятностью засоряется из-за испарения растворителя, особенно если используется летучий растворитель. Однако разрешение ННМ обычно ниже,

чем у КНМ. Кроме того, осаждение мелких фрагментированных капель на пластины поля может изменить электрическое поле и в худшем случае может привести к отказу принтера. Повторное использование чернил может также привести к загрязнению и потребовать повторной регулировки концентрации чернил для учета испарения растворителя. Струйная печать типа КНМ используется более широко, где капля генерируется только по мере необходимости с помощью термического или пьезоэлектрического привода. Типичная скорость капли составляет около 5–8 м/с [15]. Недостатком струйной печати является высыхание чернил в сопле во время простоя, что может привести к осаждению частиц в сопле и возможному засорению.



Рисунок 7 - Принцип работы метода струйной печати [16]

Параметры производительности печати. Ключевые показатели производительности включают:

Разрешение измеряется в точках на дюйм (DPI), зависит от объема капли, который определяется рабочим напряжением, продолжительностью импульса, диаметром сопла и типом подложки, и угла контакта. Для КНМ составляет порядка десятков микрон [15]. Консистенция зависит от свойств жидкости, таких как реология и поверхностное натяжение. Точность размещения капли: разница между целевым и фактическим местом падения капли (обычно угол отклонения равен $\pm 0,95^\circ$) [17].

Характеристика чернил. Вязкость и поверхностное натяжение. Измерение поверхностного натяжения: методы включают пластину Вильгельми, кольцо Дю Нуи и метод висячей капли [18].

Реологическая характеристика: ньютоновские жидкости имеют постоянную вязкость, в то время как неньютоновские жидкости демонстрируют поведение разжижения или загустевания при сдвиге, который составляет порядка 10^4 с^{-1} [19].

Распад струи и образование капли. Формирование капли регулируется инерционными, вязкими, упругими и поверхностными силами. Наиболее часто влияние вышеперечисленных свойств и других параметров, например диаметра сопла, на печатаемость чернил оценивается с использованием трех безразмерных чисел: числа Рейнольдса (для стабильного образования капель лежит в пределах от 1 до 10), описывающего соотношение между инерционными и вязкими силами, числа Вебера (для стабильного образования капель лежит в пределах от 4 до 1000), описывающего соотношение между инерционными и поверхностными силами, числа

Онезорге (для стабильного образования капель лежит в пределах от 0,1 до 1), описывающего отношение вязких и поверхностных сил [20–22].

Чернила. Практически любой материал может использоваться в качестве чернил: керамика, полимеры, коллоидные и гидрогели, металлические сплавы.

В современных процессах печати электроники чаще всего используются серебряные наночернила, хотя также доступны и золотые, медные и никелевые варианты. Серебро (Ag) и золото (Au) являются предпочтительными благодаря своей высокой стабильности, низкой химической активности и отличной электропроводности. В отличие от них, медь (Cu) и никель (Ni) применяются реже, так как подвержены окислению, что негативно сказывается на долговечности чернил и требует применения дополнительных защитных покрытий или печати в инертной атмосфере.

Металлоорганические чернила представляют собой металлическую соль, растворенную в специальном растворителе, которая восстанавливается в металлические частицы с помощью оптических или термических методов. Эти чернила существуют в растворенной форме, что предотвращает агломерацию и засорение сопла. Исследования показали, что металлоорганические частицы обеспечивают лучшую проводимость линий по сравнению с аналогами из наночернил и позволяют спекать при более низких температурах (ниже +150 °C).

Чернила на основе нанопроволок используются гораздо реже, чем наночернила, из-за высокого аспектного отношения нанопроволок и их низкой концентрации в чернилах, что может приводить к засорению сопел и необходимости многократной печати для достижения нужной проводимости. Тем не менее, они демонстрируют более высокую механическую пластичность, что делает их подходящими для создания антенн и мобильной электроники [23,24].

Для изготовления гибких проводников применяются чернила из композиции оксида графена, технического углерода и карбоксиметилцеллюлозы с сопротивлением 0,6 Ом на см.

Для изоляции обычно применяют как подложки, так и специальные чернила, такие как SU-8, SunTronic Solsys Jettable Insulator EMD 6415, поли(4-винилфенол) (ПВП, PVP) и другие. В гибкой электронике часто используют подложки [25] из полиимидов (PI, полиимидная пленка, например, Dupont Kapton), полиэтилентерефталата (ПЭТ, PET), полиэтиленнафталата (ПЭН, PEN) и полидиметилсилоксана (ПДМС, PDMS).

Многофункциональное нанесение материала (МФНМ).

Технология многофункционального нанесения обладает своей уникальностью, которая выделяет его среди многих других технологий, вместо использования традиционного ИК-нагрева, как это происходит в 3D-принтерах от компаний NanoDimension и BotFactory, в этом методе раскрывается потенциал УФ-излучения [2]. УФ-излучение может не только преобразовывать полимерные материалы, но и спекать наночастицы серебра, что является ключевым моментом в создании проводящих дорожек.

В качестве фундамента этой технологии лежит метод интенсивного импульсного света (IPL), основанный на фототермическом механизме, ксеноновые лампы генерируют короткие импульсы света, которые нагревают чернила, в следствии фотонного поглощения и дальнейшей генерации тепла [2]. Во время всего процесса следует внимательно контролировать термический аспект, чтобы избежать разрушение проводников в следствии резких температурных перепадов. Для серебряных наночернил с размером частиц менее 50 нм

УФ-излучение в диапазоне 390 нм является самым эффективным методом спекания без необходимости в термообработке [2]. Одной из важных особенностей данной технологии является то, что процесс фототермического спекания затрагивает только проводящие чернила, не нарушая ранее напечатанные полимерные компоненты [2].

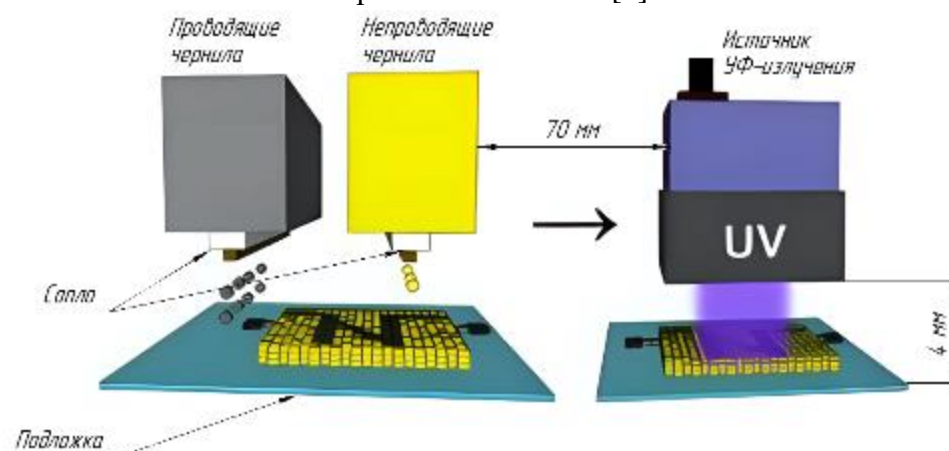


Рисунок 8 – Принцип работы метода МФМ [26]

Чернила. Современные установки используют следующие УФ-отверждаемые чернила: серебряные наночернила SilverJet DGP-40LT-15C фирмы Advanced Nano Products (ANP), состоящие из 38,85 мас.% частиц серебра, диспергированных в монометиловом эфире триэтиленгликоля (triethylene glycol monomethyl ether, TGME), графитовые чернила на водной основе серии 3800 фирмы Methode Development Co., диакрилатные мономерные диэлектрические чернила [2].

Получаемые структуры. Технологией многофункционального нанесения можно получать точные, с точки зрения геометрии, структуры, размером до 50-30 мкм, по сравнению с некоторыми другими методами.

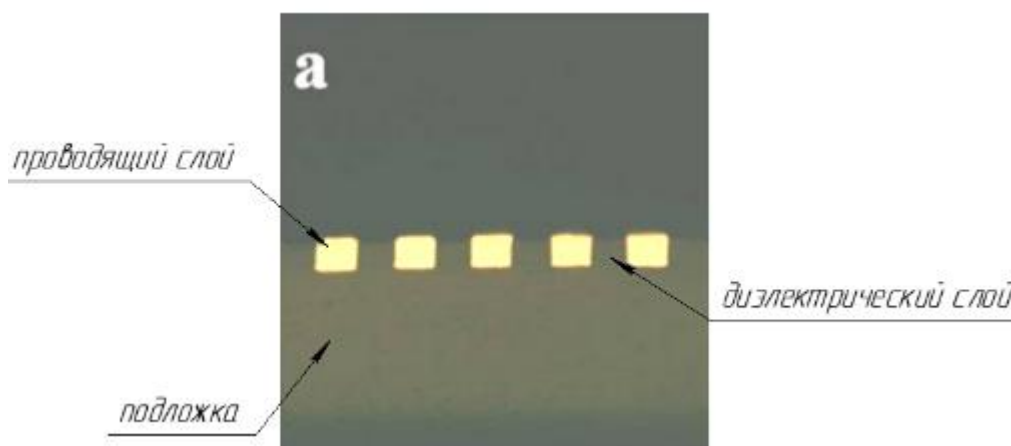


Рисунок 9 - Структура, получаемая технологией МФМ [27]

На Рисунке 9 представлено поперечное сечение тонких линий полученных с помощью МФМ, представляющие собой правильные прямоугольники, при этом средняя ширина нижней и верхней части очень близка к расчетным значениям (50 мкм), поскольку при изготовлении тонких линий из МФМ исключается процесс травления, медные линии без взаимодействия с раствором для травления получаются более ровными, и фактическая ширина

Технологии 3D-печати для изготовления печатных плат: методы, преимущества и недостатки / Соловьев В.А., Канюков А.Р., Сапунов Д.М. и др. // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 1(51) с. 152–167

проводника соответствует расчетной [27]. Таким образом высокая точность и гибкость и выделяет этот метод среди других.

Заключение.

Было проведено сравнение параметров печатных плат, получаемых методами 3D-печати (Таблица 1).

Таблица 1. - Сравнение методов 3D-печати для изготовления печатных плат

Общие сведения		Характеристика			
Наименование метода	Капельное нанесение материала	Непрерывное нанесение материала	Послойное наложение филамента	Многофункциональное нанесение материала	Аэрозольное нанесение материала
Класс точности ПП (ГОСТ Р 53429)	>7 - в теории, 5-6 - на практике [28]	3 [28]	5 [28]	6 [28]	>7 [28]
Тип изготавливаемых ПП	ЖПП/ГПП [28]	ЖПП/ГПП [28]	ЖПП/ГПП [28]	ЖПП [28]	ЖПП/ГПП [28]
Количество слоев ПП, шт.	>2 [28]	>2 [28]	>3 [28]	>2 [28]	>2 [28]
Минимальная ширина проводника, мкм	30 - в теории, 75 - на практике [5,29,30]	200 [15]	100 [30]	40 [27]	10 [9]
Минимальная толщина проводника, мкм	0,01-2 [5,31]	200 [32]	200 [31]	25 [27]	1,4 [5]
Минимальное расстояние между проводниками, мкм	100 [33]	400 [16]	100 [33]	80 [27]	20 [2]
Материал	Токопроводящий: Ag, Au, графен, реже Cu и Ni Изоляционный: полиимид, SU-8, SunTronic Solsys Jetttable Insulator EMD 6415, поли(4-винилфенол) (ПВП, PVP) и другие [25]	Токопроводящий: Ag, Au, графен, Cu и Ni, металлоорганика Изоляционный: полиимид, стекло, оксиды алюминия, керамика [25]	Токопроводящий: композитное углеродное волокно Изоляционный: полиамиды, керамика, высокотемпературные полимеры, термопластичный полиуретан [34]	Токопроводящий: Ag Изоляционный: диакрилатные мономерные диэлектрические чернила, содержащие три (пропиленгликоль) диакрилат, 2,4-диэтилтиоксанон и этил 4-(диметиламино) бензоат [2]	Токопроводящий: наночастицы серебра, меди. Изоляционный - акрилаты, фенольные, эпоксидные, полиуретановые, силиконовые смолы, резистивные чернила на основе углерода [10]
Форма	Чернила	Чернила	Филамент	Чернила	Чернила
Размер твердых частиц, мкм	в 50 раз меньше диаметра сопла [5,35]	0,02-10 [24]	10-50 [36]	Не менее 50 [2]	0,05–5 [13]
Вязкость мПа*с	1-40 [32,35]	1-40 [32,35]	100000-800000 [37]	13 [26]	0,7-2500 [12,13]
Поверхностное натяжение мН/м	25-50 [32]	25-50 [17]	30-50 [38]	30 - 37 [26]	-
Подложка	Не требуется	Не требуется	Не требуется	Требуется (алюминиевая) [27]	Не требуется

В результате сравнительного анализа было выявлено, что наиболее передовой из рассмотренных методов – аэрозольное напыление, однако, на данный момент, он является и самым дорогим, дороже и традиционных методов производства.

Текущие исследования направлены на улучшение шероховатости поверхности и механической прочности путем оптимизации параметров температурных профилей и методов напыления. В настоящее время не существует серийного производства печатных плат методом 3D-печати. Одна из причин – недостаточность исследовательской базы, а значит и отсутствие нормативной документации. Существуют и ограничения по оборудованию: нет 3D-принтеров, способных обеспечить полный цикл производства ПП. Для увеличения производительности и размеров получаемых ПП необходимы промышленные принтеры с большой рабочей областью и несколькими печатающими головками – таким образом можно формировать проводящий рисунок сразу нескольких ПП на одной подложке, как это происходит при изготовлении конвенциональными методами. Эти недостатки обуславливают и увеличенное время производства. При устранении вышеперечисленных недостатков технологии можно говорить о масштабировании производства ПП с помощью 3D-печати.

Список литературы

1. Bolger J. et al. Multi-layer PC boards Fabricated using Aerosol-jet Printing // International Symposium on Microelectronics. 2013. Vol. 2013, № 1. p. 000921–000926.
2. Смирнова О., Боброва Ю., Моисеев К. МЕТОДЫ 3D-ПЕЧАТИ ДЛЯ ИЗГОТОВЛЕНИЯ ПЕЧАТНЫХ ПЛАТ // ELECTRONICS: SCIENCE, TECHNOLOGY, BUSINESS. 2022. Vol. 219, № 8. pp. 128–136.
3. Kang B.J., Lee C.K., Oh J.H. All-inkjet-printed electrical components and circuit fabrication on a plastic substrate // Microelectron Eng. 2012. Vol. 97. pp. 251–254.
4. Adams J.J. et al. Conformal Printing of Electrically Small Antennas on Three-Dimensional Surfaces // Advanced Materials. 2011. Vol. 23, № 11. pp. 1335–1340.
5. Wilkinson N.J. et al. A review of aerosol jet printing—a non-traditional hybrid process for micro-manufacturing // The International Journal of Advanced Manufacturing Technology. 2019. Vol. 105, № 11. pp. 4599–4619.
6. Haghsefat K., K.; Eng M., Tingting L. FDM 3D Printing Technology and Its Fundamental Properties // In Proceedings of the International Conference on Innovation and Research in Engineering Sciences / ed. Haghsefat K., K.; Eng M., Tingting L. Tbilisi, 2020.
7. Sood A.K. et al. An investigation on sliding wear of FDM built parts // CIRP J Manuf Sci Technol. 2012. Vol. 5, № 1. pp. 48–54.
8. P.M. Pandey., N. Venkata Reddy., S.G. Dhande. Part Deposition Orientation Studies in Layer Manufacturing // Journal of Material Processing Technology. 2007. Vol. 185. pp. 125–131.
9. Werum K. et al. Aerosol Jet Printing and Interconnection Technologies on Additive Manufactured Substrates // Journal of Manufacturing and Materials Processing. 2022. Vol. 6, № 5. p. 119.
10. Lewis P., White R., Smith-Draper B. Lessons learned in the implementation of aerosol jet printing for fabricating multilayer circuit boards // Advancing Microelectronics. 2017. Vol. 44, № 3. pp. 12–15.
11. Martin G.D., Hoath S.D., Hutchings I.M. Inkjet printing - the physics of manipulating liquid jets and drops // J Phys Conf Ser. 2008. Vol. 105. p. 012001.

12. Christenson K.K. et al. Direct Printing of Circuit Boards Using Aerosol Jet^{*®} // NIP & Digital Fabrication Conference. 2011. Vol. 27, № 1. pp. 433–436.
13. Gupta A.A. et al. Aerosol-Jet Printed Transmission Lines for Microwave Packaging Applications // IEEE Trans Compon Packaging Manuf Technol. 2019. Vol. 9, № 12. pp. 2482–2489.
14. Derby B. Inkjet Printing of Functional and Structural Materials: Fluid Property Requirements, Feature Stability, and Resolution // Annu Rev Mater Res. 2010. Vol. 40, № 1. pp. 395–414.
15. Hutchings I. M., Martin G. D. Inkjet Technology for Digital Fabrication / ed. Hutchings I. M., Martin G. D. Manchester: Wiley, 2012.
16. Martin G.D., Hoath S.D., Hutchings I.M. Inkjet printing - the physics of manipulating liquid jets and drops // J Phys Conf Ser. 2008. Vol. 105. P. 012001.
17. Lean M. H. Method and apparatus for reducing drop placement error in printers: pat. US6367909B1 USA. United States, 2002.
18. Arthur W. Adamson., Alice P. Gast. Physical Chemistry of Surfaces. 6th ed. / ed. Arthur W. Adamson., Alice P. Gast. New York: Wiley, 1997.
19. Reis N., Ainsley C., Derby B. Ink-jet delivery of particle suspensions by piezoelectric droplet ejectors // J Appl Phys. 2005. Vol. 97, № 9.
20. DUINEVELD P.C. The stability of ink-jet printed lines of liquid with zero receding contact angle on a homogeneous substrate // J Fluid Mech. 2003. Vol. 477.
21. Reis N., Derby B. Ink Jet Deposition of Ceramic Suspensions: Modeling and Experiments of Droplet Formation // MRS Proceedings. 2000. Vol. 625. p. 117.
22. Son Y. et al. Spreading of an Inkjet Droplet on a Solid Surface with a Controlled Contact Angle at Low Weber and Reynolds Numbers // Langmuir. 2008. Vol. 24, № 6. pp. 2900–2907.
23. Huang G.-W., Xiao H.-M., Fu S.-Y. Wearable Electronics of Silver-Nanowire/Poly(dimethylsiloxane) Nanocomposite for Smart Clothing // Sci Rep. 2015. Vol. 5, № 1. p. 13971.
24. Seifert T. et al. Additive Manufacturing Technologies Compared: Morphology of Deposits of Silver Ink Using Inkjet and Aerosol Jet Printing // Ind Eng Chem Res. 2015. Vol. 54, № 2. pp. 769–779.
25. Beedasy V., Smith P.J. Printed Electronics as Prepared by Inkjet Printing // Materials. 2020. Vol. 13, № 3. p. 704.
26. Saleh E. 3D inkjet printing of digital composites for tailored dielectric properties // International Conference on Composites/Nano Engineering / ed. Saleh E. 2017.
27. He H. et al. Fabrication and surface treatment of fine copper lines for HDI printed circuit board with modified full-additive method // Circuit World. 2017. Vol. 43, № 3. pp. 131–138.
28. Е.В. Пирогова. Проектирование и технология печатных плат // Москва: ИНФРА-М, 2005.
29. Zhang H., Moon S.K., Ngo T.H. 3D Printed Electronics of Non-contact Ink Writing Techniques: Status and Promise // International Journal of Precision Engineering and Manufacturing-Green Technology. 2020. Vol. 7, № 2. pp. 511–524.
30. Nelson M.D., Ramkumar N., Gale B.K. Flexible, transparent, sub-100 μ m microfluidic channels with fused deposition modeling 3D-printed thermoplastic polyurethane // Journal of Micromechanics and Microengineering. 2019. Vol. 29, № 9. p. 095010.

31. Benedict. Voxel8 Developer's Kit 3D printer now shipping // Journal 3D printings and 3D printers news. 2016.
32. Antohe B. V., Wallace D.B. Acoustic Phenomena in a Demand-Mode Piezoelectric Ink-Jet Printer // NIP & Digital Fabrication Conference. 2001. Vol. 17, № 1. pp. 885–889.
33. Paul Hanaphy. Nano Dimension unveils new DragonFly IV and FLIGHT software: technical specifications and pricing // Journal of 3D printing industry. 2021.
34. Flowers P.F. et al. 3D printing electronic components and circuits with conductive thermoplastic filament // Addit Manuf. 2017. Vol. 18. pp. 156–163.
35. Cummins G., Desmulliez M.P.Y. Inkjet printing of conductive materials: a review // Circuit World. 2012. Vol. 38, № 4. pp. 193–213.
36. Singh R. et al. Effect of single particle size, double particle size and triple particle size Al₂O₃ in Nylon-6 matrix on mechanical properties of feed stock filament for FDM // Compos B Eng. 2016. Vol. 106. pp. 20–27.
37. Khaliq M.H. et al. On the use of high viscosity polymers in the fused filament fabrication process // Rapid Prototyp J. 2017. Vol. 23, № 4. pp. 727–735.
38. Sun Q. et al. Effect of processing conditions on the bonding quality of FDM polymer filaments // Rapid Prototyp J. 2008. Vol. 14, № 2. pp. 72–80

References

1. Bolger J. et al. Multi-layer PC boards Fabricated using Aerosol-jet Printing // International Symposium on Microelectronics. 2013. Vol. 2013, № 1. p. 000921–000926.
2. Smirnova O., Bobrova Y., Moiseev K. 3D PRINTING METHODS FOR THE MANUFACTURE OF PRINTED CIRCUIT BOARDS. 2022. Vol. 219, № 8. pp. 128–136.
3. Kang B.J., Lee C.K., Oh J.H. All-inkjet-printed electrical components and circuit fabrication on a plastic substrate // Microelectron Eng. 2012. Vol. 97. pp. 251–254.
4. Adams J.J. et al. Conformal Printing of Electrically Small Antennas on Three-Dimensional Surfaces // Advanced Materials. 2011. Vol. 23, № 11. pp. 1335–1340.
5. Wilkinson N.J. et al. A review of aerosol jet printing—a non-traditional hybrid process for micro-manufacturing // The International Journal of Advanced Manufacturing Technology. 2019. Vol. 105, № 11. pp. 4599–4619.
6. Haghsefat K., K.; Eng M., Tingting L. FDM 3D Printing Technology and Its Fundamental Properties // In Proceedings of the International Conference on Innovation and Research in Engineering Sciences / ed. Haghsefat K., K.; Eng M., Tingting L. Tbilisi, 2020.
7. Sood A.K. et al. An investigation on sliding wear of FDM built parts // CIRP J Manuf Sci Technol. 2012. Vol. 5, № 1. pp. 48–54.
8. P.M. Pandey., N. Venkata Reddy., S.G. Dhande. Part Deposition Orientation Studies in Layer Manufacturing // Journal of Material Processing Technology. 2007. Vol. 185. pp. 125–131.
9. Werum K. et al. Aerosol Jet Printing and Interconnection Technologies on Additive Manufactured Substrates // Journal of Manufacturing and Materials Processing. 2022. Vol. 6, № 5. p. 119.
10. Lewis P., White R., Smith-Draper B. Lessons learned in the implementation of aerosol jet printing for fabricating multilayer circuit boards // Advancing Microelectronics. 2017. Vol. 44, № 3. pp. 12–15.

11. Martin G.D., Hoath S.D., Hutchings I.M. Inkjet printing - the physics of manipulating liquid jets and drops // J Phys Conf Ser. 2008. Vol. 105. p. 012001.
12. Christenson K.K. et al. Direct Printing of Circuit Boards Using Aerosol Jet^{®®} // NIP & Digital Fabrication Conference. 2011. Vol. 27, № 1. pp. 433–436.
13. Gupta A.A. et al. Aerosol-Jet Printed Transmission Lines for Microwave Packaging Applications // IEEE Trans Compon Packaging Manuf Technol. 2019. Vol. 9, № 12. pp. 2482–2489.
14. Derby B. Inkjet Printing of Functional and Structural Materials: Fluid Property Requirements, Feature Stability, and Resolution // Annu Rev Mater Res. 2010. Vol. 40, № 1. pp. 395–414.
15. Hutchings I. M., Martin G. D. Inkjet Technology for Digital Fabrication / ed. Hutchings I. M., Martin G. D. Manchester: Wiley, 2012.
16. Martin G.D., Hoath S.D., Hutchings I.M. Inkjet printing - the physics of manipulating liquid jets and drops // J Phys Conf Ser. 2008. Vol. 105. P. 012001.
17. Lean M. H. Method and apparatus for reducing drop placement error in printers: pat. US6367909B1 USA. United States, 2002.
18. Arthur W. Adamson., Alice P. Gast. Physical Chemistry of Surfaces. 6th ed. / ed. Arthur W. Adamson., Alice P. Gast. New York: Wiley, 1997.
19. Reis N., Ainsley C., Derby B. Ink-jet delivery of particle suspensions by piezoelectric droplet ejectors // J Appl Phys. 2005. Vol. 97, № 9.
20. DUINEVELD P.C. The stability of ink-jet printed lines of liquid with zero receding contact angle on a homogeneous substrate // J Fluid Mech. 2003. Vol. 477.
21. Reis N., Derby B. Ink Jet Deposition of Ceramic Suspensions: Modeling and Experiments of Droplet Formation // MRS Proceedings. 2000. Vol. 625. p. 117.
22. Son Y. et al. Spreading of an Inkjet Droplet on a Solid Surface with a Controlled Contact Angle at Low Weber and Reynolds Numbers // Langmuir. 2008. Vol. 24, № 6. pp. 2900–2907.
23. Huang G.-W., Xiao H.-M., Fu S.-Y. Wearable Electronics of Silver-Nanowire/Poly(dimethylsiloxane) Nanocomposite for Smart Clothing // Sci Rep. 2015. Vol. 5, № 1. p. 13971.
24. Seifert T. et al. Additive Manufacturing Technologies Compared: Morphology of Deposits of Silver Ink Using Inkjet and Aerosol Jet Printing // Ind Eng Chem Res. 2015. Vol. 54, № 2. pp. 769–779.
25. Beedasy V., Smith P.J. Printed Electronics as Prepared by Inkjet Printing // Materials. 2020. Vol. 13, № 3. p. 704.
26. Saleh E. 3D inkjet printing of digital composites for tailored dielectric properties // International Conference on Composites/Nano Engineering / ed. Saleh E. 2017.
27. He H. et al. Fabrication and surface treatment of fine copper lines for HDI printed circuit board with modified full-additive method // Circuit World. 2017. Vol. 43, № 3. pp. 131–138.
28. E.V. Pirogova. Design and Technology of Printed Circuit Boards // Moscow: INFRA-M, 2005
29. Zhang H., Moon S.K., Ngo T.H. 3D Printed Electronics of Non-contact Ink Writing Techniques: Status and Promise // International Journal of Precision Engineering and Manufacturing-Green Technology. 2020. Vol. 7, № 2. pp. 511–524.

30. Nelson M.D., Ramkumar N., Gale B.K. Flexible, transparent, sub-100 μ m microfluidic channels with fused deposition modeling 3D-printed thermoplastic polyurethane // *Journal of Micromechanics and Microengineering*. 2019. Vol. 29, № 9. p. 095010.
 31. Benedict. Voxel8 Developer's Kit 3D printer now shipping // *Journal 3D printings and 3D printers news*. 2016.
 32. Antohe B. V., Wallace D.B. Acoustic Phenomena in a Demand-Mode Piezoelectric Ink-Jet Printer // *NIP & Digital Fabrication Conference*. 2001. Vol. 17, № 1. pp. 885–889.
 33. Paul Hanaphy. Nano Dimension unveils new DragonFly IV and FLIGHT software: technical specifications and pricing // *Journal of 3D printing industry*. 2021.
 34. Flowers P.F. et al. 3D printing electronic components and circuits with conductive thermoplastic filament // *Addit Manuf*. 2017. Vol. 18. pp. 156–163.
 35. Cummins G., Desmulliez M.P.Y. Inkjet printing of conductive materials: a review // *Circuit World*. 2012. Vol. 38, № 4. pp. 193–213.
 36. Singh R. et al. Effect of single particle size, double particle size and triple particle size Al₂O₃ in Nylon-6 matrix on mechanical properties of feed stock filament for FDM // *Compos B Eng*. 2016. Vol. 106. pp. 20–27.
 37. Khaliq M.H. et al. On the use of high viscosity polymers in the fused filament fabrication process // *Rapid Prototyp J*. 2017. Vol. 23, № 4. pp. 727–735.
 38. Sun Q. et al. Effect of processing conditions on the bonding quality of FDM polymer filaments // *Rapid Prototyp J*. 2008. Vol. 14, № 2. pp. 72–80
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

ЗАЩИТА ОТ АТАК С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ ТАБЛИЦ В БАЗАХ ДАННЫХ

Троян И.В.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
it.bonch@gmail.com

Временные таблицы широко используются в базах данных для хранения промежуточных данных, однако они могут стать вектором атак, если не обеспечена надлежащая защита. В статье рассматриваются основные угрозы, связанные с использованием временных таблиц, такие как SQL-инъекции, эксплуатация временных таблиц для эскалации привилегий, а также методы защиты, включая контроль доступа, шифрование и мониторинг активности.

Ключевые слова: Временные таблицы, базы данных, SQL-инъекции, безопасность, эскалация привилегий, контроль доступа, шифрование.

PROTECTING AGAINST ATTACKS USING TEMPORARY TABLES IN DATABASES

Troyan I.V.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: it.bonch@gmail.com

Temporary tables are widely used in databases for storing intermediate data, but they can become an attack vector if not properly secured. This article explores the main threats associated with temporary tables, such as SQL injection and privilege escalation, and discusses protection methods, including access control, encryption, and activity monitoring.

Keywords: Temporary tables, databases, sql injection, security, privilege escalation, access control, encryption..

Введение

Временные таблицы являются важным инструментом в базах данных, поскольку они позволяют хранить временные данные, используемые для выполнения сложных операций, оптимизации запросов или выполнения аналитических вычислений. Однако, несмотря на их полезность, временные таблицы могут представлять угрозу для безопасности, если они используются неправильно или без должной защиты. Злоумышленники могут использовать уязвимости, связанные с временными таблицами, для кражи данных, изменения конфиденциальной информации или даже получения доступа к системам, которые выходят за рамки базы данных.

Одной из наиболее распространённых атак на базы данных является использование SQL-инъекций, с помощью которых злоумышленники получают возможность создавать или модифицировать временные таблицы для достижения своих целей. Например, при

недостаточной валидации входных данных злоумышленник может создать временные таблицы, содержащие вредоносные данные, или использовать их для обхода механизмов аутентификации. Проблема осложняется тем, что временные таблицы часто не подвергаются такому же уровню защиты, как основные таблицы базы данных, из-за их временной природы.

В статье рассматриваются основные риски, связанные с временными таблицами, и предлагаются методы их предотвращения, включая внедрение строгих политик доступа, использование современных технологий шифрования и мониторинг активности для обнаружения подозрительных действий.

Защита от атак с использованием временных таблиц в базах данных

Временные таблицы, как правило, создаются для выполнения промежуточных операций, таких как сортировка, агрегация данных или хранение результатов сложных вычислений. Однако их временный характер и высокая степень использования в процессе обработки данных делают их привлекательным объектом для атак. Одна из главных проблем заключается в том, что временные таблицы создаются и используются во временных пространствах, доступ к которым может быть плохо контролируемым. Злоумышленники могут использовать этот недостаток для реализации атак, направленных на нарушение конфиденциальности, целостности или доступности данных[1].

Наиболее известный тип атак, связанный с временными таблицами, — это SQL-инъекции. В рамках такой атаки злоумышленники вводят вредоносные SQL-запросы через пользовательский ввод или API-интерфейсы, которые затем исполняются сервером базы данных. Если временные таблицы используются для хранения результатов запросов, атакующий может вставить туда вредоносные данные. Например, временная таблица, используемая для проверки идентификаторов сессий, может быть скомпрометирована для предоставления атакующему доступа к данным других пользователей[2].

Ещё одной угрозой является эксплуатация временных таблиц для эскалации привилегий. Если пользователь базы данных имеет право на создание временных таблиц, он потенциально может попытаться модифицировать данные в основной базе, используя свои привилегии через временные таблицы. Например, временные таблицы могут быть использованы для выполнения сложных SQL-запросов, которые маскируют доступ к конфиденциальной информации или попытки её изменения[3].

Важной частью защиты временных таблиц является управление доступом. Рекомендуется ограничивать права на создание и модификацию временных таблиц только для тех пользователей, которым это действительно необходимо. Например, использование принципа наименьших привилегий может значительно снизить вероятность эксплуатации временных таблиц в качестве вектора атаки. Кроме того, использование механизмов аутентификации и авторизации, таких как роли и группы, может помочь в ограничении доступа к временным таблицам[4].

Шифрование данных, хранящихся во временных таблицах, — ещё один важный аспект безопасности. Современные базы данных предоставляют возможности шифрования на уровне столбцов или таблиц, что позволяет защитить данные, даже если атакующий получит к ним доступ. Однако стоит учитывать, что шифрование увеличивает нагрузку на сервер, поэтому его следует использовать выборочно, исходя из чувствительности данных.

Мониторинг активности базы данных помогает обнаруживать подозрительное поведение, связанное с временными таблицами. Например, аномально большое количество создаваемых временных таблиц или использование сложных SQL-запросов, которые отклоняются от стандартных рабочих процессов, могут указывать на попытки злоумышленников проникнуть в систему. Использование инструментов журналирования и анализа логов позволяет выявлять и предотвращать подобные атаки до того, как они нанесут ущерб[5].

Важно учитывать, что временные таблицы также могут стать вектором атак в случае их неправильного удаления. Например, если временная таблица не удаляется после завершения её использования, она может быть использована злоумышленником для внедрения вредоносных данных или выполнения атак. Поэтому рекомендуется использовать автоматическое удаление временных таблиц после завершения транзакции или сессии, а также регулярно проверять временные пространства на предмет остатков данных.

Заключение

Временные таблицы являются неотъемлемой частью современных баз данных, однако их использование сопряжено с рядом рисков для безопасности. Уязвимости, связанные с временными таблицами, могут быть использованы злоумышленниками для выполнения SQL-инъекций, эскалации привилегий и других видов атак. Эти угрозы требуют внедрения надёжных механизмов защиты, включая строгий контроль доступа, шифрование данных и мониторинг активности.

Защита временных таблиц должна быть приоритетом для разработчиков и администраторов баз данных, поскольку они часто становятся незамеченными объектами атак. Соблюдение принципов минимизации прав, регулярное обновление систем безопасности и автоматическое удаление временных таблиц после их использования — всё это ключевые меры для обеспечения надёжной защиты.

В условиях, когда базы данных продолжают оставаться одной из основных целей кибератак, эффективная защита временных таблиц становится необходимым элементом стратегии безопасности организаций. Только комплексный подход, сочетающий технические и организационные меры, способен предотвратить потенциальные угрозы и сохранить конфиденциальность, целостность и доступность данных в информационных системах.

Список литературы

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. – 2004.
4. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

5. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 92-101

References

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
 2. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed information systems of personal data //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Dushin S. E. et al. Synthesis of structurally complex nonlinear control systems. – 2004.
 4. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
 5. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology //Ophthalmosurgery. - 2022. – No. 4s. – pp. 92-101.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

ЭФФЕКТИВНЫЕ МЕТОДЫ РАЗБИЕНИЯ И ИЗОЛЯЦИИ МЕТАДАНЫХ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ

Троян И.В.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: it.bonch@gmail.com

Метаданные часто являются ценным источником информации для злоумышленников, поскольку они могут содержать ключевую информацию о пользователях, приложениях и системах. Статья описывает подходы к разбиению и изоляции метаданных, такие как минимизация их сбора, применение принципа наименьших привилегий и использование специальных хранилищ для предотвращения несанкционированного доступа. Эти методы помогают значительно повысить уровень безопасности данных и защитить конфиденциальную информацию.

Ключевые слова: Метаданные, разбиение, изоляция, безопасность данных, принцип наименьших привилегий, защита информации, хранилище метаданных.

EFFECTIVE METHODS FOR PARTITIONING AND ISOLATING METADATA TO ENHANCE SECURITY

Troyan I.V.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: it.bonch@gmail.com

Metadata is often a valuable information source for attackers, as it can contain critical insights about users, applications, and systems. This article outlines approaches to partitioning and isolating metadata, such as minimizing its collection, applying the principle of least privilege, and using dedicated storage solutions to prevent unauthorized access. These methods significantly improve data security and safeguard sensitive information.

Keywords: Metadata, partitioning, isolation, data security, principle of least privilege, information protection, metadata storage.

Введение

Метаданные, представляющие собой данные о данных, играют важную роль в современных системах. Они содержат информацию о структурах баз данных, логах событий, сессиях пользователей и многом другом. Несмотря на их полезность, метаданные представляют значительный риск для безопасности. Злоумышленники часто используют их для анализа инфраструктуры, выявления уязвимых мест и выполнения целенаправленных атак. Например, метаданные логов могут содержать ключевую информацию о работе приложений или сети, включая IP-адреса, идентификаторы пользователей и временные метки.

В условиях увеличивающегося числа атак, связанных с утечкой данных, важно разработать и внедрить стратегии по защите метаданных. Одним из наиболее эффективных

методов является разбиение и изоляция метаданных. Это подразумевает их разделение на независимые сегменты с ограничением доступа к каждому из них, а также изоляцию в специализированных хранилищах. Подход позволяет минимизировать ущерб в случае успешной атаки и снизить вероятность компрометации всей системы.

Эффективные методы разбиения и изоляции метаданных для повышения безопасности

Разбиение и изоляция метаданных — это фундаментальные методы, направленные на минимизацию рисков, связанных с их утечкой или несанкционированным доступом. Первый шаг в этом процессе — минимизация объема собираемых метаданных. Организации часто собирают больше информации, чем необходимо для выполнения бизнес-задач, что увеличивает риск её компрометации. Например, в логах веб-приложений могут сохраняться конфиденциальные данные пользователей, которые не требуются для мониторинга или отладки. Оптимизация процессов сбора данных, включая использование инструментов фильтрации и маскирования, помогает исключить хранение избыточной информации[1].

Далее, метаданные должны быть разделены на логически независимые сегменты. Например, данные о пользователях и данные об их активности в системе могут храниться в разных хранилищах, чтобы ограничить последствия в случае утечки. Разделение данных также должно учитывать их уровень критичности. Высококчувствительные данные, такие как персональные данные или информация о платежах, должны быть строго отделены от менее критичных данных. Это позволяет применить к различным сегментам разные уровни защиты, включая использование более сложных механизмов шифрования и усиленных политик доступа для особо важных данных[2].

Изоляция метаданных предполагает использование физических или логических методов защиты. Например, критически важные метаданные могут храниться в изолированных сегментах облачной инфраструктуры, доступ к которым осуществляется через строго контролируемые API-интерфейсы. Локальные хранилища метаданных могут быть защищены дополнительными уровнями аутентификации и авторизации. Применение технологии виртуализации также может быть эффективным решением: виртуальные машины или контейнеры могут использоваться для хранения и обработки метаданных, обеспечивая их логическую изоляцию[3].

Ещё одним важным аспектом является управление доступом к метаданным. Принцип наименьших привилегий (Least Privilege) требует, чтобы пользователи и приложения имели доступ только к тем данным, которые необходимы для выполнения их задач. Например, разработчики могут иметь доступ к логам только тех компонентов системы, которые они поддерживают, в то время как доступ к логам всего приложения может быть ограничен только для системных администраторов[4].

Для повышения безопасности также рекомендуется использовать механизмы шифрования. Даже если злоумышленник получит доступ к метаданным, их зашифрованное состояние затруднит их использование. Современные методы шифрования, такие как AES или RSA, могут быть интегрированы в процесс хранения и передачи метаданных, обеспечивая их защиту на всех этапах жизненного цикла.

Важным элементом является аудит и мониторинг доступа к метаданным. Логирование всех операций, связанных с чтением, изменением или удалением метаданных, позволяет

выявить подозрительные активности и своевременно реагировать на инциденты. Инструменты анализа логов с применением технологий машинного обучения могут помочь обнаруживать аномалии и предотвращать угрозы[5].

Наконец, сегментация сети, в которой работают приложения, использующие метаданные, также играет важную роль. Изоляция сетевых сегментов позволяет предотвратить распространение угроз в случае успешной атаки. Например, если злоумышленник получит доступ к одному сегменту, строгая сегментация ограничит его возможность проникнуть в другие части системы.

Заключение

Эффективные методы разбиения и изоляции метаданных являются важной частью современной стратегии обеспечения безопасности. В условиях увеличивающегося числа кибератак, направленных на компрометацию данных, эти подходы позволяют минимизировать потенциальные риски и обеспечить защиту конфиденциальной информации.

Разделение данных на логически независимые сегменты, их изоляция в специализированных хранилищах, шифрование и строгий контроль доступа помогают снизить вероятность утечек и защитить критически важные ресурсы. Применение принципа наименьших привилегий и использование сегментации сети дополняют комплексный подход к защите метаданных.

Организации, стремящиеся повысить уровень безопасности своих систем, должны интегрировать описанные методы в свои стратегии защиты данных. Это не только укрепит их защиту от киберугроз, но и поможет обеспечить соблюдение регуляторных требований и защиту репутации.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.

2. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Lesnova E. M., Pestov I. E. Development of a method of error detection and correction for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 5. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelecommunications in science and education. - 2021. – pp. 409-414.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738: 004.897

ИССЛЕДОВАНИЕ ПРЕИМУЩЕСТВ ИСПОЛЬЗОВАНИЯ ЗАЩИЩЕННЫХ ЛОКАЛЬНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Шмидт А.А.

ООО "ГАЗПРОМ ДОБЫЧА ЯМБУРГ", Новый Уренгой, Россия (629306, Ямало-Ненецкий автономный округ, город Новый Уренгой, ул. Геологоразведчиков, д.9); ФГБОУ ВО "СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ", Новосибирск, Россия (630102, Новосибирская область, город Новосибирск, ул. Кирова, д. 86), e-mail: a.shmidt@yamburg.gazprom.ru

Статья посвящена исследованию преимуществ использования защищённых локальных сетей передачи данных. Отмечается, что защищенные локальные сети передачи данных представляют собой эффективное средство обеспечения безопасности и конфиденциальности информации. Автор приводит преимущества использования ЗЛС, выделяет основные компоненты защищённых локальных сетей. В завершение автор делает вывод о том, что использование защищённых локальных сетей передачи данных — это не просто вопрос технологического прогресса, но необходимость в условиях современного информационного мира. Преимущества, такие как защита конфиденциальности, предотвращение несанкционированного доступа, повышение надёжности и соответствие законодательным требованиям, делают защищённые ЛС неотъемлемой частью инфраструктуры любой успешной организации.

Ключевые слова: Защищенные локальные сети, передача данных, конфиденциальность, кибератака, шифрование, защита, контроль, угрозы безопасности.

EXPLORING THE BENEFITS OF USING SECURE LOCAL DATA NETWORKS

Schmidt A.A.

GAZPROM DOBYCHA YAMBURG LLC, Novy Urengoy, Russia (629306, Yamalo-Nenets Autonomous Okrug, Novy Urengoy, Geologorazvedchikov St., 9); SIBIRIAN STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Novosibirsk, Russia (86, Kirova st., Novosibirsk, Novosibirsk region, 630102, Russia), e-mail: a.shmidt@yamburg.gazprom.ru

The article is devoted to the study of the advantages of using secure local data networks. It is noted that secure local data transmission networks are an effective means of ensuring the security and confidentiality of information. The author cites the advantages of using a VPN, highlights the main components of secure local area networks. In conclusion, the author concludes that the use of secure local data transmission networks is not just a matter of technological progress, but a necessity in the modern information world. Advantages such as privacy protection, prevention of unauthorized access, increased reliability and compliance with legal requirements make secure personal data an integral part of the infrastructure of any successful organization.

Keywords: Secure local area networks, data transmission, confidentiality, cyberattack, encryption, protection, control, security threats.

Цель исследования – установить преимущества использования защищённых локальных сетей передачи данных. Проблема исследования состоит в том, что в наше время, когда информация становится одним из самых ценных ресурсов, вопросы её безопасности выходят

на первый план. В условиях стремительного развития технологий и увеличения количества киберугроз обеспечение безопасности данных становится особенно актуальным. Одним из решений для повышения безопасности передачи данных является использование защищённых локальных сетей. Методология исследования включает в себя анализ отечественной и зарубежной научной литературы[1].

Защищённая локальная сеть передачи данных — это сеть, которая использует специальные меры и технологии для обеспечения конфиденциальности, целостности и доступности передаваемой информации. Основная цель таких сетей — минимизация рисков, связанных с угрозами, которые могут возникнуть в процессе передачи и хранения данных. Защищённые ЛСПД могут быть реализованы как в рамках организации, так и между различными организациями. Основные компоненты защищённых локальных сетей:

1. Шифрование данных.
2. Системы аутентификации.
3. Межсетевые экраны и системы предотвращения вторжений.
4. Сегментация сети[2].

Первое и самое очевидное преимущество защищённых локальных сетей – это обеспечение конфиденциальности передаваемой информации. Использование шифрования и других методов защиты позволяет избежать несанкционированного доступа к данным. Это особенно актуально для организаций, которые работают с чувствительной информацией, такой как финансовые данные, личные данные клиентов и сотрудники. Защищённые локальные сети значительно снижают риск кибератак. Киберпреступники часто нацеливаются на уязвимости в сетевой инфраструктуре для получения доступа к данным. Применение современных технологий защиты, таких как системы предотвращения вторжений, межсетевые экраны и аутентификация пользователей, делает сети более стойкими к атакам, таким как DDoS, фишинг и других видов киберугроз[3].

Защищённые локальные сети позволяют применять строгие меры контроля доступа к данным. Системы аутентификации и авторизации гарантируют, что только уполномоченные пользователи могут получить доступ к определённым ресурсам. Это значительно снижает риск утечки данных и несанкционированного доступа, так как только определённые сотрудники могут работать с конфиденциальной информацией. Современные системы защищённых локальных сетей часто сопровождаются инструментами для мониторинга и управления сетевым трафиком. Администраторы могут отслеживать активность пользователей, выявлять подозрительные действия и оперативно реагировать на возможные угрозы. Это позволяет не только предотвратить инциденты, но и улучшить общую безопасность сети.

Кибератаки и утечки данных могут привести к значительным финансовым потерям для организаций. Инвестиции в защищённые локальные сети могут помочь избежать высоких затрат, связанных с восстановлением после инцидента, утратой репутации и юридическими последствиями. В долгосрочной перспективе это может значительно уменьшить общие расходы на управление безопасностью[4].

Одним из главных преимуществ защищённых локальных сетей передачи данных является повышенный уровень безопасности. Защита данных важна для предотвращения утечек конфиденциальной информации, хакерских атак и других угроз. Защищённые сети предоставляют возможность шифрования передаваемых данных, авторизации пользователей,

контроля доступа и других методов, обеспечивающих безопасность передачи данных. Защищенные локальные сети также способствуют повышению производительности и эффективности работы предприятия. Благодаря защите данных и их надежной передаче устраняются возможные задержки, сбои и потери информации. Это позволяет сотрудникам работать более эффективно и безопасно, не тратя время на восстановление данных или борьбу с угрозами. Создание защищенных сетей передачи данных также способствует сокращению расходов на обслуживание и поддержку информационной инфраструктуры предприятия. Благодаря надежной защите данных уменьшается вероятность возникновения проблем, снижается риск потери информации и снижаются затраты на устранение последствий нарушений безопасности.

Еще одним важным преимуществом защищенных локальных сетей передачи данных является обеспечение соблюдения законодательства и нормативных требований по защите данных. В современном мире все чаще встречаются случаи нарушения конфиденциальности информации и утечек данных. Защищенные сети позволяют предотвратить подобные ситуации и обеспечить соблюдение законодательства в области информационной безопасности[5].

Одним из самых эффективных способов защиты информации является шифрование трафика, особенно в рамках защищённых локальных сетей передачи данных. Шифрование трафика — это процесс преобразования данных в такую форму, которая делает их недоступными для несанкционированного доступа. Это достигается с помощью криптографических алгоритмов, которые кодируют информацию, передаваемую по сети. Лишь авторизованные пользователи с соответствующими ключами могут расшифровать и получить доступ к данным. Преимущества шифрования трафика:

1. Защита конфиденциальности: Одним из самых очевидных преимуществ шифрования является обеспечение конфиденциальности передаваемой информации. Это особенно критично для бизнеса, работающего с личными данными клиентов, финансовой информацией и другим чувствительным контентом.

2. Защита от утечек данных: Шифрование снижает риск утечек и несанкционированного доступа к данным. Даже если злоумышленник перехватит трафик, он не сможет расшифровать информацию без доступа к ключам. Это становится особенно важным в условиях растущей киберугрозы.

3. Соблюдение нормативных требований: Во многих странах существуют законы и нормативные акты, требующие защиты данных. Шифрование помогает компаниям соблюдать эти правила, минимизируя риски юридических последствий[1].

В современном мире, где информация становится одним из самых ценных ресурсов, вопросы безопасности передачи данных и оптимизации производительности сетей выходят на первый план. Защищенные локальные сети (ЗЛС) предлагают решение этих задач, обеспечивая не только высокий уровень защиты информации, но и улучшение её обработки. Одной из главных задач любой организации является защита корпоративных данных от несанкционированного доступа. ЗЛС используются для создания безопасного информационного пространства, где данные передаются через защищенные каналы. Основные механизмы защиты включают:

- Шифрование данных: Применение современных алгоритмов шифрования делает информацию недоступной для посторонних лиц. Даже в случае перехвата данных, без ключа шифрования они остаются бесполезными.
- Аутентификация пользователей: Использование многофакторной аутентификации и ограничение прав доступа помогает гарантировать, что только уполномоченные пользователи могут получить доступ к важной информации.
- Системы защиты от вторжений: Интеграция технологий обнаружения и предотвращения вторжений (IDS/IPS) позволяет сразу выявлять и блокировать подозрительную активность в сети.
- Файрволлы и VPN: Защита периметра сети с помощью файрволлов и создание виртуальных частных сетей (VPN) способствуют созданию дополнительного уровня безопасности и позволяют безопасно передавать данные между удаленными офисами и пользователями[6].

Кроме обеспечения безопасности, ЗЛС также способствуют повышению производительности организации. Их преимущества можно выделить следующим образом:

- Оптимизация трафика: Защищенные локальные сети позволяют использовать технологии управления трафиком, что снижает задержки и увеличивает скорость передачи данных. Это особенно важно для приложений в реальном времени, таких как видеоконференции и онлайн-совещания.
- Снижение нагрузки на серверы: Использование ЗЛС позволяет распределять нагрузки между несколькими серверами, что способствует более равномерному распределению ресурсов и увеличивает общую производительность системы.
- Улучшение качества обслуживания (QoS): Современные ЗЛС могут использовать механизмы QoS для приоритизации трафика, что позволяет минимизировать задержки критически важных приложений и сервисов.
- Локализация данных: Хранение и обработка данных в пределах защищенной сети позволяет существенно сократить время доступа к информации и снизить риск потери данных.

Таким образом, защищенные локальные сети передачи данных представляют собой эффективное средство обеспечения безопасности и конфиденциальности информации. Их использование позволяет повысить уровень защиты от киберугроз, обеспечить безопасное подключение к общественным сетям и увеличить производительность сети. Использование защищённых локальных сетей передачи данных — это не просто вопрос технологического прогресса, но необходимость в условиях современного информационного мира. Преимущества, такие как защита конфиденциальности, предотвращение несанкционированного доступа, повышение надёжности и соответствие законодательным требованиям, делают защищённые ЛС неотъемлемой частью инфраструктуры любой успешной организации. Инвестирование в безопасность локальных сетей не только защищает данные, но и создает стабильную основу для роста и развития бизнеса.

Список литературы

1. Визавитин, О. И. Применение современных алгоритмов шифрования при обеспечении информационной безопасности беспроводных локальных сетей / О. И. Визавитин, Д. А. Логинова, С. Д. Таякин. — Текст : непосредственный // Молодой ученый. — 2016. — №

- 10 (114). — С. 138-142. — URL: <https://moluch.ru/archive/114/29954/> (дата обращения: 21.11.2024).
2. Храмов Н.Р. ЗАЩИТА РЕСУРСОВ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VPN // Международный студенческий научный вестник. — 2019. — № 1. ; URL: <https://eduherald.ru/ru/article/view?id=19473> (дата обращения: 21.11.2024).
 3. Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК // Современные проблемы науки и образования. — 2014. — № 2. ; URL: <https://science-education.ru/ru/article/view?id=12875> (дата обращения: 21.11.2024).
 4. Кондратьев А.А., Тищенко И.П., Фраленко В.П. Разработка распределенной системы защиты облачных вычислений // Программные системы: теория и приложения : электрон. научн. журн. — 2011. — № 4 (8). — С. 61-70
 5. Морозов А. В., Шахов В. Г. Анализ атак на беспроводные компьютерные интерфейсы // Омский научный вестник. 2012. № 3 (113). С. 323-327.
 6. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. — 2015. — С. 193-197.

References

1. Vizavitin O. I., Loginova D. A., Tayakin S. D. Primenenie sovremennykh algoritmov kriptirovani pri obespecheniye informatsionnoy bezopasnosti wireless local networks [Application of modern encryption algorithms in ensuring information security of wireless local networks]. — Text : immediate // Young scientist. — 2016. — № 10 (114). — .pp. 138-142. URL: <https://moluch.ru/archive/114/29954/> (accessed: 21.11.2024).
 2. Khramov N.R. PROTECTION OF NETWORK RESOURCES BASED ON VPN TECHNOLOGY // International Student Scientific Bulletin. — 2019. — № 1. ; Available at: <https://eduherald.ru/ru/article/view?id=19473> (accessed: 21.11.2024).Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. — 2018.
 3. Kondratiev A.A., Talalaev A.A., Tishchenko I.P., Fralenko V.P., Khachumov V.M. METHODOLOGICAL SUPPORT OF INTELLIGENT SYSTEMS OF PROTECTION FROM NETWORK ATTACKS. — 2014. — № 2; Available at: <https://science-education.ru/ru/article/view?id=12875> (accessed: 21.11.2024).
 4. Kondratiev A.A., Tishchenko I.P., Fralenko V.P. Development of a distributed system for the protection of cloud computing. Scientific. Journ. — 2011. — № 4 (8). — pp. 61-70/
 5. Morozov A. V., Shakhov V. G. Analysis of attacks on wireless computer interfaces. 2012. № 3 (113). pp. 323-327.
 6. Andrianov V. I., Romanov G. G., Shterenberg S. I. Expert systems in the field of information security. — 2015. — pp. 193-197.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.736

МИНИМИЗАЦИЯ ВРЕМЕННЫХ ФАЙЛОВ ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ ИЗ БАЗЫ

Троян И.В.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
it.bonch@gmail.com

Временные файлы, создаваемые системами управления базами данных (СУБД), являются важной частью работы с запросами, но при неправильной настройке они могут стать источником утечки данных. В статье рассматриваются риски, связанные с временными файлами, такие как несанкционированный доступ и эксплуатация остаточных данных, а также предлагаются методы минимизации их использования, включая шифрование, ограничение прав доступа и оптимизацию запросов.

Ключевые слова: Временные файлы, утечка данных, базы данных, безопасность СУБД, шифрование, оптимизация запросов, минимизация рисков.

MINIMIZING TEMPORARY FILES TO PREVENT DATA LEAKS FROM DATABASES

Troyan I.V.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: it.bonch@gmail.com

Temporary files created by database management systems (DBMS) are an essential part of query processing, but when improperly managed, they can become a source of data leaks. This article explores the risks associated with temporary files, such as unauthorized access and residual data exploitation, and suggests methods to minimize their usage, including encryption, access control, and query optimization.

Keywords: Temporary files, data leaks, databases, DBMS security, encryption, query optimization, risk minimization.

Введение

Современные системы управления базами данных (СУБД) обрабатывают огромные объёмы данных, и временные файлы являются неотъемлемой частью этого процесса. Они используются для хранения промежуточных результатов выполнения сложных запросов, операций сортировки и индексации. Однако, несмотря на их важность, временные файлы могут стать уязвимым местом в системе безопасности базы данных. Остаточные данные, сохраняемые во временных файлах, часто остаются без должного внимания и защиты, что делает их привлекательной целью для злоумышленников.

Утечка данных из временных файлов может произойти через несанкционированный доступ к системам хранения, уязвимости операционной системы или даже через ошибки в конфигурации самой СУБД. Это особенно критично для организаций, работающих с конфиденциальной информацией, включая финансовые данные, персональные данные

пользователей или коммерческую тайну. Задача минимизации временных файлов заключается не только в их ограничении, но и в создании многоуровневой защиты, предотвращающей потенциальные утечки.

Минимизация временных файлов для предотвращения утечек данных из базы

Использование временных файлов в СУБД связано с необходимостью обеспечения высокой производительности при выполнении ресурсоёмких операций. Например, временные таблицы могут использоваться для хранения промежуточных данных при выполнении сложных SQL-запросов с объединением таблиц или при обработке больших объёмов данных. Однако каждая такая операция увеличивает риск утечки данных, если временные файлы не защищены должным образом[1].

Одной из основных проблем является сохранение остаточных данных во временных файлах. Даже после завершения запроса или удаления временного файла информация может оставаться в системе хранения в виде фрагментов, которые могут быть восстановлены злоумышленниками с помощью специальных инструментов. Это особенно опасно в условиях, когда диски, на которых хранятся временные файлы, недостаточно защищены или не используют механизмы шифрования[2].

Важным шагом к минимизации утечек данных через временные файлы является шифрование. Многие современные СУБД, такие как PostgreSQL, MySQL и Microsoft SQL Server, поддерживают шифрование временных файлов. Эта функция позволяет зашифровать данные на уровне хранения, делая их недоступными для несанкционированного доступа даже в случае компрометации системы. Однако шифрование не решает всех проблем — требуется также контроль за доступом к файлам[3].

Ограничение прав доступа играет ключевую роль в обеспечении безопасности временных файлов. Настройка системы таким образом, чтобы временные файлы были доступны только для процессов СУБД, предотвращает их просмотр и модификацию со стороны других приложений или пользователей. Помимо этого, важно использовать сегментацию сети, чтобы отделить сервер баз данных от других элементов инфраструктуры, минимизируя риск прямого доступа к файловой системе[4].

Ещё одним способом уменьшения зависимости от временных файлов является оптимизация SQL-запросов. Хорошо спроектированный запрос, например, с использованием индексов, может значительно сократить необходимость создания временных таблиц и файлов. Это не только повышает производительность системы, но и снижает вероятность утечки данных. Кроме того, администраторы баз данных могут настроить ограничение на размер временных файлов и их время хранения, чтобы уменьшить вероятность их использования злоумышленниками.

Не менее важен мониторинг работы системы. Инструменты для анализа активности файловой системы могут помочь обнаружить подозрительные действия, связанные с временными файлами, такие как их внезапное увеличение в объёме или попытки доступа со стороны непривилегированных процессов. В сочетании с журналированием событий в СУБД это позволяет администратору оперативно реагировать на возможные инциденты безопасности[5].

В современных условиях также стоит рассмотреть использование облачных решений, где временные файлы обрабатываются на виртуализированных и защищённых платформах.

Такие платформы часто предоставляют встроенные механизмы защиты, включая шифрование данных в режиме реального времени и автоматическое удаление временных файлов после завершения операций. Однако и здесь не стоит полагаться исключительно на поставщиков облачных услуг — необходимо проводить регулярные аудиты безопасности и следить за правильной настройкой системы

Заключение

Минимизация временных файлов и защита их содержимого являются важными аспектами управления безопасностью базы данных. Несмотря на то, что временные файлы играют важную роль в производительности СУБД, они остаются одной из наиболее уязвимых точек для утечки данных. Использование шифрования, настройка прав доступа, оптимизация запросов и мониторинг активности системы — всё это ключевые меры, которые помогают значительно снизить риск утечки через временные файлы.

С ростом объёмов данных и усложнением архитектуры современных систем управление безопасностью становится ещё более критичным. Органы, обрабатывающие конфиденциальную информацию, включая финансовые учреждения и медицинские организации, особенно уязвимы перед угрозами утечек. Поэтому внедрение лучших практик, таких как многоуровневая защита данных и регулярные аудиты безопасности, становится обязательным условием для предотвращения утечек через временные файлы.

Интеграция автоматизированных инструментов защиты и настройка политики безопасности позволяют создать надёжную защиту от современных угроз. В конечном итоге, эффективная защита временных файлов — это не только технический, но и организационный процесс, который требует постоянного внимания и обновления.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
3. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
 2. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.
 3. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 5. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 629.4.014.64

ПРОБЛЕМАТИКА ЭЛЕКТРОПИТАНИЯ ПАССАЖИРСКИХ ВАГОНОВ

¹Шульгинов П.А., ²Вахромов А.О., ³Чебаков С.А.

ФГБОУ ВО "УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ",
Екатеринбург, Россия (620034, Свердловская область, город Екатеринбург, ул. Колмогорова,
д. 66), e-mail: ¹pavel.shulginov55@gmail.com, ²arkadij392004@yandex.ru, ³SChebakov@usurt.ru

В статье рассматриваются проблемы электропитания пассажирских вагонов. Описываются преимущества и недостатки подвагонных генераторов пассажирских вагонов, а также их неисправности. Кроме того, в статье приведены схемы подвагонного генератора и обычного генератора постоянного тока. Анализируются недостатки методов электропитания, существующих на сегодняшний день, их последствия для проводника и пассажиров и возможные способы их решения, цель которых – повысить эффективность эксплуатации электрооборудования.

Ключевые слова: Пассажирский вагон, электрооборудование, генератор, вагон-электростанция, рекуперативное торможение, аккумуляторная батарея.

THE PROBLEM OF POWER SUPPLY FOR PASSENGER CARS

¹Shulginov P.A., ²Vakhromov A.O., ³Chebakov S.A.

URAL STATE UNIVERSITY OF RAILWAY ENGINEERING, Yekaterinburg, Russia (620034,
Sverdlovsk region, Yekaterinburg, Kolmogorova st., 66) e-mail: ¹pavel.shulginov55@gmail.com,
²arkadij392004@yandex.ru, ³SChebakov@usurt.ru

The article discusses the problems of power supply for passenger cars. The advantages and disadvantages of wagon generators of passenger cars, as well as their malfunctions, are described. In addition, the article provides diagrams of a wagon generator and a conventional DC generator. The disadvantages of current power supply methods are analyzed, their consequences for the conductor and passengers and possible ways to solve them, the purpose of which is to increase the efficiency of operation of electrical equipment.

Keywords: Passenger Car, electrical equipment, generator, power station car, regenerative braking, battery.

Проблемы и преимущества генераторов пассажирских вагонов

Все вагоны для перевозки пассажиров оснащены системой, которая обеспечивает их электроэнергией. В этих системах основными источниками электричества являются генераторы. В вагонах с автономной системой электроснабжения генераторы приводятся в движение от оси колёсной пары. В автономной системе электроснабжения для питания потребителей используется только постоянный ток. Это связано с тем, что на вагоне, помимо генератора, установлена аккумуляторная батарея. Она служит резервным и аварийным источником питания. В пассажирских вагонах используются генераторы не только постоянного, но и переменного тока. Во втором случае для подключения генератора к батарее требуется выпрямитель. Генераторы в системах с приводом от оси колёсной пары работают в условиях, которые отличаются от условий работы стационарных генераторов:

- частота вращения генератора и его напряжение меняются в зависимости от скорости движения поезда;
- при изменении направления движения вагона меняется полярность генератора постоянного тока;
- на низкой скорости мощность генератора снижается и не может обеспечить энергией всех потребителей.

Поэтому нужны генераторы со сложными системами автоматического регулирования, которые гарантируют получение электроэнергии надлежащего качества. [1]

Генератор пассажирского вагона состоит, как и любой генератор, из статора — неподвижной части генератора, состоящей из магнитопровода и обмотки возбуждения; ротора — вращающейся части генератора, в состав которой входит сердечник, обмотка возбуждения и полюсы; корпуса — внешнего корпуса генератора, предназначенного для защиты внутренних частей от внешних воздействий. Также у генератора имеется привод, соединяющий его с осью колёсной пары. В применяемых на железной дороге системах электроснабжения используют, в основном, следующие генераторы: постоянного тока с поперечным магнитным полем смешанного возбуждения; постоянного тока с продольным магнитным полем и параллельным возбуждением; индукционные генераторы переменного 3-фазного тока.

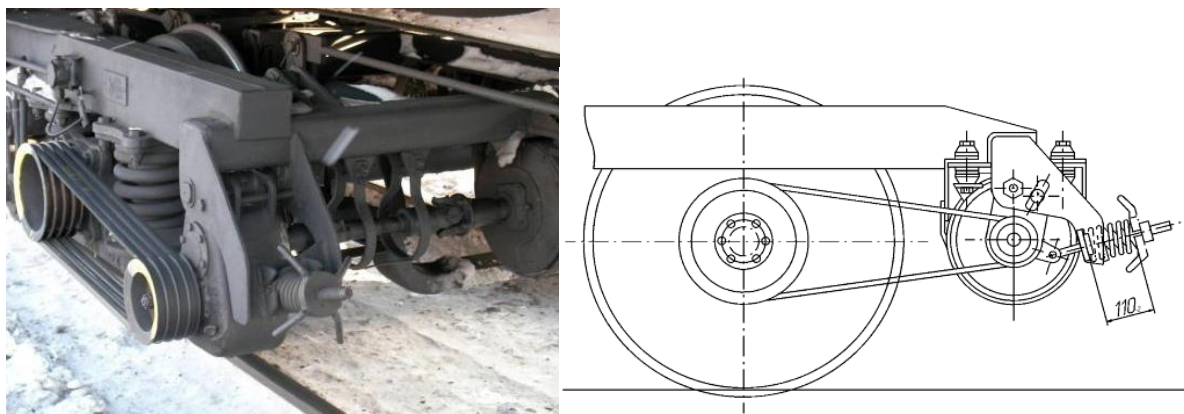


Рисунок 1 - Подвагонный генератор

Неисправности генераторов пассажирских вагонов

Наиболее частой причиной неисправностей генераторно-приводной установки пассажирского вагона является поломка карданного привода генератора. Генераторно-приводная установка (ГПУ) состоит из генератора, закреплённого на кузове вагона и карданного привода, соединяющего генератор с осью колёсной пары. В ходе эксплуатации выяснилось, что карданный привод имеет очень низкую надёжность и является слабым местом ГПУ. Как показывает статистика, около 1/3 всех поломок пассажирских вагонов приходится на ГПУ, причём почти половина из них — это разрушение карданного вала привода генератора. По причине данной неисправности весь вагон может остаться без электричества, а также это часто приводит к остановке поезда и, как следствие, задержкам. Чтобы избежать данных неисправностей, можно создать генератор, который будет располагаться на тележке вагона и вращаться непосредственно от оси колёсной пары, то есть без карданной передачи крутящего момента. В таком случае крутящий момент будет передаваться через напрессованный на ось фланец на эластичную муфту ГПУ, а далее на редуктор и через предохранительную муфту на

генератор. Данная конструкция поможет избежать не только частых поломок генератора, но и снизить передаваемые на вагон вибрации и шум, а также повысить рабочий диапазон скоростей генератора до 35–200 км/ч. [2]

Что касается диапазона скоростей, при которых генератор способен эффективно работать, то тут возникает следующий недостаток. При низкой скорости движения поезда, а также на стоянках генераторы вагонов не функционируют. В таком случае электроснабжение происходит от аккумуляторной батареи, но при этом освещение становится более тусклым, а батарея со временем разряжается. Решением данной проблемы может послужить вагон-электростанция, работающий на дизельном топливе. При наличии вагона-электростанции весь поезд обеспечивается электроэнергией и отоплением бесперебойно. Ещё одно преимущество применения вагона-электростанции заключается в том, что обычные низковольтные генераторы пассажирских вагонов сильно затрудняют тягу поезда, а если имеется вагон-электростанция, то такая проблема исчезает. Это играет очень важную роль для высокоскоростных поездов. [3]

У генераторов переменного тока в пассажирских вагонах существует недостаток, который заключается в отсутствии защиты от перегрева обмоток, возникающего из-за перегрузки генератора или неисправности автоматического регулирования возбуждения. Исправить данный недостаток генератора может позволить установка в статор генератора датчика температуры, выполненного в виде обмоток из медного провода определённого сопротивления. Эти обмотки будут проходить вдоль проводников силовых обмоток генератора и подключаться к вторичному прибору измерения температуры, который в свою очередь подсоединён к регулятору напряжений. Это позволит осуществить защиту обмоток генератора от перегрева, а также повысит надёжность устройства. [4]

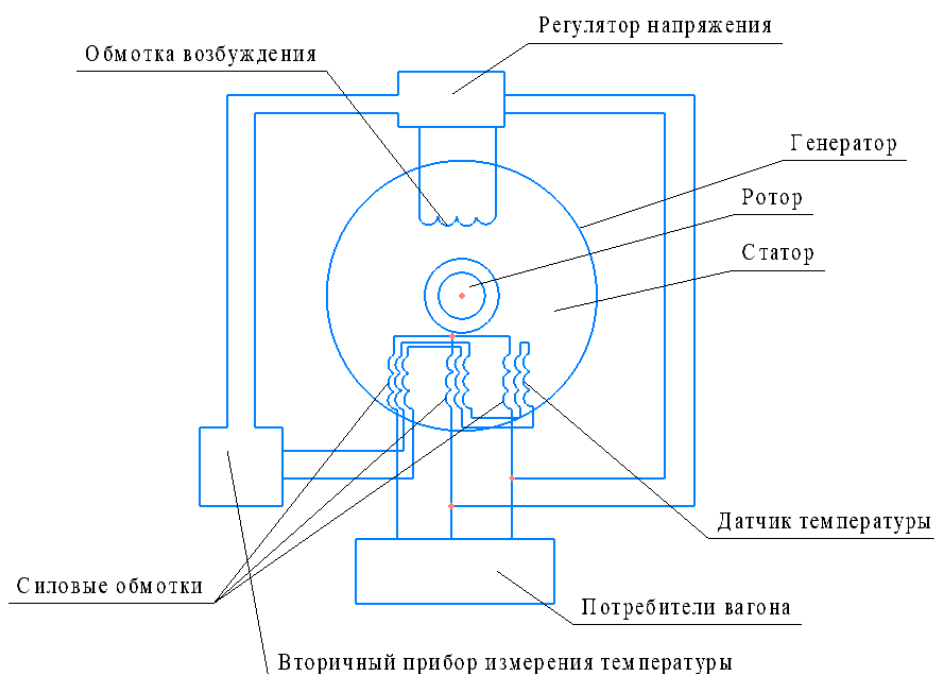


Рисунок 2 - Генератор постоянного тока

Преимущества и недостатки генераторов постоянного тока

К преимуществам можно отнести:

1. Простота конструкции
2. Может работать в сложных условиях
3. Эффективная производительность.

К недостаткам можно отнести:

1. Сложность конструкции
2. Малую надёжность
3. Необходимость частых ревизий
4. Высокую стоимость.
5. Ограниченный срок службы щеточно-коллекторного узла. [5]

Возможные методы решения проблем электропитания пассажирских вагонов

К сожалению, в пассажирских вагонах во время движения поезда нередко случаи выхода из строя систем жизнеобеспечения, а именно: освещения, биотуалетов (особенно вакуумного типа), кипятильников, отопления и самого уязвимого – установки кондиционирования воздуха. Причины таких случаев заключаются по большей части в том, что электроэнергии, запаасающейся в аккумуляторных батареях и вырабатываемой теми приборами, которые имеются на вагонах на сегодняшний день – подвагонными генераторами – недостаточно для непрерывной работы всех этих систем.

Приведём пример из практики проводника пассажирского вагона, работавшего летом на одном из рейсов южного направления. Пока поезд движется по перегону со скоростью более 40 км/ч, питание систем жизнеобеспечения вагона происходит за счёт вращения генератора, принимающего крутящий момент от колёсных пар. Все системы работают нормально. Однако по прибытии на станцию, где стоянка длится более 5 минут, отключается кондиционер и снова он включится, когда поезд разгонится до 40 км/ч. Пассажиры, очевидно, недовольны, но у проводника на это есть объяснение – установка кондиционирования воздуха пассажирского вагона (УКВ ПВ) потребляет электроэнергии намного больше, чем все остальные приборы, а генератор на стоянке электричество не вырабатывает. Следовательно, всё электрооборудование автоматически переходит на питание от аккумуляторной батареи, и если УКВ ПВ при таком питании оставить работающим, то батарея очень быстро разрядится и тогда в вагоне перестанет работать практически всё: остынет кипятильник, не включится кондиционер, выйдет из строя санузел, останется работать лишь аварийное освещение – вплоть до возвращения поезда в пункт формирования. Именно поэтому проводник ОБЯЗАН при стоянке дольше 5 минут отключать кондиционер, даже если стоянка техническая. Хотя, есть одно исключение из правил – допускается оставлять кондиционер работающим на длительной стоянке, пока напряжение в аккумуляторе не менее 100 В. Но такие случаи редки, а значит поиск решений по усовершенствованию электропитания вагона актуален.

Рассмотрим 2 варианта усовершенствования системы электропитания, их достоинства и недостатки:

1. Использование вагона-электростанции;
2. Использование рекуперативного торможения в качестве дополнительного источника питания вагонов.

1. Вагон-электростанция

Вагон-электростанция содержит кузов с машинным отделением, в котором установлены дизель-генераторы с оборудованием для подачи топлива, запуска и охлаждения, и

расположенные в одном из торцов кузова вагона служебное помещение и купе с туалетом для бригады обслуживания. [6]

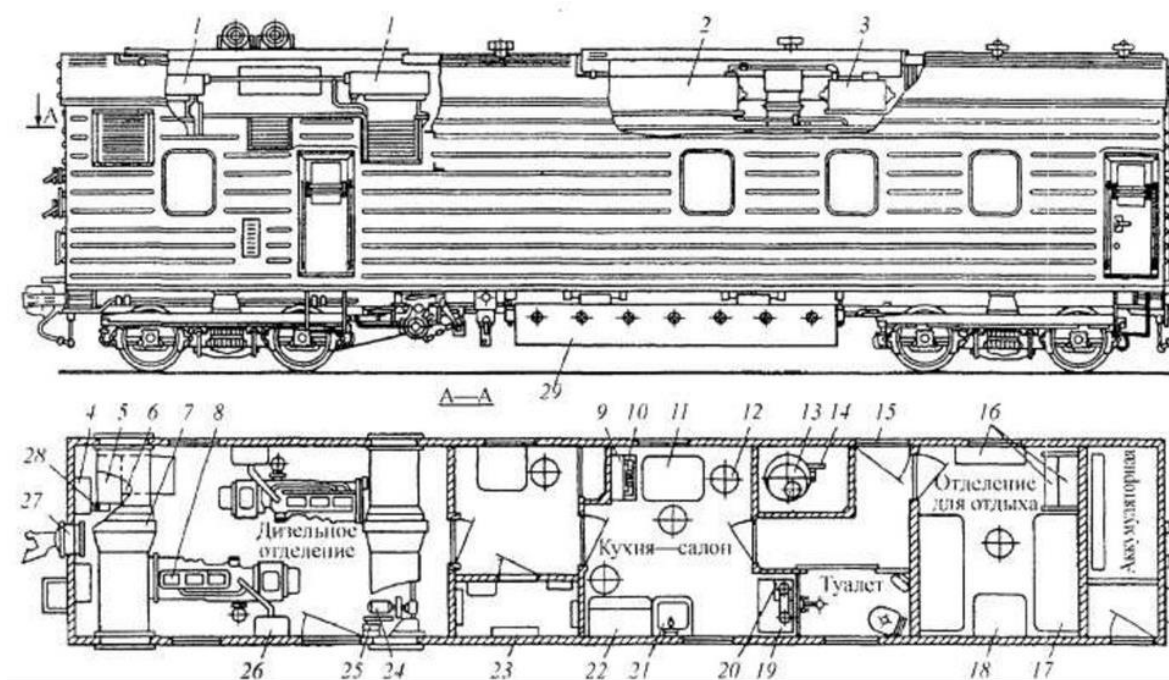


Рисунок 3 - Вагон-электростанция

Достоинства:

- Использование вагона-электростанции позволяет обеспечить полностью автономное электроснабжение пассажирского состава в том числе во время стоянки, когда подвагонный генератор не работает.
- Решается проблема эксплуатации во время длительных стоянок оборудования, требующего высоких энергозатрат (в частности УКВ ПВ), снижается нагрузка на подвагонный аккумулятор.

Недостатки:

- Вагон-электростанция намного тяжелее пассажирских вагонов, поэтому его добавление в состав потребует увеличения локомотивной тяги, в противном случае скорость движения уменьшится, что в свою очередь приведёт к массовым задержкам поездов.
- Обслуживание вагона-электростанции очень дорого: необходимо будет дополнительно оплачивать дизельное топливо для выработки электричества и работу бригады, обслуживающей такой вагон. Это негативно скажется на стоимости билетов.
- Вагон-электростанция занимает полезную длину станционного пути, что усложняет посадку-высадку пассажиров на малых станциях. Кроме того, для проводника головного вагона усложняется ещё и взаимодействие с локомотивной бригадой (например, машинист может не увидеть сигнал, подаваемый проводником).

2. *Использование рекуперативного торможения в качестве дополнительного источника питания вагонов.*

Рекуперативным торможением на железнодорожном транспорте называется процесс преобразования кинетической энергии движения поезда в электрическую энергию тяговыми электродвигателями (ТЭД), работающими в режиме генераторов. Эта энергия, как правило, возвращается в контактную сеть, либо же просто греет машинное отделение локомотива (всё равно, что тратится впустую). В этой статье предлагается следующий вариант: вся энергия, выработанная ТЭД в режиме генератора, уходит не в контактную сеть, а расходуется на зарядку аккумуляторных батарей. [7]

Достоинства:

- Появляется дополнительный источник энергии для зарядки аккумуляторов пассажирских вагонов.
- Такой способ расходования энергии, вырабатываемой ТЭД в режиме генератора, более эффективен, чем её возвращение в контактную сеть.
- Может применяться при движении поезда в режиме выбега в гористой местности.

Недостатки:

- В отличие от вагона-электростанции, этот метод не решает полностью проблему эксплуатации энергозатратного оборудования во время длительной стоянки.
- Реализация такого метода требует переоборудования тягового электродвигателя электровоза и аккумуляторов вагонов таким образом, чтобы можно было соединить их друг с другом – это довольно трудоёмкий процесс.

Заключение

Анализируя эти методы, приходим к выводу, что оба этих метода имеют место быть, однако на сегодняшний день применение вагона-электростанции более реально, чем использование рекуперативного торможения. Рекуперативное торможение, конечно, более экологичный вариант, чем вагон-электростанция, но пока ещё нет локомотивов с такими тяговыми электродвигателями, которые могут использовать энергию рекуперативного торможения для зарядки аккумуляторных батарей вагона.

Список литературы

1. Понкратов Ю. И. Электропривод и преобразователи подвижного состава: Учебник для техникумов и колледжей ж.-д. транспорта. – М.: ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2007. – 190 с.
2. Ведется разработка новой генераторно-приводной установки для пассажирских вагонов [Электронный ресурс]. URL: <https://dzen.ru/a/ZcUw4CfcYBZn0hbD> (дата обращения 16.11.2024)
3. И у любви у нашей не сядет батарейка. Красивое описание и неясная экономика: на сеть РЖД поставили очередной вагон-электростанцию [Электронный ресурс]. URL: <https://vgudok.com/lenta/i-u-lyubvi-u-nashey-ne-syadet-batareyka-krasivoe-opisanie-i-neyasnaya-ekonomika-na-set-rzhd> (дата обращения 16.11.2024)
4. RU5954U1 – Генератор пассажирского вагона [Электронный ресурс]. URL: https://yandex.ru/patents/doc/RU5954U1_19980216 (дата обращения 16.11.2024)
5. Плюсы и минусы генератора постоянного тока [Электронный ресурс]. URL: <https://plusiminusi.ru/plyusy-i-minusy-generatora-postoyannogo-toka/> (дата обращения 16.11.2024)

6. Вагон-электростанция [Электронный ресурс]. URL: <https://elibrary.ru/item.asp?id=38460813> (дата обращения 21.11.2024)
7. Рекуперативное торможение [Электронный ресурс]. URL: [https://ru.wikipedia.org/wiki/Рекуперативное_торможение#:~:text=Рекуперативное%20торможение%20\(от%20лат.%20recuperatio,или%20возвращается%20в%20электрическую%20сеть](https://ru.wikipedia.org/wiki/Рекуперативное_торможение#:~:text=Рекуперативное%20торможение%20(от%20лат.%20recuperatio,или%20возвращается%20в%20электрическую%20сеть) (дата обращения 21.11.2024).

References

1. Ponkratov Yu. I. Electric drive and converters of rolling stock: Textbook for technical schools and colleges of railway transport. – M.: State Educational Institution "Educational and methodological Center for education in railway transport", 2007. – 190 p.
 2. A new generator-drive unit for passenger cars is being developed [Electronic resource]. URL: <https://dzen.ru/a/ZcUw4CfcYBZn0hbD> (accessed 11/16/2024)
 3. And our love will not run out of battery. A beautiful description and an obscure economy: another power station wagon was installed on the Russian Railways network [Electronic resource]. URL: <https://vgudok.com/lenta/i-u-lyubvi-u-nashey-ne-syadet-batareyka-krasivoe-opisanie-i-neyasnaya-ekonomika-na-set-rzhd> (accessed 11/16/2024)
 4. RU5954U1 – Passenger car generator [Electronic resource]. URL: https://yandex.ru/patents/doc/RU5954U1_19980216 (accessed 11/16/2024)
 5. The pros and cons of a DC generator [Electronic resource]. URL: <https://plusminusi.ru/plyusy-i-minusy-generatora-postoyannogo-toka/> (accessed 11/16/2024)
 6. The power station wagon [Electronic resource]. URL: <https://elibrary.ru/item.asp?id=38460813> (accessed 11/21/2024)
 7. Regenerative braking [Electronic resource]. URL: [https://ru.wikipedia.org/wiki/Regenerative_inhibition#:~:text=Regenerative%20inhibition%20\(from%20\).%20recuperatio,or%20returns%20to%20electric%20grid](https://ru.wikipedia.org/wiki/Regenerative_inhibition#:~:text=Regenerative%20inhibition%20(from%20).%20recuperatio,or%20returns%20to%20electric%20grid) (accessed 11/21/2024).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 629.4.014.64

УВЕЛИЧЕНИЕ КОЭФФИЦИЕНТА ИЗВЛЕЧЕНИЯ КОНДЕНСАТА С ПОМОЩЬЮ САЙКЛИНГ-ПРОЦЕССА НА МЕСТОРОЖДЕНИЯХ ЗАПАДНОЙ СИБИРИ

¹Кабилов А.Н., ²Мытник Д.И., ³Катренко А.И., ⁴Мархиль М.В.

ФГБОУ ВО "ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ", Тюмень, Россия (625000, Тюменская область, город Тюмень, ул. Володарского, д. 38), e-mail: ¹aleksey.cabirov@yandex.ru, ²danamytnik9577@mail.ru, ³antonkatrenko72@gmail.com, ⁴mmarhil@mail.ru

Данная статья посвящена исследованию методов повышения коэффициента извлечения конденсата на газоконденсатных месторождениях Западной Сибири. Рассматривается эффективность применения сайклинг-процесса — технологии поддержания пластового давления с помощью обратной закачки сухого газа в продуктивный горизонт. Оценены перспективы этого метода для месторождений с высокой степенью неоднородности коллекторов и значительным содержанием конденсата в пластовом газе.

Ключевые слова: сайклинг-процесс, коэффициент извлечения конденсата, газоконденсатные месторождения, поддержание пластового давления, Западная Сибирь.

INCREASING THE CONDENSATE RECOVERY COEFFICIENT USING THE CYCLING PROCESS IN THE FIELDS OF WESTERN SIBERIA

¹Kabirov A.N., ²Mytnik D.I., ³Katrenko A.I., ⁴Markhil M.V.

TYUMEN INDUSTRIAL UNIVERSITY, Tyumen, Russia (625000, Tyumen Region, Tyumen, Volodarskogo St., 38), e-mail: ¹aleksey.cabirov@yandex.ru, ²danamytnik9577@mail.ru, ³antonkatrenko72@gmail.com, ⁴mmarhil@mail.ru

This article is devoted to the study of methods for increasing the condensate recovery coefficient at gas condensate fields in Western Siberia. The effectiveness of the cycling process, a technology for maintaining reservoir pressure by pumping dry gas back into a productive horizon, is considered. The prospects of this method for deposits with a high degree of reservoir heterogeneity and a significant condensate content in the reservoir gas are evaluated.

Keywords: Cycling process, condensate recovery coefficient, gas condensate deposits, reservoir pressure maintenance, Western Siberia.

Введение

В отечественной практике разработки газоконденсатных месторождений традиционно используется метод истощения пластовой энергии, что зачастую приводит к потерям значительных объемов углеводородного конденсата. Конденсат, растворенный в пластовом газе, при снижении давления выпадает из газовой фазы, осаждается в пласте и становится частично или полностью неподвижным. Для месторождений, содержащих значительное количество конденсата в пластовом газе, целесообразно применение технологий, направленных на поддержание пластового давления с целью увеличения коэффициента извлечения конденсата.

Основным методом поддержания пластового давления на нефтяных месторождениях является закачка воды. Однако для газоконденсатных месторождений с неоднородными по коллекторским свойствам пластами вода может вызывать потери газа и конденсата. Альтернативой является сайклинг-процесс — метод разработки, при котором газ закачивается обратно в пласт, что позволяет поддерживать давление и предотвращать потерю конденсата.

Сайклинг-процесс и его особенности

Сайклинг-процесс подразумевает обратную закачку газа в продуктивный горизонт для поддержания пластового давления. Это предотвращает конденсацию углеводородов при снижении давления, что позволяет избежать потерь конденсата. Полный и частичный сайклинг-процессы могут быть применены как на начальных этапах разработки месторождения, так и на более поздних стадиях, когда происходит истощение пластового давления. Однако, чем позже начинается процесс, тем ниже эффективность извлечения конденсата.

Результаты применения сайклинг-процесса

Примером успешного применения сайклинг-процесса является месторождение Ред-Хок в Мексиканском заливе, где в течение 8 лет поддерживалось пластовое давление с помощью закачки газа. [4] Глубина продуктивного горизонта на этом месторождении составляла 1955 м, с пористостью песчаника 22,2% и проницаемостью 0,52 мДа. За время закачки газа было возвращено 97% добытого сухого газа, что позволило избежать потери конденсата в пласте. Результатом этого процесса стало извлечение 88,8% первоначально содержащегося конденсата, при этом в последующий период разработки месторождения было извлечено еще 20,8% конденсата.[5]

Применение технологии сайклинга на месторождениях Западной Сибири

В Западной Сибири находится множество газоконденсатных месторождений, на которых возможно воспользоваться сайклинг-процессом для увеличения коэффициента извлечения конденсата. Примером такого месторождения является Юрхаровское, расположенное в Ямало-Ненецком автономном округе. Оно имеет свою специфику, так как большая часть его площади находится под акваторией Тазовской губы, что создает дополнительные сложности для освоения. [6] Одним из решений этой проблемы является строительство кустовой площадки в акватории и использование сайклинг-процесса через нагнетательные скважины, расположенные на искусственно отсыпном острове. Это позволит увеличить давление в пластах, находящихся под акваторией, и повысить конденсатоотдачу.

Рассмотрение возможности применения сайклинга также актуально для других месторождений Западной Сибири, таких как Восточно-Тамбейское и Северо-Обское, а также для месторождений, расположенных в Обской губе. [7] Анализ данных о проницаемости пластов и коэффициенте извлечения конденсата позволяет утверждать, что применение сайклинга в этих регионах может существенно повысить эффективность добычи.[8].

Заключение

Технология сайклинг-процесса имеет значительный потенциал для повышения коэффициента извлечения конденсата на месторождениях Западной Сибири. Применение данной технологии позволяет эффективно поддерживать пластовое давление, предотвращать потери конденсата и увеличивать зону дренирования, что особенно важно для месторождений с высоко неоднородными пластами и значительным содержанием конденсата в газе. Успешное применение сайклинга на примере месторождений Ла Глория и Юрхаровского демонстрирует высокую экономическую эффективность этого метода. Внедрение сайклинга на других месторождениях региона может стать важным шагом в увеличении извлечения углеводородного конденсата.

Список литературы

1. Tarek A. Reservoir engineering handbook. – London, UK: Elsevier Science & Technology, Gulf Professional Publ., 2010. – p. 1463
2. Al-Baqawi A.M., Al-Malki B.H. Well test analysis in naturally fractured gas condensate reservoirs below dew point pressure // Asia Pacific Oil and Gas Conference and Exhibition. – Jakarta: Society of Petroleum Engineers, 2009.
3. Siddiqui M.A.Q., Alnuaim S., Khan R.A. Well placement and rate optimization for gas cycling in gas condensate reservoirs // SPE Middle East Oil & Gas Show and Conference. – Manama, Bahrain: Society of Petroleum Engineers, 2015.
4. Закономерности истощения запасов нефти и газа в России и прогноз их воспроизводства / И.В. Филимонова, Л.В. Эдер, И.В. Проворная, А.В. Комарова // Экологический вестник России. – 2018. – № 4. – С. 4–12. 5. Current state and problems of integrated development of mineral resources base in Russia / I.V. Filimonova, L.V. Eder, M.V. Mishenin, T.M. Mamakhatov // IOP Conference Series: Earth and Environmental Science. – 2017. – V. 84. – № 1. – pp. 1–5.
5. Key problems in the development of the power of Siberia project / A.E. Kontorovich, L.V. Eder, I.V. Filimonova, S.M. Nikitenko // Regional Research of Russia. – 2018. – V. 8. – № 1. – P. 92–100.
6. Эдер Л.В., Проворная И.В., Филимонова И.В. Проблемы рационального использования попутного нефтяного газа в России // География и природные ресурсы. – 2019. – Т. 40. – № 1. – С. 9–14.
7. Sharf I., Tsibulnikova M., Dmitrieva N. Economic evaluation of the approaches to associated petroleum gas utilization // Ecology, Economics, Education and Legislation: Proc. 16th International multidisciplinary scientific geoconference (SGEM 2016). – Sofia: STEF92 Technology Ltd, 2016. – V. 2–5. – pp. 153–160.
8. PVTi and ECLIPSE 300. An Introduction to PVT analysis and compositional simulation. – Houston, USA: Schlumberger, Abingdon Technology Center Training 2005. – p. 402

References

1. Tarek A. Reservoir engineering handbook. – London, UK: Overview Science & Technology, Gulf Regional Publ., 2010. – p. 1463

2. Al-Baqawi A.M., Al-Malki B.H. Well test analysis in naturally fractured gas condensate reservoirs below dew point pressure // Asia Pacific Oil and Gas Conference and Exhibition. – Jakarta: Society of Petroleum Engineers, 2009.
 3. Siddiqui M.A.Q., Alnuaim S., Khan R.A. Well placement and rate optimization for gas cycling in gas condensate reservoirs // SPE Middle East Oil & Gas Show and Conference. – Manama, Bahrain: Society of Petroleum Engineers, 2015.
 4. Patterns of depletion of oil and gas reserves in Russia and the forecast of their reproduction / I.V. Filimonova, L.V. Eder, I.V. Nimornaya, A.V. Komarova // Ecological Bulletin of Russia. – 2018. – No. 4. – pp. 4-12.
 5. Current state and problems of integrated development of mineral resources base in Russia / I.V. Filimonova, L.V. Eder, M.V. Mishenin, T.M. Mamakhatov // IOP Conference Series: Earth and Environmental Science. – 2017. – V. 84. – No. 1. – pp. 1-5.
 5. Key problems in the development of the power of Siberia project / A.E. Kontorovich, L.V. Eder, I.V. Filimonova, S.M. Nikitenko // Regional Research of Russia. – 2018. – V. 8. – No. 1. – pp. 92-100.
 6. Eder L.V., Nimble I.V. Filimonova I.V. Problems of rational use of associated petroleum gas in Russia // Geography and natural Resources. – 2019. – Vol. 40. – No. 1. – pp. 9-14.
 7. Sharf I., Tsibulnikova M., Dmitrieva N. Economic evaluation of the approaches to associated petroleum gas utilization // Ecology, Economics, Education and Legislation: Proc. 16th International multidisciplinary scientific geoconference (SGEM 2016). Sofia: STEF92 Technology Ltd, 2016. V. 2-5. pp. 153-160.
 8. PVTi and ECLIPSE 300. An Introduction to PVT analysis and compositional simulation. – Houston, USA: Schlumberger, Abingdon Technology Center Training 2005. – p. 402
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 669.296

ИЗУЧЕНИЕ СТРУКТУРЫ ЦИРКОНИЯ В ЗАВИСИМОСТИ ОТ ОБРАБОТКИ

Го Кэнань

Цзилинский университет, Чанчунь, Китай (130012, КНР, провинция Цзилинь, Чанчунь, ул. Цяньцзинь, район Чаоян, 2699) e-mail: guokenan10@gmail.com

В работе исследуются вопросы подготовки образцов методом мокрого фрезерования, нанесения покрытий магнетронным напылением, определения структурных характеристик циркониевых сплавов и измерение нанотвердости для целей дальнейшего улучшения различных свойств материалов оболочек ядерных реакторов.

Ключевые слова: Циркониевые сплавы, нанотвердость, рентгеноструктурный анализ, металлографический анализ, мокрое шлифование.

STUDYING THE STRUCTURE OF ZIRCONIUM DEPENDING ON PROCESSING

Guo Henan

Jilin University, Changchun, China (130012, China, Jilin Province, Changchun, Qianjin Street, Chaoyang District, 2699) e-mail: guokenan10@gmail.com

The paper examines the issues of sample preparation by wet milling, magnetron sputtering coating, determination of structural characteristics of zirconium alloys and measurement of nanohardness for further improvement of various properties of nuclear reactor shell materials.

Keywords: Zirconium alloys, nanohardness, X-ray diffraction analysis, metallographic analysis, wet grinding.

Ядерная энергия - это высокоэффективный вид энергии, плотность которой более чем в несколько сотен раз превышает плотность энергии ископаемых. Атомная энергетика - одна из ключевых основ энергоснабжения и обеспечения национальной безопасности. Доля атомной энергетики в общем объеме мирового производства электроэнергии составляет 10,4 процента, и по состоянию на март 2019 года в 30 странах мира эксплуатируется 449 коммерческих ядерных энергетических реакторов общей установленной мощностью 396 ГВт, а в стадии строительства находится 55 ядерных энергоблоков, установленная мощность которых составляет 57 ГВт.[1,2] Ожидается, что по мере развития технологий ядерная энергия выйдет за рамки своей роли простого поставщика электроэнергии и будет использоваться в различных сферах, включая производство ядерного водорода, высокотемпературного технологического тепла, ядерного отопления и опреснения.[3]

Циркониевые сплавы обладают превосходным сочетанием свойств, при этом сечение поглощения тепловых нейтронов составляет всего $0,18 \times 10^{-28} \text{ м}^2$. Циркониевые сплавы Zircaloy-2, Zircaloy-4 и Zr-1Nb имеют сечение поглощения тепловых нейтронов всего $(0,20 - 0,24) \times 10^{-28} \text{ м}^2$. Они обладают хорошей коррозионной стойкостью к высокотемпературной воде и пару под высоким давлением при температуре $300^\circ\text{C} \sim 400^\circ\text{C}$, а

также хорошей стойкостью к нейтронному облучению внутри сваи. Кроме того, циркониевый сплав обладает такими преимуществами, как малый коэффициент теплового расширения, высокая теплопроводность, хорошая совместимость с ядерным топливом и легкость холодной обработки. Поэтому циркониевые сплавы широко используются в качестве материалов для корпусов ядерных реакторов.

В ядерных реакторах тепловыделяющая оболочка, являясь первым защитным барьером, не только заполняет активную зону ядерного топлива, но и поддерживает структурную целостность всей оболочки при передаче тепла для предотвращения утечки продуктов деления в ходе ядерной реакции, поэтому работоспособность тепловыделяющей оболочки напрямую влияет на безопасность эксплуатации ядерных реакторов.

Соответствующие исследования показали, что модификация поверхности оболочечных материалов из циркониевого сплава с помощью технологии напыления может значительно улучшить их характеристики безопасности при аварийном разрушении, метод напыления не требует изменения существующей ядерной системы, а используемая технология обработки оболочечных труб из циркониевого сплава становится все более совершенной, что имеет такие преимущества, как экономическая простота, короткий цикл исследований и разработок, легкость применения и т.д.

Исследованию подвергались пластинчатые образцы из сплава Э110 в различном состоянии. Образцы были облучены ионами на циклотроне тяжелых ионов ДЦ-60 до дозы 3 сна.

Образцы для исследований отрезали на станке «Accutom 5» (Рисунок 1а) фирмы «Struers» алмазным отрезным диском толщиной 0,5 мм и запрессовывали методом холодной заливки с применением эпоксидной смолы Specifix-40.



а



б

Рисунок 1 – Внешний вид прецизионного отрезного станка Accutom 5 (а) и шлифовально–полировального станка Tegra System

Исследование нанотвердости проводилось с использованием системы наноиндентирования Agilent G200 и лазерного конфокального микроскопа Olympus Lext OLS3000. Суть метода заключается в определении характеристик твердости при наноиндентировании на участках вблизи наружной поверхности с последующим построением зависимости твердость - удаленность от поверхности. Нагрузка при наноиндентировании была выбрана исходя из требуемой толщины отпечатка и составила (0,5-1) gf.

На Рисунке 2а представлено типичное изображение поверхности образца проведения одной серии испытаний, на рисунке 2б участок этого же образца в сопоставлении с расчетными координатами для индентирования.

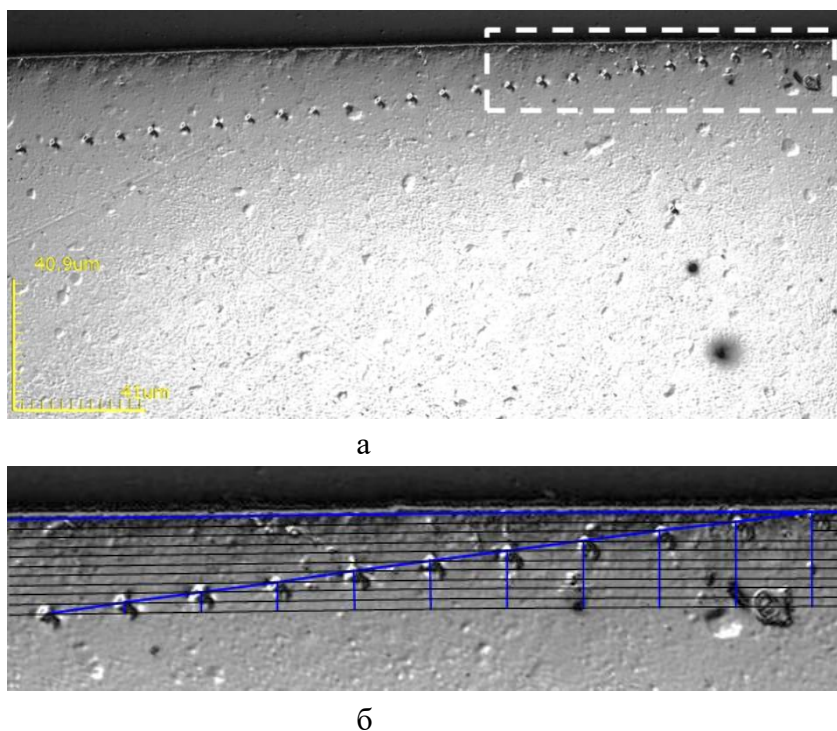


Рисунок 2 – Внешний вид поверхности образца после испытания по определению нагартованного слоя (а) и сопоставление расположения полученных отпечатков с расчетными координатами (б)

Точное расстояние полученных отпечатков от наружной поверхности образца определялось в программном обеспечении лазерного конфокального микроскопа Olympus Lext OLS3000 при увеличении $\times 2000$. Таким образом, проведение нескольких серий измерений позволяет с высокой точностью определять зависимость величины нанотвердости от расстояния от наружной поверхности.

Оценка структуры металлографическим и рентгеновским анализом и анализ механических свойств покрытия путем измерения нанотвердости сплава E110 с хромовым покрытием.

Например, четыре вещества, Zr-Nb, Zr-1%Nb+Cr, Zr-исх (обл.) и Zr+H (обл.), были проанализированы, и были получены следующие Рисунки 3-6.

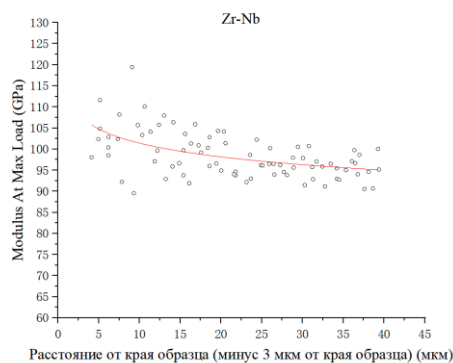


Рисунок 3- Максимальная нагрузка Zr-Nb в зависимости от расстояния от края образца

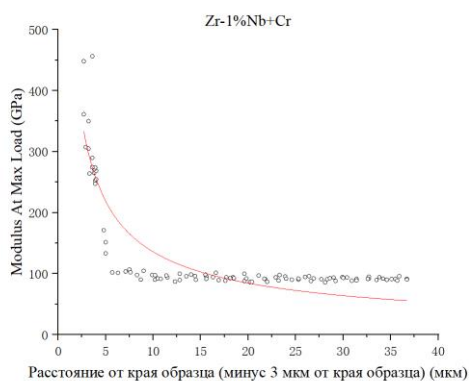


Рисунок 4-Максимальная нагрузка Zr-1%Nb+Cr в зависимости от расстояния от края образца

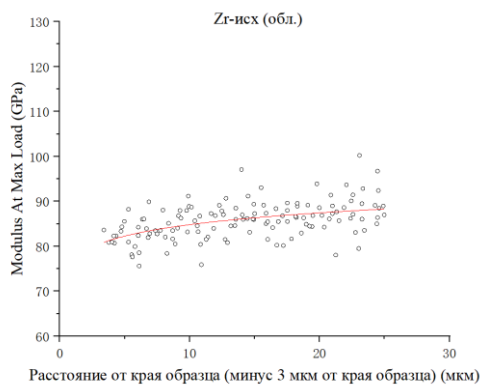


Рисунок 5-Максимальная нагрузка Zr-исх (обл.) в зависимости от расстояния от края образца

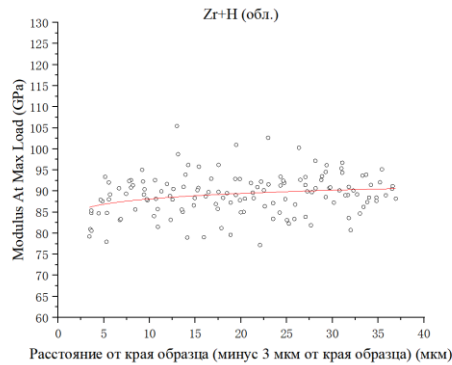


Рисунок 6-Максимальная нагрузка Zr-1%Nb+Cr (обл.) в зависимости от расстояния от края образца.

Во-первых, чтобы выяснить, разрушает ли процесс хромирования собственные свойства сплава e110 и образуются ли новые соединения, мы провели XRD-анализ сплавов Zr-1%Nb и Zr-1%Nb-Cr, соответственно, и получили Рисунок 7.

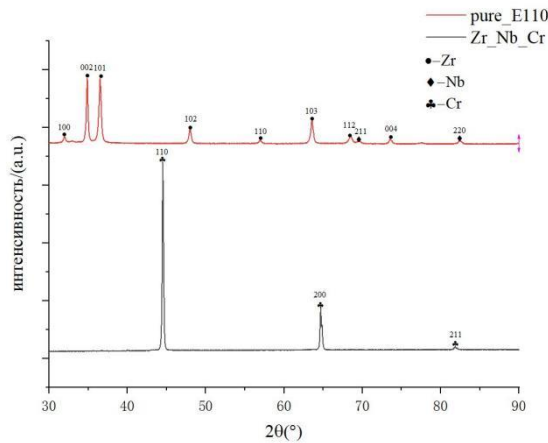


Рисунок. 7 - Сравнение дифрактограмм рентгеновских лучей Zr-Nb и Zr-Nb-Cr.

Таблица 1 – Результаты рентгеноструктурного анализа системы Zr1%Nb

Sample	Phase	Phase content, vol.%	Lattice parameters	Crystallite size according to CSR, nm	Microvoltage, Δd/d·10-3
Zr1%Nb	Zr	100	a: 3,2357 c: 5,1465	42	1,9
Zr1%Nb-Cr	Cr	100	a: 2,8869	54	0,4

По результатам РСА и данным, приведенным в Таблице 1, видно, что хромовое покрытие нанесено равномерно, и дополнительных фаз оксида хрома и оксида циркония не образуется.

Рентгеноструктурный анализ образца (Zr-Nb_исходный и Zr-Nb+Cr_исходный) проведён и получено изображение XRD. Добавление Cr изменяет положение пиков на изображении, поэтому хромовое покрытие может изменить способность циркониевого сплава рассеивать рентгеновские лучи.

При наноиндентировании твердость сплавов Zr-Nb медленно уменьшается с увеличением расстояния от края образца, а твердость сплавов Zr-Nb+Cr резко уменьшается с увеличением расстояния до 5 мкм от края образца, а затем медленно уменьшается, когда расстояние превышает 5 мкм. Твердость сплавов Zr-исх (обл.) и Zr-1%Nb+Cr (обл.) медленно увеличивается с увеличением расстояния от края образца.

Список литературы

1. МЭА. Статистика электроэнергетики.[2019-04-03].
2. МАГАТЭ. База данных по ядерным энергетическим реакторам.[2019-04-02].
3. МАГАТЭ. Неэлектрические области применения ядерной энергии: опреснение морской воды, производство водорода и другие промышленные применения. Oarai: МАГАТЭ, 2007.
4. 李佩志. 我国锆合金的研究现状 //稀有金属材料与工程. – 1993. – Т. 22. – №. 4. – С. 7-16.
5. 王旭峰 и др. 锆合金在核工业中的应用及研究进展 //热加工工艺. – 2012. – Т. 41. – №. 2. – С. 71-74.
6. Яманака С., Мияке М., Кацура М. Исследование растворимости водорода в циркониевых сплавах //Журнал ядерных материалов. – 1997. – Т. 247. – С. 315-321.
7. Уэплинг Д., Массих А. Р., Штоле П. Модель охрупчивания, вызванного гидридами, в сплавах на основе циркония //Журнал ядерных материалов. – 1997. – Т. 249. – №. 2-3. – С. 231-238.
8. Эклэнд Г. Дж. Охрупчивание и бистабильная кристаллическая структура гидрида циркония //Physical review letters. – 1998. – Т. 80. – №. 10. – С. 2233.
9. Вариас А. Г., Массих А. Р. Моделирование водородного охрупчивания циркониевых сплавов при напряжении и температурных градиентах //Журнал ядерных материалов. – 2000. – Т. 279. – №. 2-3. – С. 273-285.
10. Чжан Ю. и др. Путь образования гомогенного гидрида в α -Zr: моделирование молекулярной динамики с оптимизированным по заряду многочастичным потенциалом //Acta Materialia. – 2016. – Т. 111. – С. 357-365.

References

1. IEA. Electricity Statistics.[2019-04-03].
2. IAEA. The database on nuclear power reactors.[2019-04-02].
3. IAEA. Non-electric applications of nuclear power: Seawater desalination, hydrogen production and other industrial applications. Oarai: IAEA, 2007.
4. 李佩志. 我国锆合金的研究现状 //稀有金属材料与工程. – 1993. – Т. 22. – №. 4. – С. 7-16.
5. 王旭峰 et al. 锆合金在核工业中的应用及研究进展 //热加工工艺. – 2012. – Т. 41. – №. 2. – pp. 71-74.
6. Yamanaka S., Miyake M., Katsura M. Study on the hydrogen solubility in zirconium alloys

- //Journal of Nuclear Materials. – 1997. – Т. 247. – pp. 315-321.
7. Wäppling D., Massih A. R., Stähle P. A model for hydride-induced embrittlement in zirconium-based alloys //Journal of nuclear materials. – 1997. – Т. 249. – №. 2-3. – pp. 231-238.
 8. Ackland G. J. Embrittlement and the bistable crystal structure of zirconium hydride //Physical review letters. – 1998. – Т. 80. – №. 10. – pp. 2233.
 9. Varias A. G., Massih A. R. Simulation of hydrogen embrittlement in zirconium alloys under stress and temperature gradients //Journal of Nuclear Materials. – 2000. – Т. 279. – №. 2-3. – pp. 273-285.
 10. Zhang Y. et al. Homogeneous hydride formation path in α -Zr: Molecular dynamics simulations with the charge-optimized many-body potential //Acta Materialia. – 2016. – Т. 111. – pp. 357-365.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 614.84:51

ВЛИЯНИЕ МАТЕМАТИКИ НА ПОЖАРОТУШЕНИЕ

¹Ряпусов А.Р., Шпаньков А.В.

ФГБОУ ВО "УРАЛЬСКИЙ ИНСТИТУТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ", Екатеринбург, Россия (620062, Свердловская область, город Екатеринбург, ул. Мира, д.22), e-mail: ¹tolikry.990@gmail.com

В статье рассматривается влияние математических методов, расчетов на процессы пожаротушения, что становится особенно актуальным в условиях глобального изменения климата и увеличения числа природных и техногенных пожаров в России. Математика играет ключевую роль в оптимизации распределения ресурсов, прогнозировании возникновения пожаров и моделировании процессов горения. Использование статистических методов и алгоритмов позволяет значительно повысить эффективность работы служб экстренного реагирования, минимизируя время реакции и улучшая стратегии тушения. В статье также анализируются современные подходы к автоматизации принятия решений и оценке рисков, связанных с пожарами. Результаты исследования подчеркивают необходимость интеграции математических технологий в практику пожарной безопасности для повышения уровня защиты населения и окружающей среды.

Ключевые слова: Пожаротушение, математика, модели горения, прогнозирование, оптимизация ресурсов, алгоритмы принятия решений, оценка рисков, статистический анализ.

THE IMPACT OF MATHEMATICS ON FIREFIGHTING

¹Ryapusov A.R., Shpankov A.V.

URAL INSTITUTE OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS, Yekaterinburg, Russia (620062, Sverdlovsk Region, Yekaterinburg, Mira st., 22), e-mail: ¹tolikry.990@gmail.com

The article examines the influence of mathematical methods and calculations on fire extinguishing processes, which is becoming especially relevant in the context of global climate change and an increase in the number of natural and man-made fires in Russia. Mathematics plays a key role in optimizing the allocation of resources, predicting the occurrence of fires and modeling gorenje processes. The use of statistical methods and algorithms can significantly improve the efficiency of emergency response services, minimizing reaction time and improving extinguishing strategies. The article also analyzes modern approaches to automating decision-making and assessing fire-related risks. The results of the study emphasize the need to integrate mathematical technologies into the practice of fire safety in order to increase the level of protection of the population and the environment.

Keywords: Fire extinguishing, mathematics, combustion models, forecasting, resource optimization, decision-making algorithms, risk assessment, statistical analysis.

Изучение влияния математики на пожаротушение имеет ключевое значение для повышения эффективности работы Министерства по чрезвычайным ситуациям по нескольким причинам. Статистические методы и модели машинного обучения могут использоваться для анализа исторических данных и прогнозирования вероятности возникновения пожаров в

определенных условиях, что позволяет заранее принимать меры предосторожности. Статистические методы и модели машинного обучения могут использоваться для анализа исторических данных и прогнозирования вероятности возникновения пожаров в определенных условиях, что позволяет заранее принимать меры предосторожности. Модели горения помогают понять динамику распространения огня, что позволяет более точно предсказывать его поведение и разрабатывать стратегии тушения. Алгоритмы могут использоваться для автоматизации принятия решений в экстренных ситуациях, что сокращает время реакции и повышает точность действий. Изучение алгоритмов оптимизаций или маршрутизаций для перемещения пожарных машин, статистический анализ или расчеты с моделированием при помощи программного обеспечения для симуляции сценариев тушения с помощью математических моделей позволит не только повысить эффективность работы МЧС, но и улучшить общую безопасность населения и защиту окружающей среды от последствий пожаров [1].

Математическая модель для алгоритма распределения ресурсов при тушении пожара может быть построена на основе различных подходов, включая теорию графов, линейное программирование и методы оптимизации. Рассмотрим основные компоненты такой модели.

1. Ресурсы: обозначим количество доступных ресурсов (пожарные машины, бригады, оборудование) как $R = \{r_1, r_2, \dots, r_n\}$.

2. Очаги пожара: обозначим местоположение и интенсивность каждого очага пожара как $F = \{f_1, f_2, \dots, f_m\}$, где f_i характеризуется координатами и уровнем угрозы.

3. Расстояния: расстояние между ресурсами и очагами можно обозначить как $d(r_i, f_j)$.

Целью модели может быть минимизация общего времени реакции или максимизация эффективности тушения. Например, целевая функция может выглядеть так:

$$T = \sum_{i=1}^n \sum_{j=1}^m x_{ij} \cdot d(r_i, f_j),$$

где x_{ij} — бинарная переменная, принимающая значение 1, если ресурс r_i назначен для тушения очага f_j , и 0 в противном случае. Так же введем ограничения по доступным ресурсам - сумма ресурсов, назначенных для тушения всех очагов, не должна превышать доступное количество ресурсов:

$$\sum_{j=1}^m x_{ij} \leq 1,$$

Потребности очагов: каждый очаг должен быть охвачен определенным количеством ресурсов в зависимости от его интенсивности:

$$\sum_{i=1}^n x_{ij} \geq p_j,$$

где p_j — минимальное количество ресурсов, необходимых для тушения очага f_j . Время, необходимое для достижения очага, не должно превышать заданного предела. Для решения данной модели можно использовать линейное программирование, если все функции и ограничения линейны. Либо методы целочисленного программирования, для случаев, когда ресурсы должны быть распределены в целых числах. После разработки модели ее можно интегрировать в системы управления экстренными службами. Модель будет использоваться для прогнозирования возникновения новых очагов пожара на основе исторических данных, оптимизации маршрутов передвижения ресурсов, оценки рисков и принятия решений в реальном времени [2].

Компьютерное моделирование может сыграть ключевую роль в разработке математической модели алгоритма распределения ресурсов при тушении пожара, обеспечивая более эффективное и оперативное реагирование на чрезвычайные ситуации. В первую

очередь, важно создать модель, которая учитывает множество переменных, связанных с распространением огня, такими как тип местности, погодные условия, наличие растительности и материалов, а также инфраструктуру в зоне пожара. Для этого можно использовать методы численного моделирования, которые позволят предсказать, как огонь будет распространяться в зависимости от этих факторов. Кроме того, важно проводить симуляции различных сценариев развития пожара. Это позволит оценить влияние изменений в погодных условиях или в структуре местности на поведение огня и на необходимость перераспределения ресурсов. Например, если ожидается изменение направления ветра, модель может пересчитать оптимальные маршруты и количество необходимых ресурсов для тушения в новых условиях [3]. Анализ исторических данных о пожарах также может быть интегрирован в модель. Используя методы машинного обучения, можно выявить паттерны и предсказать вероятность возникновения новых очагов возгорания в определенных районах. Это даст возможность заранее планировать распределение ресурсов и повышать готовность служб к потенциальным угрозам. Интерактивные карты, созданные на основе модели, могут визуализировать текущее состояние пожара и расположение доступных ресурсов. Это позволит оперативно принимать решения в реальном времени, а также улучшить координацию между различными командами и службами.

Таким образом, математика проявляется в алгоритме распределения ресурсов при тушении пожара через формализацию проблемы, создание целевых функций и ограничений, а также применение методов оптимизации для нахождения наилучших решений. Это позволяет значительно повысить эффективность реагирования на чрезвычайные ситуации и минимизировать ущерб от пожаров. Применение математических подходов, таких как дифференциальные уравнения для моделирования распространения огня, статистические методы для анализа данных о пожарах и оптимизационные алгоритмы для планирования ресурсов, позволяет более точно предсказывать поведение огня и разрабатывать стратегии его тушения. Кроме того, использование математических моделей способствует улучшению подготовки пожарных служб, позволяя им принимать обоснованные решения на основе количественных данных. Это, в свою очередь, может снизить риски для жизни и здоровья людей, а также минимизировать материальные потери от пожаров. Интеграция математических методов в практику пожаротушения не только способствует более эффективному реагированию на чрезвычайные ситуации, но и открывает новые горизонты для научных исследований в области пожарной безопасности. Рекомендуется продолжать развивать и внедрять математические модели в практику, что позволит значительно повысить уровень защиты от пожаров и улучшить качество жизни в населенных пунктах.

Список литературы

1. Приложение к Приказу МЧС России от 30.06.2009 № 382 «Методика определения расчетных величин пожарного риска в зданиях, сооружениях и строениях различных классов функциональной пожарной опасности».
2. Приказ МЧС России от 16 октября 2017 г. N 444 «Об утверждении Боевого устава подразделений пожарной охраны, определяющего порядок организации тушения пожаров и проведения аварийно-спасательных работ».
3. Приказ МЧС РФ от 30 июня 2009 г. N 382 «Об утверждении методики определения расчетных величин пожарного риска в зданиях, сооружениях и строениях различных классов функциональной пожарной опасности» Прил. N 6. Порядок проведения расчета и

математические модели для определения времени блокирования путей эвакуации опасными факторами пожара»

4. Н.Ю. Клименти «Методики расчета сил и средств для тушения пожаров» 2013 г., 27 с.
5. Л.Ю. Катаева, М.Н. Ильичева, А.А. Лошилов Научная статья «Математическое моделирование тушения лесного пожара путем доставки воды в его очаг с помощью капсул с термически активной оболочкой». 2020 г.

References

1. . Appendix to the Order of the Ministry of Emergency Situations of Russia dated 30.06.2009 No. 382 "Methodology for determining the calculated values of fire risk in buildings, structures and constructions of various classes of functional fire hazard".
 2. Order of the Ministry of Emergency Situations of Russia dated October 16, 2017 No. 444 "On approval of the Combat Regulations of fire protection units, determining the procedure for organizing fire extinguishing and conducting emergency rescue operations".
 3. Order of the Ministry of Emergency Situations of the Russian Federation of June 30, 2009 N 382 "On approval of the methodology for determining the calculated values of fire risk in buildings, structures and structures of various classes of functional fire hazard" Appendix N 6. Procedure for carrying out calculations and mathematical models for determining the time of blocking evacuation routes by hazardous fire factors"
 4. N. Yu. Klimenti "Methodologies for calculating the forces and means for extinguishing fires" 2013, p.27
 5. L. Yu. Kataeva, M. N. Ilyicheva, A. A. Loshchilov Scientific article "Mathematical modeling of extinguishing a forest fire by delivering water to its source using capsules with a thermally active shell". 2020
-