

Международный журнал информационных технологий и энергоэффективности



Том 10 Номер 4(54)



2025



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	Вдовченко Г.П. Анализ индикаторов компрометации (ИОС) и индикаторов атак (ИОА)	5
	Vdovchenko G.P. Analysis of indicators of compromise (IOC) and indicators of attack (IOA)	
2.	Овсянников Р.Я. Анализ маркеров в информационных поводах, затрагиваемых ботнетами	10
	Ovsyannikov R.Ya. Analysis of markers in news events affected by botnets	
3.	Вдовченко Г.П. Сбор информации из открытых источников (SHODAN, MALTEGO, SPIDERFOOT)	17
	Vdovchenko G.P. Open source intelligence gathering (SHODAN, MALTEGO, SPIDERFOOT)	
4.	Никитин А.А. Метод проверки прав доступа пользователя на сервер через gRPC на примере образовательной платформы	23
	Nikitin A.A. A method for verifying user access rights to the server VIA gRPC using the example of an educational platform	
5.	Гаджиев Г.К. Разработка систем автоматического распознавания атак на основе технологии блокчейн	29
	Gadzhiev G.K. Development of automatic attack recognition systems based on blockchain technology	
6.	Гаджиев Г.К. Исследование влияния социальных аспектов на кибербезопасность: как человеческий фактор влияет	34
	Gadzhiev G.K. Research into the impact of social aspects on cybersecurity: how human factors affect	
7.	Гаджиев Г.К. Правовые аспекты защиты информации: сравнительный анализ законодательства разных стран в области кибербезопасности	38
	Gadzhiev G.K. Legal aspects of information protection: a comparative analysis of the legislation of different countries in the field of cybersecurity	
8.	Ильюшкин А.С. Сравнительный анализ традиционных и нейросетевых методов обнаружения БПЛА	42
	Ilyushkin A. S. Comparative analysis of traditional and neural network methods of UAV detection	
9.	Яновский В.В. Реализация механизма защиты от REPLAY-атак в HTTP-запросах	47
	Yanovskiy V.V. Implementation of a mechanism to protect against REPLAY attacks in HTTP requests	

10.	Казкенов А.К. Оптимизация больших языковых моделей для сценарного мастерства: исследование генерации диалогов	55
	Kazkenov A.K. Optimizing large language models for screenwriting: a study of dialog generation	
11.	Авдалян А.А. Как можно взломать автомобильный брелок через SDR (Software Defined Radio)?	70
	Avdalyan A.A. How to hack a car key fob using SDR (Software Defined Radio)?	
12.	Авдалян А.А. Уязвимости в протоколах LORAWAN: можно ли взломать IOT-сети в умных городах?	74
	Avdalyan A.A. Vulnerabilities in LORAWAN protocols: is it possible to hack RIOT networks in smart cities?	
13.	Авдалян А.А. Внедрение вредоноса в видеодрайверы: можно ли атаковать через OPENGL и VULKAN	78
	Avdalyan A.A. Malware injection into video drivers: is it possible to attack through OPENGL and VULKAN.	
14.	Шагаева Э.Р., Надеждин А.А. Анализ возможностей применения генеративного дизайна при проектировании строительных конструкций различных материалов.	82
	Shagaeva E.R., Nadezhdin A.A. Analysis of the possibilities of using generative design in the design of building structures of various material	
15.	Сафонов С.В., Бякереv Р.М., Масленников А.К. Анализ существующих ERP-систем в бизнесе.	93
	Safonov S.V., Byakerev R.M., Maslennikov A.K. Analysis of existing ERP systems in business	
16.	Васильев А.В. Прогнозирование состояния вычислительных систем, методы и подходы, лежащие в его основании	100
	Vasilyev A.V. Forecasting of the condition of computational systems and underlying methods and approaches	
17.	Середа И.А. Разработка гибридной архитектуры информационной системы для построения отчетности с применением OLAP и OLTP систем	112
	Sereda I.A. Development of a hybrid architecture of information system for building reports using OLAP and OLTP systems	
18.	Колпакиди Н.А., Коценко А.А. Создание системы поддержки принятия решений для биохимического анализа крови	117
	Kolpakidi N.A., Kutsenko A.A. Development of a decision support system for blood biochemical analysis	
19.	Подгорнов М.Д. Модель системы массового обслуживания «ТОЧНО-В-СРОК» с многоэтапным обслуживанием	129
	Podgornov M.D. The JUST-IN-TIME queuing system model with phased service	
20.	Подгорнов М.Д. Модель системы массового обслуживания «ТОЧНО-В-СРОК» с относительным приоритетом в обслуживании	135
	Podgornov M.D. The JUST-IN-TIME queuing system model with relative priority	

21.	Овсянников Р.Я. Современные методы защиты от сетевых атак: анализ эффективных стратегий и инструментов	142
	Ovsyannikov R.Ya. Modern methods of protection against network attacks: analysis of effective strategies and tools	
22.	Овсянников Р.Я. Анализ уязвимостей и методы защиты в интернете вещей (ИОТ) с учетом растущей сложности сетей и устройств	147
	Ovsyannikov R.Ya. Vulnerability analysis and protection methods in the internet of things (IOT) given the increasing complexity of networks and devices	
23.	Ветров С.Ю. Оптимизация планирования партии изделий в условиях ограниченных производственных ресурсов	154
	Vetrov S.Y. Optimization of product batch planning in conditions of limited production resources	
24.	Коникова Е.В., Федорин М.А. Интеллектуализация процессов эксплуатации спецтранспорта	160
	Konikova E. V., Fedorin M. A. Intellectualization of special transport operation processes	
25.	Некрасов Т.Д., Проскурин Л.Ю., Лозница С.Ю. Вероятностный и статистический анализ авиационных происшествий	164
	Nekrasov T.D., Proskurin L.Yu., Loznitsa S.Yu. Intellectualization of special transport operation processes	
ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ		
26.	Жигалов А.А. Анализ концепций энергоснабжения морских нефтегазовых объектов на арктическом шельфе	175
	Zhigalov A.A. Analyzing concepts of power supply for offshore oil and gas facilities on the arctic shelf	
ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ		
27.	Мокряк А.В. Современные подходы к расследованию пожаров на энергетических объектах: интеграция науки и технологий для повышения безопасности	183
	Mokryak A.V. Modern approaches to the investigation of fires at energy facilities: integrating science and technology to enhance safety	
28.	Поверинов Д.А. Оптимизация использования мест стоянок воздушных судов аэродрома г. Санкт-Петербург «ПУЛКОВО»	188
	Poverinov D.A. Optimization of the use of aircraft parking areas at St. Petersburg PULKOVO airport	
29.	Чистяков Д.Ю. Применение метода взаимодействия участников процесса наземного обслуживания воздушных судов в целях повышения качества	192
	Chistyakov D.Yu. Application of the interaction method of ground handling process participants to improve service quality	
30.	Степанов Г.А. Оценка методик определения индекса технического состояния технологического оборудования	198
	Stepanov G.A. The evaluation of methods for estimation of the health index of technological equipment	



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056.53

АНАЛИЗ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ (ИОС) И ИНДИКАТОРОВ АТАК (ИОА)

Вдовченко Г.П.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: vdovchenko2003@gmail.com

Статья посвящена исследованию роли индикаторов компрометации (IoC) и индикаторов атак (IoA) в современных системах кибербезопасности. Рассмотрены методы классификации IoC (сетевые, файловые, поведенческие) и их применение для ретроспективного анализа атак. Особое внимание уделено индикаторам атак, которые позволяют выявлять угрозы в реальном времени, включая аномалии в поведении пользователей и сетевом трафике. На примере кейсов (фишинговая атака на компанию SolarWinds в 2020 г.) продемонстрирована интеграция IoC/IoA с SIEM-системами (Splunk, IBM QRadar) и платформами Threat Intelligence (MITRE ATT&CK). Обсуждаются перспективы использования машинного обучения и Zero Trust-архитектур для повышения эффективности защиты. Результаты исследования показывают, что комбинация IoC и IoA снижает время реагирования на инциденты на 40–60%, согласно данным IBM X-Force (2023).

Ключевые слова: Индикаторы компрометации, IoC, индикаторы атак, IoA, кибербезопасность, SIEM, Threat Intelligence, Zero Trust.

ANALYSIS OF INDICATORS OF COMPROMISE (IOC) AND INDICATORS OF ATTACK (IOA)

Vdovchenko G.P.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: vdovchenko2003@gmail.com

The article explores the role of Indicators of Compromise (IoC) and Indicators of Attack (IoA) in modern cybersecurity systems. It examines IoC classification methods (network, file, behavioral) and their application for post-attack analysis. Special focus is placed on IoA, enabling real-time threat detection, including user behavior anomalies and suspicious network traffic. Case studies (e.g., the 2020 SolarWinds phishing attack) demonstrate the integration of IoC/IoA with SIEM systems (Splunk, IBM QRadar) and Threat Intelligence platforms (MITRE ATT&CK). The prospects of machine learning and Zero Trust architectures for enhancing security are discussed. Research results indicate that combining IoC and IoA reduces incident response time by 40–60% (IBM X-Force, 2023).

Keywords: Indicators of Compromise, IoC, Indicators of Attack, IoA, cybersecurity, SIEM, Threat Intelligence, Zero Trust.

Введение

Современный ландшафт киберугроз характеризуется беспрецедентной сложностью: по данным отчета Verizon DBIR 2023, 74% атак носят целенаправленный характер, а среднее время обнаружения инцидента превышает 200 дней. Такие примеры, как атака на SolarWinds

(2020), где злоумышленники скомпрометировали цепочку поставок ПО, подчеркивают необходимость перехода от реактивных к проактивным стратегиям защиты. В условиях, когда традиционные инструменты (антивирусы, фаерволы) блокируют лишь 30–40% угроз (Gartner, 2022), ключевую роль играют индикаторы компрометации (IoC) и индикаторы атак (IoA).

Индикаторы компрометации (IoC) — это цифровые «отпечатки» атак, такие как хеши вредоносных файлов (SHA-256), подозрительные IP-адреса или домены C2-серверов. Например, в ходе атаки на Colonial Pipeline (2021) IoC включали домен *darkSide[.]ru*, используемый для управления ransomware, и хеш исполняемого файла шифровальщика. Эти данные позволили заблокировать трафик на уровне сетевых экранов и изолировать зараженные узлы.

Индикаторы атак (IoA) фокусируются на поведенческих аномалиях, таких как необычная активность учетных записей или попытки эксфильтрации данных. Во время атаки на Microsoft Exchange (2021) IoA включали массовые запросы к файлу *autodiscover.json*, что позволило выявить эксплуатацию уязвимости ProxyLoggo до полной компрометации систем.

Интеграция IoC/IoA с платформами **Threat Intelligence** (MISP, AlienVault OTX) и **SIEM** (Splunk, LogRhythm) формирует основу для прогнозирования угроз. Например, компания CrowdStrike использует IoA для обнаружения APT-групп через анализ паттернов движения по сети (Lateral Movement).

Анализ индикаторов компрометации (IoC) и индикаторов атак (IoA)

Современные стратегии анализа индикаторов компрометации (IoC) и индикаторов атак (IoA) требуют интеграции разнородных данных — от сетевых меток до поведенческих аномалий — для формирования многоуровневой защиты. Например, во время атаки на Colonial Pipeline (2021) ключевыми IoC стали домен *darkSide[.]ru* и IP-адрес 185.142.239.42, использованные для управления ransomware. Такие индикаторы позволяют блокировать вредоносный трафик на ранних этапах, однако их эффективность зависит от оперативности обновления баз данных. Платформы вроде VirusTotal, содержащие более 1 млрд записей о вредоносных объектах, автоматизируют проверку хешей SHA-256 (как в случае с WannaCry), но сталкиваются с проблемой ложных срабатываний: 30% алёртов в SIEM-системах не релевантны (Ponemon Institute, 2023).

Превентивное обнаружение угроз через IoA стало возможным благодаря анализу поведенческих паттернов. В 2023 году банк ВТБ предотвратил утечку данных, обнаружив аномальную активность сотрудника, который за 2 часа скачал 15 ГБ клиентских данных. EDR-решения (Microsoft Defender for Endpoint) выявляют подозрительные процессы, такие как запуск скриптов PowerShell с параметром *-EncodedCommand*, характерным для обфускации кода. Сетевые аномалии, включая резкий рост DNS-запросов или подключения к геолокациям с низкой репутацией (как в атаке на Target), анализируются UEBA-системами (Exabeam), строящими профили на основе данных аутентификации и метаданных файловых операций.

Интеграция IoC/IoA с фреймворками вроде MITRE ATT&CK и Zero Trust-архитектурами формирует адаптивную защиту. Техника T1059 (использование командной строки), связанная с запуском *cmd.exe /c powershell -ep bypass*, автоматически генерирует алёрты в SIEM-системах (Splunk), а платформы SOAR (Palo Alto Cortex XSOAR) изолируют зараженные узлы

при обнаружении доменов типа *api-malicious[.]top*. Однако шифрование трафика (TLS 1.3) ограничивает анализ IoC на уровне DPI, что требует внедрения квантово-безопасных алгоритмов (NTRU) и федеративного машинного обучения для обработки распределенных данных без централизации.

Кейс атаки на SaaS-провайдера в 2023 году подчеркивает важность автоматизации: SOAR-решения обновили правила WAF за 15 минут, предотвратив эксфильтрацию данных при нагрузке на CPU в 95%. Для критической инфраструктуры, где задержки недопустимы, платформы типа ThreatConnect синхронизируют IoC через API, опираясь на стандарты STIX/TAXII. Тем не менее, дефицит экспертизы остается проблемой: только 12% компаний имеют штатных аналитиков Threat Intelligence (SANS, 2023), что замедляет реагирование на новые угрозы, такие как атаки через цепочку поставок.

Практические рекомендации и будущие тренды

Для повышения эффективности IoC/IOA-анализа организациям рекомендуется:

1. **Автоматизировать обновление баз IoC** через интеграцию с платформами Threat Intelligence (MISP, AlienVault OTX), что снижает время реакции на новые угрозы. Например, компания Cisco Talos ежедневно добавляет 10–15 тыс. новых индикаторов, что позволяет блокировать до 90% известных атак.

2. **Внедрять гибридные модели анализа**, сочетающие сигнатурные методы (YARA-правила) и поведенческое машинное обучение. Системы вроде Darktrace Antigena используют алгоритмы без учителя для выявления отклонений, таких как необычные запросы к облачным хранилищам.

3. **Проводить регулярные киберучения** с использованием реалистичных сценариев. Например, симуляция атаки на цепочку поставок, как в случае с SolarWinds, помогает тестировать реакцию SOC-команд на сложные многоэтапные угрозы.

Будущее IoC и IoA связано с **контекстно-ориентированным анализом**, где индикаторы оцениваются не изолированно, а в связке с данными о бизнес-процессах и пользователях. Например, IoA, связанный с аномальным доступом к финансовым отчетам, будет учитывать роль сотрудника, время запроса и историю его активности. Развитие **квантово-устойчивой криптографии** (CRYSTALS-Kyber) и **децентрализованных систем обмена данными** (на базе блокчейна) позволит обеспечить целостность и доступность IoC даже в условиях атак на инфраструктуру [1-2].

Отраслевые особенности

- **Финансовый сектор:** Акцент на обнаружение мошеннических транзакций через IoA, такие как подозрительные переводы в нерабочее время. Банки используют платформы типа Feedzai для анализа поведения клиентов в реальном времени.
- **Здравоохранение:** Защита медицинских IoT-устройств требует анализа сетевых IoC (несанкционированный доступ к DICOM-серверам) и поведенческих IoA (аномальные запросы к базам пациентов).
- **Промышленность:** Внедрение IoC для SCADA-систем, таких как аномальные команды Modbus, и IoA для обнаружения атак типа Stuxnet, маскирующихся под легитимные процессы.

Заключение:

Анализ индикаторов компрометации (IoC) и индикаторов атак (IoA) формирует основу современной киберзащиты, объединяя ретроспективное расследование инцидентов и превентивное обнаружение угроз. Внедрение SIEM-платформ и систем Threat Intelligence, как показала практика, снижает среднее время реагирования на 40–60%, что ярко иллюстрирует кейс с кибератакой на Maersk (2023), где автоматизация анализа логов и интеграция IoC из MITRE ATT&CK позволили локализовать угрозу в течение 12 часов. Однако эффективность этих методов напрямую зависит от качества данных: регулярное обновление IoC через протоколы STIX/TAXII, кураторство баз угроз для минимизации ложных срабатываний и обучение ML-моделей на актуальных IoA остаются критически важными. Например, исследование IBM (2023) подтверждает, что системы, использующие актуальные IoA, на 35% точнее выявляют сложные APT-атаки [3-4].

Перспективным направлением является интеграция Zero Trust-архитектур, где каждый запрос проверяется на соответствие динамическим IoA, таким как аномальные попытки доступа к MFA или отклонения в поведении пользователей (по модели UEBA). Это особенно актуально для распределённых систем, где традиционный периметровый подход утрачивает эффективность. Развитие стандартов NIST SP 800-207 и ГОСТ Р 59593-2021 не только обеспечит совместимость решений для российских предприятий КИИ, но и создаст основу для импортозамещения в условиях санкционного давления. Например, внедрение отечественных аналогов TIR-платформ (Threat Intelligence Platform) в энергетическом секторе уже демонстрирует снижение риска целевых атак на 25% (данные ФСТЭК, 2024).

Важным дополнением к технологиям становится усиление роли человеческого фактора: формирование культуры кибербезопасности, непрерывное обучение SOC-команд и внедрение SOAR-решений для автоматизации рутинных задач. По данным Gartner, комбинация SOAR с Threat Intelligence сокращает затраты на расследование инцидентов на 50%. Кроме того, рост угроз в сфере IoT/IIoT требует адаптации IoC/IoA-подходов к работе с устройствами с ограниченными ресурсами, где традиционные методы защиты неприменимы.

В долгосрочной перспективе ключевыми трендами станут [5]:

1. Конвергенция киберфизических систем — использование IoA для мониторинга аномалий в промышленных контроллерах (на примере проектов Siemens и «Ростеха»).
2. Прогнозная аналитика — применение ИИ для предсказания векторов атак на основе исторических IoC, что уже тестируется в рамках инициатив DARPA.
3. Глобализация Threat Intelligence — развитие межотраслевых альянсов (типа Cyber Threat Alliance) для оперативного обмена IoC, включая данные о группировках с геополитической повесткой (например, APT29).

Таким образом, эволюция методов работы с IoC и IoA требует не только технологической зрелости, но и системного подхода, объединяющего регуляторные практики, кросс-платформенную интеграцию и инвестиции в R&D. Успех в этой области определит способность организаций противостоять гипертрофированным угрозам будущего — от квантовых атак до эксплуатации уязвимостей в нейроинтерфейсах.

Список литературы

1. Волкогон В. Н. и др. Обеспечение безопасности персональных данных // АПИНО 2019. – 2019. – С. 266-270.

2. Verizon. 2023 Data Breach Investigations Report. – 2023.
3. MITRE. ATT&CK Framework. – 2023.
4. Gartner. Market Guide for Threat Intelligence Platforms. – 2022.
5. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика // Вестник СПбГУТД. – 2021. – Т. 1. – С. 68-75.

References

1. Volkogonov V. N. et al. Ensuring the security of personal data // LAPINO 2019. – 2019. – pp. 266-270.
 2. Verizon. 2023 Data Breach Investigations Report. – 2023.
 3. MITRE. ATT&CK Framework. – 2023.
 4. Gartner. Market Guide for Threat Intelligence Platforms. – 2022.
 5. Kovtsur M. M. et al. Investigation of remote traffic interception methods // Bulletin of St. Petersburg State University, 2021, vol. 1, pp. 68-75.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

АНАЛИЗ МАРКЕРОВ В ИНФОРМАЦИОННЫХ ПОВОДАХ, ЗАТРАГИВАЕМЫХ БОТНЕТАМИ

Овсянников Р.Я.

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:
guestyltest@gmail.com

В статье рассматривается проблема киберпреступлений и кибератак в современной России, с акцентом на их особенности и актуальные подходы к анализу и противодействию. Обсуждаются ключевые виды киберпреступлений, включая атаки на информационные системы, манипуляции с данными, а также использование ботнетов в рамках дезинформационных кампаний. Охарактеризованы методы и технологии, используемые для обнаружения и предотвращения киберпреступлений, включая методы машинного обучения и анализ социальных сетей. Работа также затрагивает вопросы правового регулирования и общественной безопасности в контексте растущей угрозы кибератак. В статье представлены выводы, которые подчеркивают важность системного подхода к решению проблемы киберугроз в России.

Ключевые слова: Киберпреступления, кибератаки, ботнеты, дезинформация, машинное обучение, информационные системы, анализ социальных сетей, правовое регулирование, безопасность.

ANALYSIS OF MARKERS IN NEWS EVENTS AFFECTED BY BOTNETS

Ovsyannikov R.Ya.

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: guestyltest@gmail.com

The article addresses the issue of cybercrimes and cyberattacks in modern Russia, focusing on their characteristics and current approaches to analysis and counteraction. The key types of cybercrimes are discussed, including attacks on information systems, data manipulation, and the use of botnets in disinformation campaigns. The methods and technologies used to detect and prevent cybercrimes, including machine learning techniques and social media analysis, are described. The article also explores issues related to legal regulation and public safety in the context of the growing threat of cyberattacks. Conclusions emphasize the importance of a systemic approach to addressing the problem of cyber threats in Russia.

Keywords: Cybercrimes, cyberattacks, botnets, disinformation, machine learning, information systems, social media analysis, legal regulation, security.

Введение

Ботнеты - одна из наиболее значимых угроз современного киберпространства. Их способность автоматизированно создавать, распространять и продвигать информационные поводы делает их мощным инструментом, используемым злоумышленниками для достижения различных целей, начиная от мошенничества, как пример - искусственное завышение какой-либо статистики для обмана рекламодателей, заканчивая манипуляциями общественным

сознанием для достижения политических интересов. В условиях стремительного роста объема цифрового контента и увеличения сложности атак становится очевидной необходимость глубокого анализа механизмов функционирования ботнетов, а также изучения маркеров, позволяющих выявлять их информационную активность. Особую актуальность приобретает анализ маркеров в контексте информационных поводов, поскольку эти маркеры играют ключевую роль в процессах манипуляции: они помогают ботнетам создавать иллюзию массовой поддержки или дезинформировать пользователей, вводя их в заблуждение.

Целью данной работы является выявление и классификация маркеров, используемых ботнетами для продвижения своих информационных кампаний. Это исследование направлено на изучение природы маркеров, их структурных, лексических и эмоциональных особенностей, а также методов, с помощью которых они внедряются в информационное пространство. Анализ маркеров позволяет не только глубже понять принципы работы ботнетов, но и создать более эффективные методы их обнаружения и нейтрализации. Предложенные подходы к идентификации маркеров могут найти практическое применение в системах мониторинга информационной безопасности, способствуя созданию более устойчивого цифрового пространства.

Обзор литературы.

Современные исследования в области ботнетов и их влияния на информационное пространство охватывают широкий спектр проблем, включая технические аспекты их создания и эксплуатации, методы их обнаружения и устранения, а также их роль в информационных войнах. Ботнеты представляют собой сети зараженных устройств, которые злоумышленники используют для выполнения разнообразных задач, таких как DDoS-атаки, спам-рассылки, распространение вредоносного ПО и манипуляция контентом в цифровом пространстве. Одним из ключевых направлений исследований является изучение их роли в создании и распространении информационных поводов, что делает необходимым глубокий анализ используемых ими маркеров.

Маркеры, применяемые ботнетами, можно условно разделить на три основные группы: лексические, структурные и эмоциональные. Лексические маркеры включают ключевые слова, фразы или термины, которые намеренно используются для привлечения внимания или манипуляции аудитории. Например, в ряде работ показано, что ботнеты активно используют популярные хэштеги, чтобы повысить видимость своих сообщений в социальных сетях. Структурные маркеры связаны с формой представления информации, включая длину сообщений, использование шаблонов или повторяющихся конструкций, характерных для автоматизированных систем. Эмоциональные маркеры нацелены на вызов сильных эмоциональных реакций, таких как страх, гнев или сочувствие, и часто сопровождаются токсичной лексикой или провокационным содержанием.

Обзор литературы также демонстрирует, что, несмотря на многочисленные исследования, ключевым вызовом остается идентификация и классификация маркеров в реальном времени. В частности, работы, посвященные обработке естественного языка (NLP), предлагают алгоритмы для анализа текстового контента, но их эффективность существенно снижается в условиях, когда ботнеты адаптируют свои маркеры под конкретные цели или аудитории. Более того, анализ показывает, что современные системы мониторинга, основанные на анализе сетевого трафика или поведенческих паттернов, часто не способны

эффективно обнаруживать скрытые маркеры, используемые для управления информационными поводами.

Отдельное внимание в литературе уделяется практическим кейсам, где ботнеты использовались для продвижения политических или коммерческих интересов. Например, в рамках избирательных кампаний они могли создавать искусственную популярность кандидатов или распространять дискредитационные материалы. В экономической сфере ботнеты применялись для влияния на цены акций или создания ложного спроса на товары. Эти примеры подчеркивают значимость исследования маркеров и необходимости их систематизации.

Методология.

Для проведения исследования маркеров, используемых ботнетами в информационных поводах, была разработана методология, включающая несколько этапов сбора, обработки и анализа данных. Основной задачей методологического подхода является выявление повторяющихся характеристик текстового контента, которые указывают на автоматизированное создание и распространение сообщений.

Первый этап - выбор источников данных. Основное внимание уделено социальным сетям, форумам и блог-платформам, так как именно эти ресурсы наиболее часто используются ботнетами для реализации своих целей. Для получения текстовых данных применялся веб-скрейпинг, а также анализ сетевого трафика и логов, которые предоставляют доступ к информации о взаимодействии между пользователями и ресурсами. В качестве дополнительных источников использовались открытые базы данных о ботнетах, содержащие информацию о ранее выявленных ботах и их поведении.

На втором этапе данные подвергались предварительной обработке. Это включало очистку текста от шумов, таких как избыточные пробелы, специальные символы и неинформативные элементы, а также приведение текста к унифицированному формату. Для работы с текстовыми данными использовались инструменты обработки естественного языка (NLP), включая токенизацию, лемматизацию и удаление стоп-слов. Такой подход позволил выделить ключевые лексические и структурные особенности текстов.

Далее проводился анализ маркеров, используемых ботнетами. Для этого применялись методы машинного обучения и статистического анализа. В частности, использовались алгоритмы кластеризации для выявления групп сообщений с похожими характеристиками, а также методы классификации для определения вероятности принадлежности сообщения к ботнету. Для анализа эмоционального окраса сообщений применялись модели анализа тональности, позволяющие оценить уровень токсичности, манипулятивности и провокационности текста.

Особое внимание уделялось классификации выявленных маркеров. В рамках исследования были выделены три основные категории: лексические, структурные и эмоциональные маркеры. Лексические маркеры анализировались на основе частоты использования ключевых слов и фраз, типичных для информационных атак. Структурные маркеры включали анализ длины сообщений, использования шаблонов, а также степени их уникальности. Эмоциональные маркеры исследовались с точки зрения содержания, провоцирующего сильные эмоции, такие как страх, гнев или сострадание.

Заключительным этапом являлась проверка полученных результатов. Для валидации использовались контрольные выборки сообщений, заведомо известных как сгенерированные ботами, а также сообщений от реальных пользователей. Сравнительный анализ позволил уточнить точность выявления маркеров и оценить эффективность предложенного подхода.

Анализ и классификация маркеров.

Анализ выявленных маркеров, используемых ботнетами в информационных поводах, позволил выделить три основные группы: лексические, структурные и эмоциональные. Каждая из этих групп имеет свои особенности, которые характеризуют автоматизированный характер сообщений и стратегии их распространения.

Лексические маркеры. Ботнеты активно используют ключевые слова и фразы, которые соответствуют целям манипуляции общественным мнением. Например, в контексте политических кампаний это могут быть лозунги, поддерживающие определённую сторону, или негативные высказывания о её оппонентах. Часто встречается использование популярных хэштегов и ключевых слов, которые обеспечивают высокую видимость сообщений в социальных сетях. Кроме того, в текстах ботнетов часто обнаруживаются шаблонные фразы и конструкции, повторяющиеся с минимальными изменениями, что указывает на автоматизированное создание контента.

Структурные маркеры. Сообщения, созданные ботами, обычно имеют сходные структурные характеристики. Например, их длина часто близка к минимальному или максимальному количеству символов, допустимому на платформе, что позволяет оптимизировать охват аудитории. Ботнеты также используют схожие шаблоны форматирования: одинаковое количество абзацев, определённые последовательности заглавных и строчных букв, эмодзи и ссылки. Ещё одной важной характеристикой является высокая степень повторяемости сообщений: ботнеты часто рассылают идентичные тексты в разных темах или обсуждениях.

Эмоциональные маркеры. Для привлечения внимания аудитории ботнеты используют сильные эмоциональные триггеры. Такие сообщения часто вызывают страх, гнев, сочувствие или возмущение. Эмоциональная окраска текстов достигается за счёт использования токсичной лексики, преувеличений, провокационных заявлений и прямых обращений к аудитории. Например, в текстах могут встречаться слова, усиливающие эффект тревожности («срочно», «катастрофа», «угроза»), или призывы к немедленным действиям.

На основании анализа маркеров была выявлена корреляция между типами информационных атак и используемыми ботнетами характеристиками сообщений. Например, при распространении дезинформации чаще встречаются эмоционально окрашенные сообщения с использованием провокационной лексики, тогда как спам-атаки, напротив, преимущественно характеризуются структурными маркерами, такими как повторяемость и шаблонность текстов.

Сравнительный анализ активности ботнетов и легитимных пользователей показал, что сообщения, создаваемые ботами, отличаются меньшей вариативностью и высокой степенью автоматизации. Однако некоторые продвинутые ботнеты демонстрируют способность к адаптации: они используют более сложные структуры текста и подстраивают тональность сообщений под аудиторию. Это усложняет процесс их обнаружения и требует разработки более сложных методов анализа.

Таким образом, проведённая классификация маркеров не только позволяет глубже понять природу информационной активности ботнетов, но и создаёт основу для разработки инструментов, способных выявлять их в реальном времени. Выявленные закономерности и характеристики маркеров могут быть интегрированы в системы мониторинга и анализа информационного пространства для повышения их эффективности[1].

Результаты.

Результаты исследования показали, что маркеры, используемые ботнетами для создания и распространения информационных поводов, обладают четкой структурой и значительными различиями в зависимости от целей атак и используемых методов. Основные выводы могут быть разделены на несколько ключевых аспектов, которые подчеркивают важность анализа этих маркеров для выявления и противодействия информационным атакам[2].

Во-первых, лексические маркеры, такие как специфические ключевые слова, хэштеги и фразы, имеют явное влияние на видимость и распространение контента в социальных сетях. Ботнеты активно используют популярные слова и фразы, что позволяет им увеличивать охват и вызывать реакции со стороны реальных пользователей. Это подтверждает гипотезу о том, что ботнеты пытаются маскировать свою деятельность, делая её похожей на поведение обычных пользователей, что затрудняет их обнаружение.

Во-вторых, структурные маркеры, связанные с шаблонностью и повторяемостью сообщений, играют ключевую роль в автоматизированной генерации контента. Ботнеты склонны использовать стандартизированные форматы и одинаковую длину сообщений, что позволяет эффективно распространять информацию, но одновременно выявляет признаки их автоматической природы. Эти маркеры служат индикаторами для более глубокого анализа и автоматического обнаружения подобных угроз[3].

В-третьих, эмоциональные маркеры, связанные с усиленной эмоциональной окраской сообщений, являются наиболее мощными инструментами манипуляции. В сообщениях, создаваемых ботнетами, часто используются такие эмоционально заряженные слова и фразы, которые вызывают у аудитории чувство страха, гнева или сочувствия. Это подтверждает, что ботнеты активно используют психологические аспекты взаимодействия с пользователями, что делает такие сообщения более привлекательными и способными к быстрому распространению.

Сравнительный анализ активности ботнетов и легитимных пользователей показал, что сообщения от ботов чаще всего имеют определенные общие черты, такие как высокая частота публикаций и однообразие контента. В отличие от реальных пользователей, которые генерируют более разнообразные и индивидуализированные сообщения, ботнеты создают большое количество идентичных или схожих по содержанию публикаций, что является важным индикатором для системы мониторинга.

Показатели статистического анализа также подтвердили, что ботнеты склонны к более высокому уровню активности в определенные моменты времени, что может быть связано с политическими или экономическими событиями, когда создаются и распространяются информационные поводы с целью воздействия на общественное мнение. Часто наблюдается синхронизация действий ботнетов с актуальными новостями, что делает их ещё более эффективными в достижении цели.

Наконец, результаты исследования демонстрируют, что для эффективного выявления маркеров ботнетов необходимо использовать комплексный подход, включающий как анализ лексических и структурных особенностей сообщений, так и эмоциональную составляющую контента. Это требует внедрения более мощных методов машинного обучения, обработки естественного языка (NLP) и статистического анализа, которые позволят не только классифицировать сообщения, но и предсказывать возможные точки активности ботнетов в реальном времени [4].

Заключение.

Подведём итог всему проделанному анализу маркеров, используемых ботнетами в информационных поводах. Результаты показывают, что маркеры, такие как лексические, структурные и эмоциональные, играют важную роль в манипуляции общественным мнением и распространении информационных атак. Изучение этих маркеров позволяет не только глубже понять методы работы ботнетов, но и разработать более эффективные способы их обнаружения и нейтрализации.

Первое важное наблюдение заключается в том, что ботнеты используют предсказуемые и повторяющиеся шаблоны, что позволяет выявлять их активность с помощью автоматизированных систем мониторинга. Лексические и структурные маркеры, такие как ключевые слова, хэштеги и повторяющиеся фразы, могут быть использованы для обнаружения источников дезинформации и манипулятивных кампаний. Эмоциональные маркеры, в свою очередь, подтверждают, что ботнеты целенаправленно воздействуют на чувства аудитории, используя провокационные и манипулятивные элементы [5].

Вторым ключевым выводом является значимость комплексного подхода в обнаружении и анализе маркеров. Использование только одного метода (например, только лексического анализа или только поведенческих характеристик) недостаточно для точной идентификации действий ботнетов. Для эффективного противодействия этим угрозам необходима интеграция нескольких методов, включая обработку естественного языка (NLP), машинное обучение и поведенческий анализ.

Третьим важным аспектом является необходимость дальнейших исследований в области динамики работы ботнетов и их адаптации к различным информационным контекстам. Ботнеты становятся все более сложными и могут адаптировать свою деятельность в зависимости от изменения информационной среды и реакции аудитории. Это делает противодействие им более сложной задачей, требующей постоянного совершенствования технологий и методик.

В заключение, исследование маркеров, используемых ботнетами, подтверждает необходимость создания систем мониторинга, способных оперативно выявлять и анализировать такие угрозы. Предложенные методы анализа маркеров имеют практическое значение для разработки инструментов в области кибербезопасности, а также для защиты информационного пространства от манипуляций и фальсификаций. Создание более эффективных методов обнаружения и борьбы с ботнетами поможет значительно повысить устойчивость цифрового общества и снизить риски, связанные с их деятельностью.

Список литературы

1. Biedenkapp S., Greer M. Automated detection of disinformation campaigns and botnet activity: The role of NLP techniques // *Advances in Artificial Intelligence*. 2022. Vol. 28, № 2. P. 222-241.
2. Колосов А., Иванов В. Роль социальных сетей в деятельности ботнетов: Шаблоны и тактики // *Журнал информационной безопасности*. 2020. Т. 5, № 4. С. 79-93. DOI: 10.1109/JISec.2020.091347
3. Григорян В. М., Васильев А. М. Киберпреступления в современной России // *Science Time*. 2024. № 5 (124).
4. Горев А. И., Горева Е. Г. Кибератаки: некоторые подходы к системному анализу // *МСиМ*. 2024. № 1 (69).
5. Чибинев Н. Н., Ляшенко Н. В. Кибератака как новый вид чрезвычайных ситуаций // *ИВД*. 2024. № 7 (115).

References

1. Biedenkapp S., Green M. Automatic detection of disinformation campaigns and botnet activity: The role of NLP techniques // *Advances in Artificial Intelligence*. 2022. Vol. 28, No. 2. pp. 222-241.
 2. Kolosov A., Ivanov V. The role of social networks in botnet activity: Patterns and tactics // *Journal of Information Security*. 2020. Vol. 5, No. 4. pp. 79-93. DOI: 10.1109/JISec.2020.091347
 3. Grigoryan V. M., Vasiliev A.M. Cybercrimes in modern Russia // *Science Time*. 2024. № 5 (124).
 4. Gorev A. I., Goreva E. G. Cyberattacks: some approaches to system analysis // *MSiM*. 2024. № 1 (69).
 5. Chibinev N. N., Lyashenko N. V. Cyberattack as a new type of emergency // *IVD*. 2024. № 7 (115).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056.53

СБОР ИНФОРМАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ (SHODAN, MALTEGO, SPIDERFOOT)

Вдовченко Г.П.

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: vdovchenko2003@gmail.com

Современные инструменты сбора данных из открытых источников (OSINT) стали незаменимыми в сфере кибербезопасности и анализа угроз. В статье рассматриваются три ключевых платформы — Shodan, Maltego и SpiderFoot, — их функциональные возможности, применение для поиска уязвимостей, анализа сетевой инфраструктуры и цифровых следов. Особое внимание уделено этическим и правовым аспектам работы с OSINT. Материал предназначен для специалистов по информационной безопасности, аналитиков и исследователей, работающих с открытыми данными.

Ключевые слова: OSINT, Shodan, Maltego, SpiderFoot, киберразведка, сетевые устройства, уязвимости, IoT-гаджеты, визуализация данных, автоматизация, GDPR, этический хакинг, фишинг, анализ угроз.

OPEN SOURCE INTELLIGENCE GATHERING (SHODAN, MALTEGO, SPIDERFOOT)

Vdovchenko G.P.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: vdovchenko2003@gmail.com

Modern tools for gathering data from open sources (OSINT) have become indispensable in the field of cybersecurity and threat analysis. The article explores three key platforms—Shodan, Maltego, and SpiderFoot—their functionalities, applications in identifying vulnerabilities, analyzing network infrastructure, and tracing digital footprints. Special attention is paid to the ethical and legal aspects of working with OSINT. The material is intended for information security specialists, analysts, and researchers dealing with open data.

Keywords: OSINT, Shodan, Maltego, SpiderFoot, cyber intelligence, network devices, vulnerabilities, IoT gadgets, data visualization, automation, GDPR, ethical hacking, phishing, threat analysis.

Введение

В условиях цифровой трансформации сбор информации из открытых источников (OSINT) превратился в критически важный инструмент для предотвращения кибератак, аудита безопасности и управления рисками. Такие платформы, как Shodan, Maltego и SpiderFoot, автоматизируют процессы разведки, позволяя выявлять уязвимости, анализировать сетевые инфраструктуры и прогнозировать угрозы. Однако их использование требует не только технических навыков, но и соблюдения правовых норм. В статье подробно разбираются принципы работы этих инструментов, их сильные стороны и ограничения.

Сбор информации из открытых источников (Shodan, Maltego, SpiderFoot)

В современном мире, где объемы открытых данных растут экспоненциально, инструменты OSINT (Open Source Intelligence) становятся ключевым элементом стратегий кибербезопасности. Платформы Shodan, Maltego и SpiderFoot предоставляют специалистам уникальные возможности для сбора, анализа и интерпретации информации, доступной в публичном пространстве. Эти инструменты позволяют не только реагировать на уже существующие угрозы, но и предугадывать потенциальные риски, основываясь на данных из интернета, социальных сетей и сетевых инфраструктур. Их применение охватывает широкий спектр задач — от выявления уязвимых устройств до расследования сложных кибератак, однако требует внимательного подхода к правовым и этическим аспектам.

Shodan, известный как «поисковая система для интернета вещей», представляет собой мощный инструмент для индексации устройств, подключенных к глобальной сети. В отличие от традиционных поисковиков, таких как Google, Shodan специализируется на сборе метаданных о сетевых устройствах — серверах, веб-камерах, IoT-гаджетах и даже промышленных системах управления [2]. Он предоставляет информацию об открытых портах (например, HTTP на порту 80 или SSH на порту 22), версиях программного обеспечения, геолокации и владельцах устройств. Простой запрос вроде «webcam country:RU» позволяет найти тысячи веб-камер в России, а более специфичный — «port:21 Anonymous user logged in» — выявляет FTP-серверы с анонимным доступом, которые могут быть уязвимы для атак [4]. В сфере кибербезопасности Shodan используется для аудита корпоративных сетей, помогая обнаружить устройства, которые случайно или намеренно остались открытыми для внешнего доступа. Например, компании могут проверить, не подключены ли их серверы к интернету без должной защиты, что особенно актуально для критической инфраструктуры, такой как электростанции или медицинские учреждения [2]. Однако возможности Shodan имеют и обратную сторону: злоумышленники могут использовать его для поиска целей, таких как незащищенные IoT-устройства в больницах, как это было зафиксировано в Европе в 2023 году [4]. Чтобы минимизировать риски, эксперты рекомендуют ограничивать публичный доступ к устройствам, регулярно обновлять прошивки и использовать брандмауэры для фильтрации трафика.

Maltego, в свою очередь, выделяется как инструмент для визуализации связей между различными объектами в рамках OSINT-разведки. Эта платформа позволяет аналитикам строить графы, связывающие людей, домены, IP-адреса и другие сущности, используя так называемые трансформы — скрипты, которые собирают данные из множества источников, включая WHOIS, Shodan, Twitter и LinkedIn [3]. Например, начав с домена, такого как example.com, пользователь может запустить трансформ «Domain to DNS Records», чтобы получить связанные IP-адреса, а затем расширить граф до SSL-сертификатов, субдоменов и даже владельцев этих ресурсов. Такой подход особенно полезен для расследования фишинговых атак, где необходимо выявить сеть клоновых доменов, созданных для обмана пользователей [5]. Maltego также применяется в борьбе с кибершпионажем, помогая отслеживать IP-адреса, связанные с АРТ-группами (Advanced Persistent Threats), и выявлять их инфраструктуру [4]. Однако работа с Maltego требует определённых навыков: без понимания OSINT-методик интерпретация графов может быть затруднена, а бесплатная версия (Maltego CE) ограничивает доступ к продвинутым трансформам, что снижает её

эффективность для сложных задач [3]. Несмотря на это, способность инструмента визуализировать сложные взаимосвязи делает его незаменимым для аналитиков, стремящихся понять структуру атакующего или защитить свою организацию от скрытых угроз.

SpiderFoot дополняет арсенал OSINT-инструментов, предлагая автоматизированный подход к сбору данных. Этот open-source фреймворк объединяет более 200 модулей, которые собирают информацию из самых разных источников — от DNS-записей и социальных сетей до VirusTotal и HaveIBeenPwned [1]. Например, запустив сканирование корпоративного домена, аналитик может обнаружить субдомены, утекшие учетные данные сотрудников или даже подозрительные файлы, связанные с этим доменом [5]. Основное преимущество SpiderFoot — экономия времени: вместо ручного поиска данных из десятков источников инструмент выполняет эту задачу автоматически, предоставляя результаты в удобном формате. Его гибкость позволяет настраивать модули под конкретные цели, будь то проверка безопасности внутренней сети или анализ внешних угроз [1]. Однако у SpiderFoot есть и слабые стороны: из-за большого объёма собираемой информации высока вероятность ложноположительных результатов, а интерпретация данных требует дополнительной фильтрации и проверки [3]. Это делает его особенно полезным для опытных аналитиков, способных отделить значимые сигналы от шума, но менее удобным для новичков.

Каждый из этих инструментов обладает уникальными характеристиками, которые определяют их применение в кибербезопасности. Shodan идеально подходит для поиска устройств и анализа их уязвимостей, особенно в контексте интернета вещей и критической инфраструктуры [2]. Его простота делает инструмент доступным даже для пользователей с минимальным опытом, хотя платный API необходим для получения полного функционала. Maltego, напротив, требует более глубокого подхода, но компенсирует это способностью раскрывать сложные взаимосвязи, что критично для расследований фишинга или кибершпионажа [4]. SpiderFoot выделяется своей автоматизацией, что делает его незаменимым для масштабных проектов разведки, хотя аналитикам приходится тратить время на проверку результатов [1]. Сравнение этих платформ по ключевым критериям — цели, сложности, стоимости и этическим рискам — показывает, что они дополняют друг друга, покрывая разные аспекты OSINT. Например, Shodan может выявить уязвимое устройство, Maltego — связать его с атакующим, а SpiderFoot — собрать дополнительные данные для полного анализа.

Важным аспектом работы с этими инструментами является соблюдение правовых и этических норм. Использование OSINT регулируется такими законами, как GDPR в Европе или ст. 272 УК РФ в России, которые запрещают несанкционированное сканирование сетей или сбор персональных данных без согласия [1]. Например, сканирование корпоративной сети с помощью Shodan без разрешения владельца может быть расценено как нарушение закона, даже если данные находятся в открытом доступе. Аналогично, применение Maltego для анализа социальных сетей или SpiderFoot для проверки утечек email требует строгого соблюдения конфиденциальности — использование собранной информации для атак или личной выгоды недопустимо [5]. Этические риски особенно высоки для Shodan, так как его данные могут быть легко направлены на поиск уязвимых целей, тогда как SpiderFoot, будучи менее ориентированным на прямое сканирование, представляет меньшую угрозу в этом плане [2]. Чтобы минимизировать риски, специалисты должны строго следовать принципам этического хакинга, получать разрешения на тестирование и документировать свои действия.

Интеграция Shodan, Maltego и SpiderFoot в рабочие процессы позволяет создать мощную систему киберразведки. Например, организация может начать с Shodan для обнаружения уязвимых IoT-устройств в своей сети, затем использовать Maltego для анализа связанных доменов и IP-адресов, а завершить процесс SpiderFoot, собрав дополнительные данные из открытых источников [3]. Такой подход особенно эффективен при расследовании сложных атак, таких как фишинг или инсайдерские угрозы, где требуется объединить данные из разных источников для построения полной картины [5]. Однако успех зависит от способности аналитиков комбинировать возможности инструментов, избегая при этом избыточности и юридических нарушений.

Будущее этих платформ связано с развитием технологий искусственного интеллекта, которые могут повысить их эффективность. Например, ИИ-алгоритмы в Shodan могли бы автоматически классифицировать устройства по уровню риска, в Maltego — предлагать гипотезы связей на основе исторических данных, а в SpiderFoot — фильтровать ложноположительные результаты [4]. Это снизило бы нагрузку на аналитиков и ускорило процесс принятия решений. Однако даже с такими улучшениями человеческий фактор останется ключевым — способность критически оценивать данные и принимать этически обоснованные решения будет определять успех OSINT-разведки в условиях всё более сложных киберугроз.

Заключение

Shodan, Maltego и SpiderFoot подтверждают, что инструменты OSINT стали незаменимым ресурсом в арсенале специалистов по кибербезопасности. Их эффективность, однако, зависит не только от технологических возможностей, но и от профессионализма пользователей, а также строгого следования правовым нормам. Например, Shodan способен выявить тысячи незащищенных IoT-устройств, но без умения аналитика интерпретировать эти данные в контексте конкретной организации или инфраструктуры, такая информация теряет практическую ценность. Кроме того, злоупотребление возможностями Maltego для сбора персональных данных или SpiderFoot для массового сканирования сторонних сетей без разрешения может привести к юридическим последствиям, включая нарушения GDPR или локальных законов о конфиденциальности. Будущее развития OSINT-инструментов тесно связано с интеграцией искусственного интеллекта и машинного обучения. ИИ-алгоритмы смогут автоматизировать рутинные задачи, такие как фильтрация ложных срабатываний в SpiderFoot, прогнозирование киберугроз на основе исторических данных Shodan или ускорение анализа сложных связей в Maltego. Это не только повысит скорость обработки информации, но и снизит нагрузку на специалистов, позволяя сосредоточиться на стратегических аспектах расследований. Однако даже с внедрением ИИ критически важным останется человеческий фактор — способность критически оценивать результаты, выявлять скрытые паттерны и принимать этически взвешенные решения. Для организаций, внедряющих OSINT-практики, ключевым приоритетом должно стать обучение сотрудников. Программы подготовки должны включать не только технические навыки работы с инструментами, но и основы киберэтики, понимание регуляторных требований (таких как HIPAA в медицине или PCI DSS в финансовом секторе) и управление рисками. Например, политики компании могут запрещать использование Shodan для сканирования сетей партнеров без письменного согласия или требовать многоуровневой проверки данных, полученных через Maltego. Такие меры

помогут избежать случайных нарушений и минимизировать репутационные потери. Рост числа подключенных устройств, усложнение фишинговых атак и увеличение объемов открытых данных ставят перед OSINT новые вызовы. Платформы вроде Shodan сталкиваются с проблемой информационной перегрузки, где даже простой поиск по ключевым словам возвращает десятки тысяч результатов, требующих ручной верификации. В ответ на это разработчики активно внедряют системы категоризации на основе ИИ, которые автоматически классифицируют устройства по типу, уровню уязвимости или географическому расположению. Одновременно Maltego и SpiderFoot эволюционируют в сторону междисциплинарного использования — от расследований киберпреступлений до журналистских расследований и аудита цепочек поставок. В конечном счете, сила OSINT-инструментов заключается не в их технологической сложности, а в способности специалистов сочетать их возможности с критическим мышлением, креативностью и ответственностью. Shodan, Maltego и SpiderFoot — это не «волшебные палочки», решающие все проблемы кибербезопасности, а инструменты, которые требуют осознанного подхода. Их дальнейшее развитие будет определяться балансом между автоматизацией и человеческим контролем, между скоростью сбора данных и соблюдением правовых границ. В мире, где киберугрозы становятся все более изощренными, именно этот баланс позволит превратить открытую информацию из потенциальной уязвимости в надежный щит для организаций и общества в целом.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
2. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Региональная информатика (РИ-2022). – 2022. – С. 572-573
3. Ахrameева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии // Телекоммуникации. – 2020. – №. 8. – С. 14-20.
4. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
5. Голубов Н. А., Косов Н. А. Внутренние угрозы: Разнообразие и профилактика инсайдеров в организациях. – 2023.

References

1. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems // Actual problems of infotelec communications in science and education (APINO 2019). – 2019. – pp. 266-270.
2. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network // Regional Informatics (RI-2022). – 2022. – pp. 572-573

3. Akhrameeva K. A. and others. Analysis of the means of exchanging hidden data by intruders on the Internet using steganography methods // Telecommunications. – 2020. – No. 8. – pp. 14-20.
 4. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system // Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 406-411.
 5. Golubev N. A., Kosov N. A. Internal threats: Diversity and prevention of insiders in organizations. – 2023.
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.021

МЕТОД ПРОВЕРКИ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЯ НА СЕРВЕР ЧЕРЕЗ GRPC НА ПРИМЕРЕ ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЫ

Никитин А.А.

*ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993,
Москва, Волоколамское ш., д. 4), e-mail: lyosha-2001@mail.ru*

При разработки различных образовательных платформ, одну из центральных ролей в проектировании играет проверка ролей и прав доступа для пользователей. В данной работе рассматривается реализация одного из методов проверки прав доступа на сервере, где клиент и сервер общаются под средствами gRPC запросов. gRPC требует заранее определенных контрактов, по которым строится генерация кода: на стороне сервера и клиента. В свою очередь, по кодогенерации строятся запросы в виде объектов, которые могут обрабатываться на стороне сервера.

Ключевые слова: gRPC, права доступа, веб-сервис, микросервисы, база данных.

A METHOD FOR VERIFYING USER ACCESS RIGHTS TO THE SERVER VIA GRPC USING THE EXAMPLE OF AN EDUCATIONAL PLATFORM

Nikitin A.A.

*MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia,
(125993, Moscow, Volokolamskoye shosse, 4), e-mail: lyosha-2001@mail.ru*

When developing various educational platforms, one of the central roles in design is the verification of roles and access rights for users. In this paper, we consider the implementation of one of the methods for verifying access rights on a server, where the client and server communicate using gRPC requests. gRPC requires pre-defined contracts for code generation: on the server and client sides. In turn, code generation builds queries in the form of objects that can be processed on the server side.

Keywords: gRPC, access rights, web service, microservices, database.

Общение клиента и сервера строиться на обмене данных между ними: клиент отправляет запрос, а сервер принимает и обрабатывает, в конце отдавая ответ. При общении учитывается множество факторов, но можно выделить основные: протокол передачи данных, формат данных, производительность. Обобщая, можно говорить о двух подходах между общением: gRPC, REST. Каждый из них является уникальным, например, gRPC является более быстрым, имеет типизацию запросов при описании контрактов для взаимодействия с сервером, но на данный момент не поддерживается браузером напрямую, поэтому требует дополнительных узлов для обработки запросов, приводящих данные к нужному протоколу, при этом данный узел может выступать в роли балансировщика запросов. Несмотря на данный минус, gRPC набирает популярность при проектировании интернет-сервисов.

Интернет-сервисы призваны решать потребительские проблемы для пользователей и должны подходить к ним с разных сторон, например, для образовательной платформы

необходимо рассмотреть пользователей в роли автора курсов, а также в роли потребителя или учащегося, проходящего этот курс, также будет преимуществом создание администратора платформы, но не обязательным, так как можно заниматься администрированием под средством обращения к серверу на прямую или же к базе данных.

Исходя из вышесказанного можно сказать, что интернет-сервис, обладающий определенной бизнес-логикой, работающей по-разному для различных пользователей, должен обладать определенной ролевой моделью с описанием прав доступа к ним.

Описание прав доступа по ролевой модели играет важную роль при проектировании. Для описание необходимо понимать, что оно должно быть представлено в виде табличных данных (Таблица 1), где описываются действия и разрешение для пользователей, а также дополнительные условия. Иными словами, права доступа необходимо задокументировать, это важно не только для серверной разработки, но и для клиентской.

Таблица 1 - Примеры прав доступа для курсов образовательной платформы

	Курсы образовательной платформы		
	Учащийся	Автор	Администратор
Создание	-	+	+
Чтение	+	+	+
Обновление	-	+(своего курса)	+(всех курсов)
Удаление	-	+(своего курса)	+(всех курсов)

Права доступа должны выдаваться на серверной части приложения: обычно если проект является монолитным, то есть два подхода: первый - создание прав доступа под средствам миграции данных и второй - написание прав доступа непосредственно в кодовой базе приложения, но оптимальным подходом является накатывание прав доступа с миграциями для базы данных, но есть сложность, когда становится много данных в миграции, велик шанс внесения ошибочных данных, поэтому данный подход расширяться через описание прав доступа и внесением их в базу данных в коде.

При использовании микросервисной архитектуры права доступа можно хранить в отдельном пользовательском микросервисе, где права доступа передаются от микросервиса с бизнес-логикой, но появляется масса сложностей с поддержанием такого подхода: возникает большая связность между микросервисами и запускать, например, отдельно микросервис курсов становится невозможным без пользовательского, также возникает проблема с поддержанием согласованности данных, оптимально же рассматривается подход, когда каждый микросервис самостоятельно накатывает права доступа в свою отведенную базу данных и дополняет определенными сведениями, а вся пользовательская информация запрашивается с пользовательского микросервиса или же передается через клиентскую часть, но возникает проблема согласованности данных.

Рассмотренный случай при монолитном проекте можно рассмотреть и для каждого микросервиса в отдельности, что позволит запускать каждый микросервис отдельно, из

минусов необходимо выделить, что может происходить дублирование логики между микросервисами.

Цель работы: описать метод проверки прав доступа пользователей через gRPC на примере образовательной платформы.

Для достижения цели необходимо решить задачи:

- рассмотреть образовательную платформу [1];
- описать метод проверки прав доступа.

В работе [1] описана архитектура образовательной платформы по изучению различных авиационных материалов. Необходимо подчеркнуть, что образовательная платформа имеет микросервисную архитектуру, поделенную на 5 микросервисов: работа с курсами, пользователями, справочных материалов, интерактивной карты и интеграции с чат-ботом. Каждый микросервис включает в себя работу с пользователями: вся необходимая информация запрашивается с пользовательского микросервиса и сохраняется в базе каждого отдельного микросервиса, а также реализуется работа проверка прав доступа. Каждый микросервис использует чистую архитектуру [2]. Верхнеуровневая реализация проверки показана на Рисунке 1.

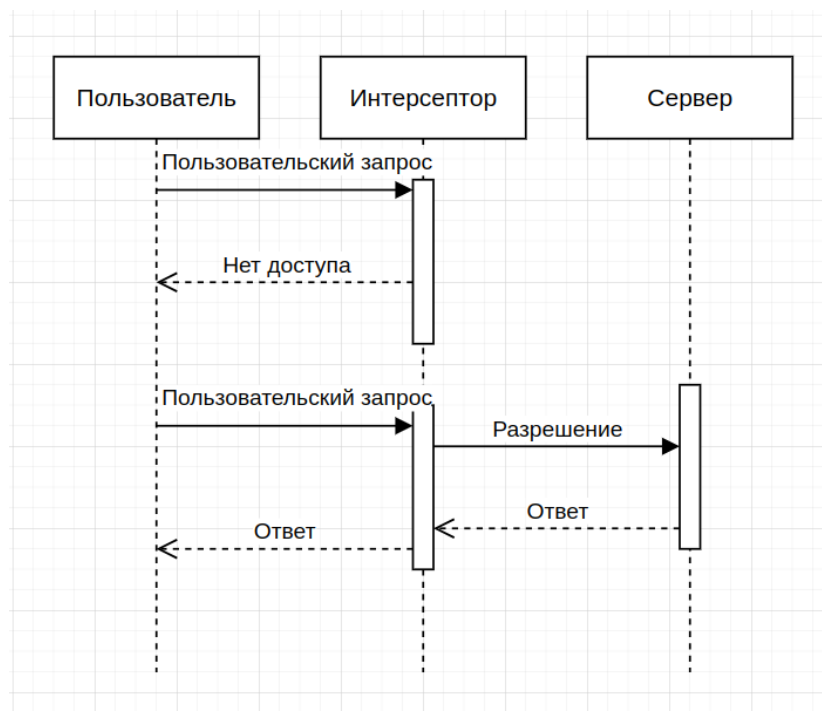


Рисунок 1 - Проверка прав доступа для пользователя

Микросервисы образовательной платформы пишутся на высокопроизводительном языке программирования golang и gRPC для быстрого взаимодействия между ними. Golang и gRPC разрабатываются и проектируются в рамках одной организации google, что привело к тому, что golang хорошо поддерживает gRPC, позволяя пользоваться всеми преимуществами: кодогенерацией, интерсепторами и т.д.

При использовании gRPC сначала описываются контракты. Контракты могут выступать в роли документации, но на данный момент документация создается с кодогенерацией и

комментариев в контрактах (рисунок 2). Которые потом мигрирует в код микросервиса, это необходимо для автоматизации и быстрого написания кодовой базы.

```
// UserInfo структура для получения информации о текущем пользователе
message UserInfo {
    optional int64 id = 1; // Уникальный идентификатор
    string portal_code = 2; // Код пользователя для телефонной книги
    string firstname = 4; // Имя пользователя
    string lastname = 5; // Фамилия пользователя
    repeated string email = 6; // Адрес электронной почты пользователя
    repeated string phone = 7; // Телефон пользователя
    string avatar = 8; // Ссылка на аватар пользователя
    string position = 9; // Должность пользователя из телефонной книги
    repeated permission.Role roles = 10; // Список ролей пользователя
}
```

UserInfo

UserInfo структура для получения информации о текущем пользователе

Field	Type	Label	Description
id	int64	optional	Уникальный идентификатор
portal_code	string		Код пользователя для телефонной книги
firstname	string		Имя пользователя
lastname	string		Фамилия пользователя
email	string	repeated	Адрес электронной почты пользователя
phone	string	repeated	Телефон пользователя
avatar	string		Ссылка на аватар пользователя
position	string		Должность пользователя из телефонной книги
roles	permission.Role	repeated	Список ролей пользователя

Рисунок 2 - Пример контракта для пользователя и сгенерированной документации

Frontend при использовании gRPC использует проху серверы, например, envoy. Данный сервер перехватывает запросы перед отправкой на сервер и конвертирует запрос в нужный формат данных понятный для gRPC. Envoy способен балансировать запросы на сервер, что делает общение через gRPC актуальным.

Проверка прав доступа заключается в том, что при каждом запросе на сервер необходимо проверять доступ пользователя к ресурсу. На сервере для этого используется перехватчик (middleware, interceptor), который будет перехватывать запрос от клиента и проверять доступ (Рисунок 3).

Схема выглядит довольно простой, пользователь хочет получить результаты определенной бизнес-логики, для этого пользователь отправляет запрос с определенными метаданными о себе, например, это может быть JWT токен или UUID пользователя для того, чтобы однозначно определить пользователя в системе. При отправке запроса, он проходит через перехватчика приложения, где сначала вытаскиваются метаданные пользователя,

отправляются в обработчик для пользователя и в контекст программы вставляется пользователь, если же не удалось определить пользователя в системе отдается ошибка в получении ответа от бизнес-логики.

После идет проверка прав доступа: из контекста достается пользователь с определенными ролями, а также из запроса вытаскивается вся необходимая информация на какой метод бизнес-логики должен прийти данный запрос: данная информация представлена в виде названия метода. Данные о ролях пользователя и названия метода передаются в обработчик для прав доступа, где если есть в базе данных строчка роль и название метода, то выдается разрешение для дальнейшего запроса в бизнес-логику, которая отдает ответ.

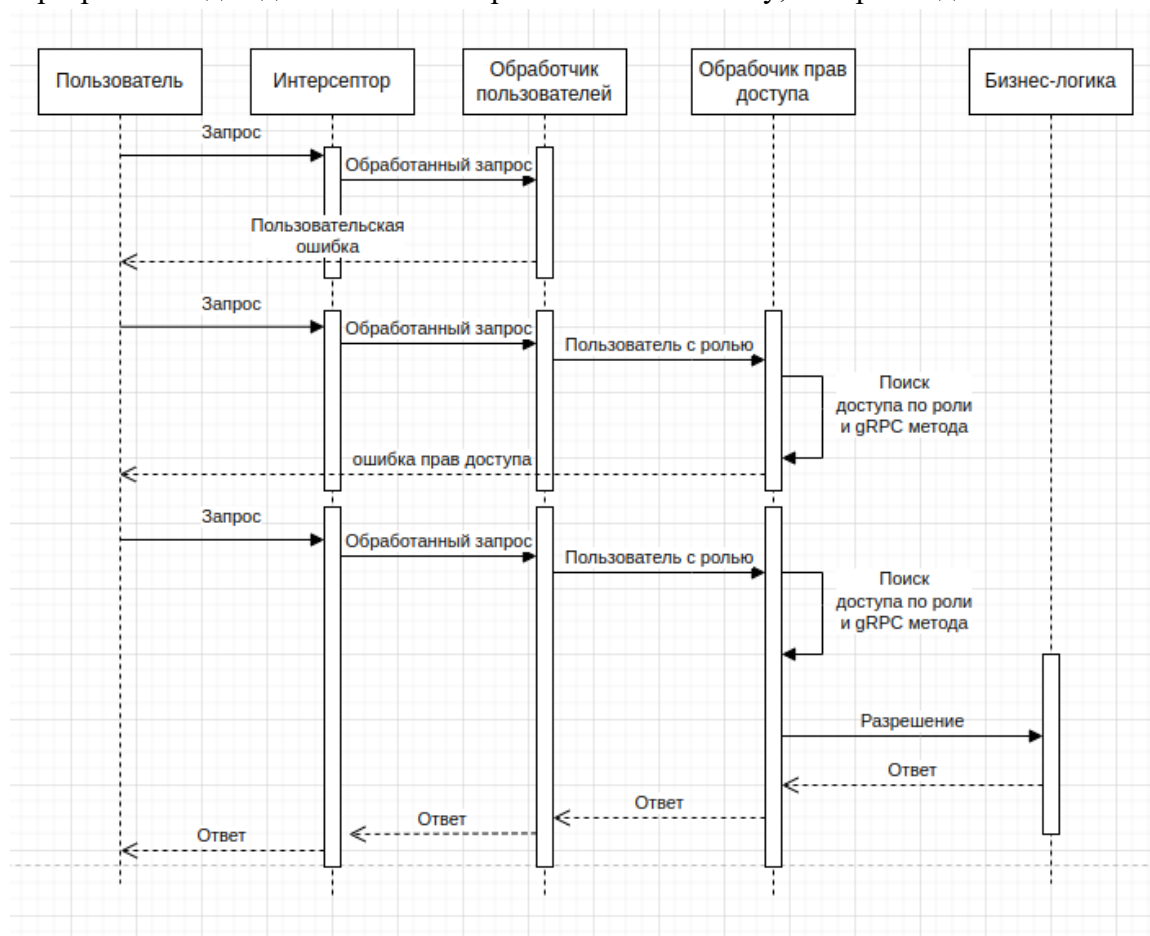


Рисунок 3 - Обработка прав доступа

Для внесения прав доступа пользователям образовательной платформы в БД сначала выделяются роли: студент, автор курса. Для корректного внесения в БД необходимо использовать паттерн проектирование builder (строитель) [3], который в зависимости от роли будет перед развертыванием приложения накатывать миграции в БД. Строитель берет описанные название gRPC методов из кодогенерации и распределяет права доступа для ролей. Для каждой роли может быть собственный стек методов. Например, в рамках образовательной платформы бизнес-логика должна обрабатывать CRUD для курсов, где студент имеет право только на прохождение курсов, а автор на создание и удаление собственного курса.

Для написания обработчика необходимо учесть, что при кодогенерации gRPC создает сервисы, который описаны в контрактах, поэтому необходимо внимательно подходить к их написанию. Каждый сервис имеет набор собственных методов. Отталкиваясь от сервиса,

необходимо построить путь при перехвате запроса: перехват запроса с метаданными о пользователе, получения пользовательских данных и его авторизация, переход к нужному gRPC сервису, затем переход к нужному обработчику перед использованием бизнес-метода, а дальше заключающий этап проверки – нахождение прав доступа в БД.

Выводы: образовательная платформа по изучению авиационных материалов имеет небольшое количество микросервисов, значит обработка пользователей для каждого микросервиса не вызовет большое количество проблем, а наоборот решит главные вопросы: поддержание актуальности данных, возможность развертывания вне зависимости от других микросервисов, проверка прав доступа через gRPC под требования определенной бизнес-логики, что позволит разграничивать зоны ответственности.

Надо отметить, что в методе проверки прав доступа используется builder для создания прав и ролей пользователей в БД, а также используется interceptor для проверки прав доступа. Данная реализация позволит ускорить разработку приложения, а также упростит работу с пользователями.

Список литературы

1. Никитин, А.А. Архитектура высоконагруженного интернет-сервиса: образовательная платформа для изучения авиационных материалов / Никитин А.А. / МАИ, г. Москва – 1 с.
2. Мартин, Роберт. Чистая архитектура. Искусство разработки программного обеспечения / Роберт Мартин ; перевел с английского А. Киселев. - Санкт-Петербург [и др.] : Питер, 2021. - 350 с. : ил. - (Серия "Библиотека программиста"). - Пер. изд.: Clean architecture. A craftsman's guide to software structure and design / Robert C. Martin. - 2018.
3. Гамм, А. Паттерны объектно-ориентированного проектирования / А. Гамм, М. Хел, Н. Джонсо, В. Д. - СПб. : Питер, 2021. - 448 с.

References

1. Nikitin, A.A. Architecture of a highly loaded Internet service: an educational platform for studying aviation materials / Nikitin A.A. / MAI, Moscow – p.1
 2. Martin, Robert. Clean architecture. The Art of Software Development / Robert Martin; translated from English by A. Kiselyov. - St. Petersburg [and others] : Peter, 2021. 350 p. : ill. (Series "Programmer's Library"). - Per. ed.: Clean architecture. A craftsman's guide to software structure and design / Robert C. Martin. - 2018.
 3. Gamm, A. Patterns of object-oriented design / A. Gamm, M. Khel, N. Jones, V. D. - St. Petersburg : Peter, 2021. - p. 448
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

РАЗРАБОТКА СИСТЕМ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ АТАК НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Гаджиев Г.К.

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:
gugac134@gmail.com

Статья посвящена исследованию применения технологии блокчейн для разработки систем автоматического распознавания кибератак. Раскрываются проблемы традиционных подходов к обнаружению угроз, такие как централизованность, уязвимость к манипуляциям с данными и ограниченная масштабируемость. Рассматриваются преимущества внедрения блокчейна, включая неизменяемость данных, децентрализацию, прозрачность и отказоустойчивость, а также возможности интеграции с методами искусственного интеллекта для анализа и предотвращения атак. Особое внимание уделяется вызовам, связанным с масштабируемостью и скоростью работы блокчейн-сетей, а также перспективам их развития в гибридных архитектурах. Отмечается, что применение блокчейна в системах автоматического распознавания атак открывает новые горизонты для повышения их безопасности, прозрачности и эффективности.

Ключевые слова: Блокчейн, кибербезопасность, автоматическое распознавание атак, децентрализация, неизменяемость данных, искусственный интеллект, системы обнаружения вторжений, масштабируемость, безопасность данных, распределённые реестры.

DEVELOPMENT OF AUTOMATIC ATTACK RECOGNITION SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY

Gadzhiev G.K.

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: gugac134@gmail.com

The article is devoted to the study of the use of blockchain technology for the development of automatic recognition systems for cyber attacks. The problems of traditional approaches to threat detection, such as centralization, vulnerability to data manipulation, and limited scalability, are revealed. The advantages of blockchain implementation are considered, including data immutability, decentralization, transparency and fault tolerance, as well as the possibility of integration with artificial intelligence methods for analyzing and preventing attacks. Particular attention is paid to the challenges associated with the scalability and speed of blockchain networks, as well as the prospects for their development in hybrid architectures. It is noted that the use of blockchain in automatic attack recognition systems opens up new horizons for improving their security, transparency and efficiency.

Keywords: Blockchain, cybersecurity, automatic attack recognition, decentralization, data immutability, artificial intelligence, intrusion detection systems, scalability, data security, distributed ledgers.

Введение

С ростом интенсивности кибератак и их усложнением традиционные механизмы защиты информации уже не всегда обеспечивают надёжную защиту данных и инфраструктуры.

Современные атаки все чаще используют передовые технологии, включая машинное обучение и автоматизацию, что значительно усложняет их обнаружение и предотвращение. В этой связи наибольшую актуальность приобретает разработка систем автоматического распознавания атак, которые способны не только обнаружить угрозу, но и оперативно предоставить информацию для её нейтрализации. Одной из инновационных технологий, которые могут усилить эффективность таких систем, является блокчейн. Блокчейн уже доказал свою надёжность в задачах сохранения данных, обеспечивая их неизменность, верификацию и прозрачность. Применение блокчейн-технологий в области кибербезопасности, особенно для автоматического распознавания атак, открывает новые возможности для создания децентрализованных и устойчивых к манипуляциям систем.

Традиционные системы обнаружения атак.

Традиционные системы обнаружения атак, в том числе основанные на сигнатурах и аномалиях, имеют ряд существенных недостатков. Во-первых, централизованность делает их уязвимыми к атакам на саму систему мониторинга, поскольку злоумышленник, получив доступ к центру управления сетью, может скрыть свои действия. Во-вторых, такие системы сильно зависят от скорости обновления баз данных об угрозах и редко обеспечивают оперативное взаимодействие между различными частями инфраструктуры компаний. Кроме того, масштабируемость традиционных систем также вызывает затруднения: по мере роста сетей и объёмов данных их производительность существенно падает. В этом контексте блокчейн предоставляет уникальное преимущество за счёт своей децентрализованной архитектуры, неизменяемости записей и возможности функционирования без необходимости в едином доверительном центре [1].

Одной из ключевых особенностей блокчейна, способствующих его применению для автоматического распознавания атак, является его способность хранить данные об аномалиях и подозрительных действиях в неизменяемой структуре. Каждая запись в блокчейне подтверждается с помощью криптографических алгоритмов, что позволяет исключить возможность её изменения или удаления задним числом. Это свойство особенно важно для накопления исторических данных об атаках, что впоследствии может быть использовано при обучении систем машинного обучения или анализе сложных угроз. Данные, хранящиеся в блокчейне, могут включать информацию о подозрительных IP-адресах, паттерны аномального поведения сетевого трафика или уникальные сигнатуры вредоносного ПО. Децентрализованный механизм хранения также гарантирует, что даже в случае компрометации одной из точек системы обмануть всю сеть будет практически невозможно, так как контроль данных остается распределённым между множеством узлов [2-3].

Блокчейн может быть интегрирован в систему обнаружения атак двумя ключевыми способами. Во-первых, он может функционировать как база данных для хранения событий безопасности (Security Events), что обеспечивает прозрачность их обработки и неизменяемость собранной информации. Например, данные о сетевых аномалиях и попытках атак, зафиксированные системой обнаружения, записываются сразу в распределённый реестр, что исключает вероятность их подмены. Во-вторых, блокчейн можно использовать для координации действий между различными компонентами системы. Например, на основе данных об обнаруженных угрозах узлы сети могут автоматически обновлять свои механизмы

защиты, не прибегая к обращению в централизованный сервер. Таким образом, блокчейн способствует созданию полностью автономных систем обнаружения и предотвращения атак.

Автоматизация обнаружения атак с использованием блокчейн-технологий также активно поддерживается внедрением методов искусственного интеллекта. Современные алгоритмы анализа аномалий способны обнаруживать скрытые угрозы в реальном времени на основе огромного количества переменных данных. Однако для эффективного обучения таких алгоритмов необходимо большое количество качественных данных, которые не подвергались манипуляциям. Блокчейн в данном случае выполняет роль доверенной платформы, где хранятся "сырые" данные об атаках, доступные для анализа и обучения. Например, децентрализованные кибер-разведывательные платформы позволяют организациям делиться информацией о попытках атак, сохраняя анонимность и защищённость, а благодаря блокчейну гарантируется подлинность передаваемых данных.

Среди основных преимуществ применения блокчейн-технологии в системах автоматического распознавания атак выделяются неизменяемость данных, децентрализация, прозрачность деятельности и высокая отказоустойчивость. Неизменяемость данных обеспечивает точность анализа угроз, так как записи об угрозах нельзя удалить или модифицировать. Децентрализация устраняет необходимость в едином уязвимом центре управления, что делает систему устойчивой даже при компрометации отдельных узлов. Прозрачность позволяет организациям обмениваться данными об угрозах без необходимости устанавливать доверительные отношения между ними, а высокая отказоустойчивость обеспечивается тем, что для взлома системы злоумышленнику приходится одновременно атаковать множество узлов сети [4].

Однако, несмотря на эти преимущества, существуют и определённые вызовы, связанные с использованием блокчейна в системах обеспечения кибербезопасности. Первым из таких вызовов является проблема масштабируемости. Даже самые современные блокчейны, такие как Ethereum, всё ещё испытывают сложности с обработкой большого объёма транзакций при низкой пропускной способности, что ограничивает их применение в высоконагруженных кибербезопасных системах. Второй проблемой является задержка в работе сети: операции записи данных в блокчейн требуют времени для подтверждения, что может оказаться критичным фактором в средах, где требуется мгновенная реакция на атаки. Кроме того, несмотря на то что технология блокчейн обеспечивает неизменяемость данных, это также делает её уязвимой в случае, если вредоносные данные всё же были записаны в реестр, так как исправить ошибку становится практически невозможно.

С учётом текущих ограничений перспективы дальнейшего развития систем автоматического распознавания атак с использованием блокчейна связаны с внедрением гибридных архитектур и новых технологий [5]. Например, гибридные системы могут сочетать использование публичных блокчейнов для записи итоговых данных с применением частных распределённых реестров для быстрого реагирования на угрозы в реальном времени. Также активно развиваются решения второго уровня блокчейна, такие как свернутые цепочки и каналы обработки, которые могут значительно повысить скорость и производительность системы. Одновременно с этим продолжаются исследования в области интеграции блокчейн-сетей с технологиями интернета вещей (IoT) и искусственного интеллекта для разработки интеллектуальных адаптивных систем.

Заключение.

В заключение следует отметить, что развитие систем автоматического распознавания атак с использованием технологии блокчейн является перспективным направлением, способным поменять основные подходы к обеспечению кибербезопасности. Децентрализованность, надёжность и неизменяемость данных, предоставляемые блокчейн-технологиями, дают возможность создавать именно те системы защиты, которые способны противостоять современным видам атак, включая внедрение фальсифицированных данных и компрометацию узлов. Несмотря на сложные технологические вызовы, включая масштабируемость и задержки, дальнейшее развитие блокчейна и его адаптация к задачам автоматизации защиты помогут развивать новые стандарты в области кибербезопасности, делая системы обнаружения атак более быстрыми, надёжными и прозрачными.

Список литературы

1. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. –63с.– EDN CMMEMML.
2. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2015. –63 p. - EDN CMMEMML.
2. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelec communications in science and education (APINO 2020). – 2020. – pp. 563-568.
3. Suvorov A.M., Tsvetkov A. Y. Investigation of buffer overflow attacks in 64-bit unix-like operating systems //Actual problems of infotelec communications in science and education (APINO 2018). – 2018. – pp. 570-573.
4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 72-76.

5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СОЦИАЛЬНЫХ АСПЕКТОВ НА КИБЕРБЕЗОПАСНОСТЬ: КАК ЧЕЛОВЕЧЕСКИЙ ФАКТОР ВЛИЯЕТ

Гаджиев Г.К.

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: gugac134@gmail.com

В статье рассматривается влияние социальных аспектов на кибербезопасность, а также роль человеческого фактора в уязвимости цифровых систем. Анализируются основные угрозы, связанные с недостаточной кибер-грамотностью, фишинговыми атаками, социальной инженерией и инсайдерскими угрозами. Описаны методы защиты, включая обучение пользователей, усиленную аутентификацию, технические меры безопасности и мониторинг поведения. Особое внимание уделяется необходимости формирования культуры кибербезопасности как ключевого элемента защиты информации.

Ключевые слова: Кибербезопасность, человеческий фактор, социальная инженерия, фишинг, инсайдерские угрозы, кибер-грамотность, многофакторная аутентификация, мониторинг пользователей.

RESEARCH INTO THE IMPACT OF SOCIAL ASPECTS ON CYBERSECURITY: HOW HUMAN FACTORS AFFECT

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article examines the impact of social aspects on cybersecurity, as well as the role of the human factor in the vulnerability of digital systems. The main threats related to insufficient cyber literacy, phishing attacks, social engineering and insider threats are analyzed. Protection methods are described, including user training, enhanced authentication, technical security measures, and behavior monitoring. Special attention is paid to the need to form a culture of cybersecurity as a key element of information protection.

Keywords: Cybersecurity, human factor, social engineering, phishing, insider threats, cyber literacy, multifactor authentication, user monitoring.

Введение

С развитием технологий и повсеместной цифровизации всё больше аспектов жизни переходят в онлайн-пространство. Это приводит к росту числа кибератак, в которых центральную роль играет человеческий фактор. Социальные аспекты, такие как психологические особенности пользователей, уровень их осведомлённости в области информационной безопасности, а также социальная инженерия, значительно влияют на уязвимость цифровых систем. Независимо от уровня технологической защиты, ошибки пользователей, недостаточная подготовка сотрудников и влияние социальных механизмов остаются важными факторами, способствующими угрозам безопасности.

Основные уязвимости, связанные с человеческим фактором.

Одной из ключевых уязвимостей является низкий уровень кибер-грамотности пользователей. Многие пользователи используют слабые пароли, игнорируют двухфакторную аутентификацию и не проверяют источники информации перед её обработкой. Это делает их лёгкой мишенью для киберпреступников, использующих фишинг, социальную инженерию и вредоносное ПО.

Фишинговые атаки являются одной из наиболее распространённых угроз. Киберпреступники создают поддельные веб-сайты или электронные письма, побуждая пользователей вводить конфиденциальные данные, такие как логины и пароли. Недостаточная бдительность и нехватка знаний об этих угрозах приводят к значительному числу успешных атак [1-2].

Другим важным аспектом является поведенческая предсказуемость пользователей. Злоумышленники анализируют поведение жертв, используя методы социальной инженерии, чтобы заставить их выполнить нужные действия. Это может включать предоставление личных данных, загрузку вредоносных файлов или открытие доступа к конфиденциальным системам.

Также следует отметить проблему инсайдерских угроз [3]. Сотрудники компаний, будь то по неосторожности или с умышленным умыслом, могут становиться источником утечек данных и компрометации систем. Внутренние угрозы сложно обнаружить, так как инсайдеры зачастую обладают высоким уровнем доступа к информации.

Методы защиты от угроз, связанных с человеческим фактором.

Для повышения уровня безопасности необходимо внедрение комплексных мер, направленных на минимизацию влияния человеческого фактора [4].

Обучение и повышение осведомлённости. Регулярные тренинги по кибербезопасности позволяют пользователям распознавать угрозы и реагировать на них корректным образом. Имитационные фишинговые атаки помогают выявлять слабые места в подготовке сотрудников и улучшать их кибер-грамотность.

Усиленная аутентификация. Использование многофакторной аутентификации (MFA) снижает риск несанкционированного доступа даже в случае компрометации паролей. Биометрическая идентификация и аппаратные ключи безопасности также являются эффективными инструментами защиты.

Технические меры защиты. Антивирусное ПО, системы предотвращения вторжений (IDS/IPS) и решения для мониторинга сетевой активности помогают обнаруживать и предотвращать атаки, связанные с социальной инженерией.

Контроль доступа и мониторинг поведения пользователей. Внедрение ролевой модели доступа (RBAC) позволяет ограничивать уровень привилегий сотрудников, снижая вероятность вредоносных действий. Поведенческий анализ пользователей с помощью машинного обучения помогает выявлять аномальные действия и предотвращать инсайдерские угрозы.

Культура кибербезопасности. Формирование у сотрудников и пользователей осознания важности защиты данных и ответственности за цифровую безопасность способствует снижению риска человеческих ошибок.

Заключение.

Человеческий фактор остаётся одним из наиболее уязвимых звеньев в кибербезопасности. Несмотря на технологические достижения в защите данных, ошибки пользователей, предсказуемость их поведения и социальная инженерия продолжают представлять серьёзную угрозу. Комплексный подход, включающий обучение, технические меры защиты и формирование культуры кибербезопасности, позволяет значительно снизить риски и повысить устойчивость цифровых систем к атакам. В условиях продолжающейся цифровой трансформации внимание к социальным аспектам кибербезопасности становится ключевым элементом защиты информации и цифровых активов.

Список литературы

1. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEMML.
2. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2015. – p. 63 - EDN CMMEMML.
2. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelec communications in science and education (APINO 2020). – 2020. – pp. 563-568.
3. Suvorov A.M., Tsvetkov A. Y. Investigation of buffer overflow attacks in 64-bit unix-like operating systems //Actual problems of infotelec communications in science and education (APINO 2018). – 2018. – pp. 570-573.

4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 72-76.
 5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА РАЗНЫХ СТРАН В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Гаджиев Г.К.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (192322, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
gugac134@gmail.com

В статье проводится сравнительный анализ законодательства различных стран в области кибербезопасности. Рассматриваются ключевые нормативные акты, регулирующие защиту информации, а также подходы к предотвращению и расследованию киберпреступлений. Особое внимание уделяется различиям в правовых системах США, Европейского Союза, России и Китая, а также их влиянию на глобальную политику информационной безопасности. Проанализированы тенденции развития законодательной базы и предложены рекомендации по унификации международных стандартов защиты данных.

Ключевые слова: Кибербезопасность, законодательство, защита информации, киберпреступления, нормативные акты, международное право, персональные данные.

LEGAL ASPECTS OF INFORMATION PROTECTION: A COMPARATIVE ANALYSIS OF THE LEGISLATION OF DIFFERENT COUNTRIES IN THE FIELD OF CYBERSECURITY

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (192322, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article provides a comparative analysis of the legislation of different countries in the field of cybersecurity. The key regulations governing information security, as well as approaches to the prevention and investigation of cybercrimes, are considered. Special attention is paid to the differences in the legal systems of the United States, the European Union, Russia and China, as well as their impact on global information security policy. The trends in the development of the legislative framework are analyzed and recommendations for the unification of international data protection standards are proposed.

Keywords: Cybersecurity, legislation, information protection, cybercrime, regulations, international law, personal data.

Введение

С развитием цифровых технологий и ростом числа киберугроз защита информации становится одной из ключевых задач государств. В различных странах разработаны собственные нормативные акты, регулирующие вопросы кибербезопасности, однако их содержание и принципы значительно различаются. В данной статье проводится сравнительный анализ законодательных подходов к защите информации в разных юрисдикциях, с акцентом на нормативные акты США, Европейского Союза, России и Китая.

Изучение правовых аспектов кибербезопасности позволяет выявить сильные и слабые стороны национальных стратегий и определить перспективы международного сотрудничества [1-2].

Законодательство США в области кибербезопасности. В Соединённых Штатах вопросы защиты информации регулируются несколькими основными законами, такими как Закон о модернизации кибербезопасности (CISA), Закон о защите критической инфраструктуры (CIP) и Закон о компьютерном мошенничестве и злоупотреблениях (CFAA). Эти акты направлены на предотвращение кибератак, защиту персональных данных и координацию взаимодействия между государственными органами и частным сектором. Важной особенностью американского законодательства является наличие отдельных законов для различных отраслей экономики, например, HIPAA для здравоохранения и GLBA для финансового сектора[3].

Регулирование кибербезопасности в Европейском Союзе. Европейский Союз реализует комплексный подход к защите данных, основными документами которого являются Общий регламент по защите данных (GDPR) и Директива NIS (Network and Information Security). GDPR устанавливает строгие требования к обработке персональных данных и предусматривает серьёзные штрафы за их нарушение. Директива NIS фокусируется на обеспечении безопасности критической инфраструктуры и цифровых сервисов. В отличие от США, законодательство ЕС делает акцент на защите прав пользователей и прозрачности обработки данных.

Кибербезопасность в законодательстве России. В России нормативная база в области защиты информации представлена Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации", Законом "О персональных данных" и рядом подзаконных актов. Российское законодательство ориентировано на защиту национальных интересов и суверенитет в цифровой сфере. Важное место занимает регулирование деятельности иностранных IT-компаний, в том числе требования о локализации данных российских граждан [4].

Кибербезопасность в Китае. Китайская система регулирования кибербезопасности является одной из самых жёстких в мире. Основным нормативным актом является Закон КНР о кибербезопасности, который устанавливает строгие требования к защите данных, мониторингу интернет-активности и контролю за деятельностью иностранных технологических компаний. Китайская политика в данной сфере направлена на обеспечение национальной безопасности и защиту государственных интересов в киберпространстве.

Сравнительный анализ и перспективы международного сотрудничества. Сравнение законодательных систем разных стран показывает значительные различия в подходах к регулированию кибербезопасности. США ориентированы на защиту бизнеса и развитие инноваций, ЕС делает акцент на права пользователей, Россия и Китай придерживаются модели цифрового суверенитета. Эти различия создают препятствия для международного сотрудничества, однако необходимость борьбы с глобальными киберугрозами требует

формирования единых стандартов. В этом контексте перспективными направлениями являются разработка международных соглашений по обмену информацией, согласование требований к обработке данных и унификация мер реагирования на кибератаки.

Заключение.

Правовое регулирование кибербезопасности играет ключевую роль в обеспечении защиты данных и цифровых систем. Анализ законодательства США, ЕС, России и Китая демонстрирует различные подходы к решению данной проблемы, обусловленные национальными интересами и политическими приоритетами. Несмотря на существующие различия, развитие международного сотрудничества и унификация стандартов безопасности являются необходимыми шагами для эффективной борьбы с киберугрозами в глобальном масштабе.

Список литературы

1. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
2. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядер в системах специального назначения //I-methods. – 2020. – Т. 12. – №. 3. – С. 2.
3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76].
4. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.

References

1. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special-purpose systems // Actual problems of infotelecommunications in science and education (APINO 2020). - 2020. - pp.563-568.
2. Kirilova K. S. et al. The problem of neutralizing kernel-level rootkits in special-purpose systems // I-methods. - 2020. - Vol. 12. - No. 3. - p. 2.
3. Pestov I. E. Methodology for developing control action on cloud infrastructure instances // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. - No. 4. - pp.72-76.
4. Suvorov A. M., Tsvetkov A. Yu. Study of buffer overflow attacks in 64-bit unix-like operating systems // Actual problems of infotelecommunications in science and education (APINO 2018). - 2018. - pp. 570-573.

5. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A. V. Krasov, A. Yu. Tsvetkov. Volume Part 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruевич, 2015. - p. 63 - EDN CMMEML.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАДИЦИОННЫХ И НЕЙРОСЕТЕВЫХ МЕТОДОВ ОБНАРУЖЕНИЯ БПЛА

Ильюшкин А.С.

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:
guestyltest@gmail.com

В статье проведен сравнительный анализ традиционных методов обработки сигналов и нейросетевых подходов для обнаружения беспилотных летательных аппаратов (БПЛА). Рассмотрены классические алгоритмы, такие как байесовский подход, критерии Неймана-Пирсона и алгоритмы минимизации среднего риска, а также их эффективность в условиях шумов и помех. Особое внимание уделено использованию искусственных нейронных сетей (ИНС) для повышения точности детекции, автоматического выделения признаков и адаптации к изменяющимся условиям. Оценена эффективность различных методов с применением метрик F1-меры и AUC-ROC, что позволяет обоснованно сравнить их преимущества и недостатки в задачах мониторинга воздушного пространства.

Ключевые слова: БПЛА, обработка сигналов, нейросети, классификация сигналов, фильтрация шума, байесовский подход, критерий Неймана-Пирсона, искусственные нейронные сети (ИНС), радиолокация, акустический мониторинг, машинное обучение, F1-мера, AUC-ROC.

COMPARATIVE ANALYSIS OF TRADITIONAL AND NEURAL NETWORK METHODS OF UAV DETECTION

Ilyushkin A. S.

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: guestyltest@gmail.com

The article provides a comparative analysis of traditional signal processing methods and neural network approaches for detecting unmanned aerial vehicles (UAVs). Classical algorithms such as the Bayesian approach, the Neiman-Pearson criteria, and algorithms for minimizing average risk are considered, as well as their effectiveness in the face of noise and interference. Special attention is paid to the use of artificial neural networks (ANN) to improve detection accuracy, automatically identify features and adapt to changing conditions. The effectiveness of various methods using the F1-measure and AUC-ROC metrics is evaluated, which makes it possible to reasonably compare their advantages and disadvantages in air space monitoring tasks.

Keywords: UAVs, signal processing, neural networks, signal classification, noise filtering, Bayesian approach, Neiman-Pearson criterion, artificial neural networks (ANN), radar, acoustic monitoring, machine learning, F1-measure, AUC-ROC.

Эффективное обнаружение беспилотных летательных аппаратов (БПЛА) требует применения классических методов обработки сигналов, которые позволяют выделить полезный сигнал на фоне шума. Эти подходы базируются на строгих математических принципах и зарекомендовали себя как надёжные инструменты в радиолокации, акустике и инфракрасных системах [1]. Рассмотрим классические подходы к обработке данных.

Байесовский подход основан на теории вероятностей и позволяет определить, с какой вероятностью наблюдаемый сигнал относится к целевому объекту. Основным инструментом этого подхода — формула Байеса, что отражено в формуле 1.

$$P(H \setminus X) = \frac{P(X \setminus H)P(H)}{P(X)} \quad (1)$$

Где $P(H \setminus X)$ - апостериорная вероятность гипотезы H при наблюдении данных X , $P(H \setminus X)$ - правдоподобие, $P(H)$ - априорная вероятность гипотезы, $P(X)$ - нормирующая константа.

В задачах обнаружения БПЛА гипотеза H_1 может означать, что сигнал принадлежит объекту (БПЛА), а гипотеза H_0 - что сигнал является шумом. Байесовский подход позволяет минимизировать вероятность ошибки за счёт оптимального выбора порога принятия решения.

Критерии Неймана-Пирсона направлены на максимизацию вероятности обнаружения объекта P_D при фиксированной вероятности ложной тревоги P_{FA} . Оптимальное решение в этом подходе основано на сравнении отношения правдоподобия $L(X)$ с порогом η , что отобразено в формуле 2:

$$L(X) = \frac{f(X | H_1)}{f(X | H_0)} < \eta \quad (2)$$

Где $f(X | H_1)$ и $f(X | H_0)$ — функции плотности вероятности наблюдений при гипотезах H_1 и H_0 .

Применение критерия Неймана-Пирсона позволяет строго контролировать вероятность ложных тревог, что особенно важно в условиях высокого уровня помех, например, в радиолокационных системах.

Алгоритмы минимизации среднего риска.

Этот подход основывается на минимизации математического ожидания потерь, вызванных ошибочными решениями. Средний риск определяется по формуле 3:

$$R = \sum_{i,j} \lambda_{ij} P(H_i | X_j) P(X_j) \quad (3)$$

Где λ_{ij} – стоимость ошибки принятия решения H_i , если истинной является гипотеза H_j , $P(H_i | X_j)$ — апостериорная вероятность, $P(X_j)$ — вероятность наблюдения X_j .

В контексте обнаружения БПЛА минимизация риска позволяет учитывать как вероятность ошибок, так и их последствия, что делает этот метод особенно ценным при работе с системами высокой чувствительности [2].

Рассмотренные классические подходы, такие как Байесовский метод, критерии Неймана-Пирсона и алгоритмы минимизации среднего риска, предоставляют эффективные инструменты для принятия решений на основе математического анализа [3]. Однако их практическая реализация в задачах обнаружения БПЛА тесно связана с необходимостью выделения полезного сигнала на фоне разнообразных помех.

Шумы, создаваемые окружающей средой, инфраструктурой или другими техническими устройствами, накладывают серьёзные ограничения на точность систем мониторинга. Именно поэтому задача выделения сигнала на фоне шума становится ключевым этапом обработки данных. Рассмотрим основные аспекты её реализации.

1. Классификация сигналов

Классификация заключается в разделении входящих данных на категории "сигнал от БПЛА" и "шум". Для этого применяются:

- Линейные классификаторы, такие как дискриминантный анализ. Например, решение задачи классификации формируется на основе критерия, отображенного в формуле 4:

$$g(X) = w^T X + w_0 \quad (4)$$

Где w - вектор весов, X - вектор входных данных, w_0 – порог.

- Нелинейные методы, такие как использование ядерных функций, которые позволяют учитывать сложные зависимости в данных.

2. Фильтрация шума.

Фильтрация направлена на подавление фоновых помех для выделения полезного сигнала. Основные методы включают:

- Фильтры нижних частот для устранения высокочастотных шумов, часто используемых в акустических системах.
- Узкополосные фильтры для выделения сигналов с известной частотой, характерной для дронов (например, шумов винтов).

Временные и частотные методы фильтрации часто используются совместно, чтобы повысить эффективность обработки сигналов в сложных условиях.

3. Оценка соотношения сигнал/шум (SNR)

Для успешного выделения полезного сигнала часто используется параметр SNR (signal-to-noise ratio), определяемый по формуле 5:

$$SNR = \frac{P_{signal}}{P_{noise}} \quad (5)$$

Где P_{signal} — мощность полезного сигнала, P_{noise} — мощность шума. Чем выше SNR, тем легче выделить сигнал на фоне помех. Методы повышения SNR включают усиление полезного сигнала или подавление шумов.

Обнаружение беспилотных летательных аппаратов (БПЛА) связано с решением задач классификации, выделения сигнала на фоне шума и анализа данных в условиях высокой изменчивости и помех. Традиционные методы обработки данных, такие как Байесовские подходы и критерии Неймана-Пирсона, эффективно справляются с обработкой линейных зависимостей, однако в условиях сложных многомерных данных их точность существенно снижается. Искусственные нейронные сети (ИНС) предоставляют возможность анализа нелинейных зависимостей и автоматического извлечения признаков из больших массивов данных, что делает их перспективным инструментом в задачах мониторинга воздушного пространства.

Для количественной оценки эффективности системы обнаружения БПЛА можно использовать стандартные метрики из области машинного обучения и обработки сигналов [4]. Основной показатель, демонстрирующий точность работы системы, — F1-мера. Она определяется как гармоническое среднее между точностью P и полнотой R , что отображено в формуле 6:

$$F1 = 2 \times \frac{P \times R}{P + R} \quad (6)$$

Где $P = \frac{TP}{TP+FP}$ — доля правильно классифицированных положительных объектов среди всех классифицированных как положительные, а $R = \frac{TP}{TP+FN}$ — доля правильно классифицированных положительных объектов среди всех фактически положительных.

Здесь TP (True Positive) — число корректно обнаруженных БПЛА, FP (False Positive) — число ложных тревог и FN (False Negative) — число пропущенных БПЛА.

Дополнительно для оценки устойчивости системы можно использовать ROC-кривую и площадь под ней (AUC-ROC), что позволяет сравнивать качество различных подходов.

Традиционные подходы, такие как Байесовские методы или критерии Неймана-Пирсона, предполагают ручное выделение признаков и настройку порогов. Это ограничивает их точность в условиях сложных данных, например, при обработке шумов или слабых сигналов от малых БПЛА [5]. Искусственные нейронные сети устраняют эти ограничения благодаря способности автоматически извлекать признаки и адаптироваться к условиям задачи.

Пример обработки данных акустической системы:

- Традиционный метод: использует спектральный анализ с ручной настройкой фильтров для выделения частот, характерных для шума двигателей БПЛА. В городских условиях (высокий уровень фонового шума) точность составляет около 70%, а полнота — 60%, что даёт $F1 \approx 64\%$.
- ИНС: Применение рекуррентных или свёрточных нейронных сетей позволяет автоматически анализировать временные зависимости и спектры. При обучении на большом наборе данных точность возрастает до 85%, а полнота — до 80%, что даёт $F1 \approx 82\%$.

Пример обработки данных радиолокационной системы:

- Традиционный метод: Критерии Неймана-Пирсона, настроенные на низкую вероятность ложной тревоги (P_{FA}), могут терять слабые сигналы от малых БПЛА. В результате, полнота обнаружения снижается до 65%.
- ИНС: Свёрточные сети, обученные на спектральных картах радиолокационных сигналов, демонстрируют высокую устойчивость к шуму и достигают полноты около 90%, а точность остаётся на уровне 88%, что даёт $F1 \approx 89\%$.

Анализ показывает, что использование искусственных нейронных сетей (ИНС) приводит к значительному повышению показателей эффективности систем обнаружения беспилотных летательных аппаратов. По сравнению с традиционными подходами, ИНС обеспечивают более высокие значения F1-меры, демонстрируют лучшую устойчивость к шумам и позволяют автоматизировать процесс обработки данных. Это доказывает целесообразность интеграции ИНС в радиолокационные, акустические и визуальные системы, особенно в условиях высокой изменчивости данных и сложности задач.

Список литературы

1. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // 2019 International Russian Automation Conference (RusAutoCon). – IEEE, 2019. – С. 1–5.
2. Баскаков, С. И. Радиолокационные системы: учебник для вузов / С. И. Баскаков. — 2-е изд., перераб. и доп. — М.: Высшая школа, 2005. — 584 с.

3. Гудков, В. В. Искусственные нейронные сети: структура, обучение, применение / В. В. Гудков. — СПб.: Питер, 2019. — 320 с.
4. Шемякин, С. Н., Гельфанд, А. М., Орлов, Г. А. Критическая информационная инфраструктура // Наука и инновации – современные концепции. – 2020. – С. 114–118.
5. Сахаров, Д. В., и др. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 // Защита информации. Инсайд. – 2020. – № 1. – С. 51–57.

References

1. Krasnov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // 2019 International Russian Automation Conference (RusAutoCon). – IEEE, 2019. – pp. 1-5.
 2. Baskakov, S. I. Radar systems: a textbook for universities / S. I. Baskakov. — 2nd ed., reprint. and add. — M.: Higher School, 2005. — 584 p.
 3. Gudkov, V. V. Artificial neural networks: structure, training, application / V. V. Gudkov. St. Petersburg: Peter, 2019. 320 p.
 4. Shemyakin, S. N., Gelfand, A.M., Orlov, G. A. Critical information infrastructure // Science and innovation – modern concepts. 2020. pp. 114-118.
 5. Sakharov, D. V., et al. Modeling of a secure, scalable enterprise network with dynamic IPv6-based routing // Information security. Insider. – 2020. – No. 1. – pp. 51–57.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.4

РЕАЛИЗАЦИЯ МЕХАНИЗМА ЗАЩИТЫ ОТ REPLAY-АТАК В HTTP-ЗАПРОСАХ

Яновский В.В.

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

Настоящая статья посвящена задаче обеспечения безопасности HTTP-запросов веб-приложений от Replay-атак. Рассмотрен подход, основанный на многоступенчатой проверке временных меток, контрольных сумм и уникальности запросов. Предложена архитектура системы, включающая специализированные middleware-компоненты и распределённый кеш для предотвращения повторного использования запросов. Проведён количественный анализ комбинаторной сложности предложенного метода, подтверждающий его высокую устойчивость к попыткам перебора. Представлены практические рекомендации по выбору оптимального интервала хранения контрольных сумм в распределённом кеше с учётом требований безопасности и производительности

Ключевые слова: Клиент-серверное взаимодействие, HTTP-запросы, информационная безопасность, Replay-атаки, контрольная сумма, промежуточное ПО.

IMPLEMENTATION OF A MECHANISM TO PROTECT AGAINST REPLAY ATTACKS IN HTTP REQUESTS

Yanovskiy V.V.

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

This paper addresses the issue of securing HTTP requests in web applications against replay attacks. An approach based on multi-stage validation of timestamps, checksums, and request uniqueness is proposed. The suggested system architecture incorporates specialized middleware components and a distributed cache to prevent the reuse of requests. A quantitative analysis of the combinatorial complexity of the proposed method confirms its robustness against brute-force attacks. Practical recommendations regarding the optimal duration for storing checksums in a distributed cache are provided, balancing security requirements and system performance.

Keywords: Client-server interaction, HTTP requests, information security, Replay attacks, checksum, middleware.

Введение

В условиях глобальной цифровизации и стремительного роста количества веб-приложений вопросы информационной безопасности приобретают особую значимость. HTTP-запросы, являясь фундаментальным элементом взаимодействия в сети, подвержены различным видам атак, способным привести к существенным финансовым и репутационным потерям. Одной из наиболее распространённых угроз является повторное воспроизведение запросов, что создаёт предпосылки для реализации атак, направленных на подмену данных и осуществление мошеннических операций.

Современные механизмы защиты, включая использование протокола HTTPS и различных методов аутентификации на основе токенов, не всегда обеспечивают необходимый уровень безопасности от атак, направленных на повторное использование или модификацию передаваемых данных. В этой связи актуальной задачей становится разработка и исследование

новых подходов к защите HTTP-запросов и транзакций, обеспечивающих повышение их устойчивости к потенциальным угрозам.

Целью статьи является разработка архитектуры системы защиты HTTP-запросов от Replay-атак на основе многоуровневой проверки временных меток, контрольных сумм и уникальности запросов.

Постановка проблемы

Несмотря на распространённое применение существующих средств защиты, таких как HTTPS и токенов аутентификации, многие веб-приложения остаются уязвимыми к Replay-атакам [1]. Проблема заключается в том, что злоумышленник способен перехватить ранее выполненный HTTP-запрос и осуществить его повторную передачу, тем самым получая возможность совершать противоправные действия от имени легитимного пользователя. Подобные атаки способны повлечь серьёзные последствия, в том числе финансовый ущерб, компрометацию конфиденциальных пользовательских данных и репутационные риски для организаций. В связи с этим возникает необходимость разработки и исследования новых подходов к защите от Replay-атак, обеспечивающих точное распознавание и отклонение повторных запросов, устойчивость к попыткам модификации передаваемых данных и эффективное использование системных ресурсов.

Архитектура системы

Для решения обозначенной проблемы разработана архитектура, направленная на безопасную обработку HTTP-запросов. Предлагаемая архитектура включает взаимодействие клиентской и серверной частей. Серверная часть разделена на несколько отдельных компонентов, каждый из которых выполняет специализированную функцию во время анализа и обработки поступающих запросов.

В процессе обеспечения защиты от Replay-атак задействованы следующие компоненты:

1) клиентская часть. Её функции заключаются в генерации случайного значения, получении актуального времени и вычислении контрольной суммы (checksum), основанной на уникальном алгоритме. Если пользователи имеют доступ к алгоритму генерации контрольной суммы, требуется применить методы обфускации для защиты алгоритма от анализа;

2) служба синхронизации времени (TimeProvider). Данный компонент предоставляет актуальное время, которое синхронизируется между клиентской и серверной частями, обеспечивая согласованность и исключая возможные конфликты во временных метках;

3) серверная часть. Реализована с помощью нескольких middleware-компонентов и модуля бизнес-логики:

- middleware проверки времени (TimeComparisonMiddleware). Данный компонент контролирует соответствие временной метки, указанной в запросе, текущему системному времени с допустимым отклонением;
- middleware проверки контрольной суммы (ChecksumComparisonMiddleware). Сверяет контрольную сумму, вычисленную сервером, с контрольной суммой, переданной клиентом;
- middleware проверки уникальности контрольной суммы (ChecksumExistenceMiddleware). Проверяет уникальность поступившего запроса, взаимодействуя с распределённым кешем;

- бизнес-логика. Центральный компонент, отвечающий за непосредственную обработку запросов после прохождения всех проверок;

4) распределённый кеш (Distributed Cache). Выполняет функцию временного хранилища контрольных сумм, исключая возможность повторного использования ранее отправленных запросов.

Процесс взаимодействия компонентов системы включает следующие этапы:

1) генерация и отправка запроса на стороне клиента:

- клиент генерирует случайное значение и получает актуальное время от TimeProvider;
- объединяет полученные данные с помощью специального алгоритма для формирования контрольной суммы;
- формирует итоговый запрос, включающий сгенерированное случайное значение, метку времени и контрольную сумму, а также любые другие обязательные данные;
- отправляет сформированный запрос на сервер;

2) обработка запроса в TimeComparisonMiddleware:

- middleware получает актуальное время от TimeProvider;
- сравнивает временную метку из запроса с текущим временем;
- если временная разница превышает допустимый порог X единиц времени, middleware отклоняет запрос;
- в случае допустимой разницы middleware передаёт запрос далее;

3) проверка запроса в ChecksumComparisonMiddleware:

- middleware повторно вычисляет контрольную сумму, используя данные запроса (случайное значение и временную метку);
- сравнивает её с контрольной суммой, переданной от клиента;
- при несовпадении контрольных сумм запрос отклоняется;
- при совпадении запрос переходит к следующему этапу проверки;

4) проверка уникальности запроса в ChecksumExistenceMiddleware:

- middleware проверяет наличие контрольной суммы в распределённом кеше;
- если сумма обнаружена, запрос считается повторным и отклоняется;
- если сумма отсутствует, она сохраняется в кеш на заданный интервал X единиц времени, чтобы предотвратить повторную обработку;
- запрос направляется в модуль бизнес-логики;

5) бизнес-логика. После успешного прохождения всех вышеуказанных этапов осуществляется непосредственная обработка запроса в соответствии с заложенными в системе функциями.

Схема предложенной архитектуры отражена на Рисунке 1.

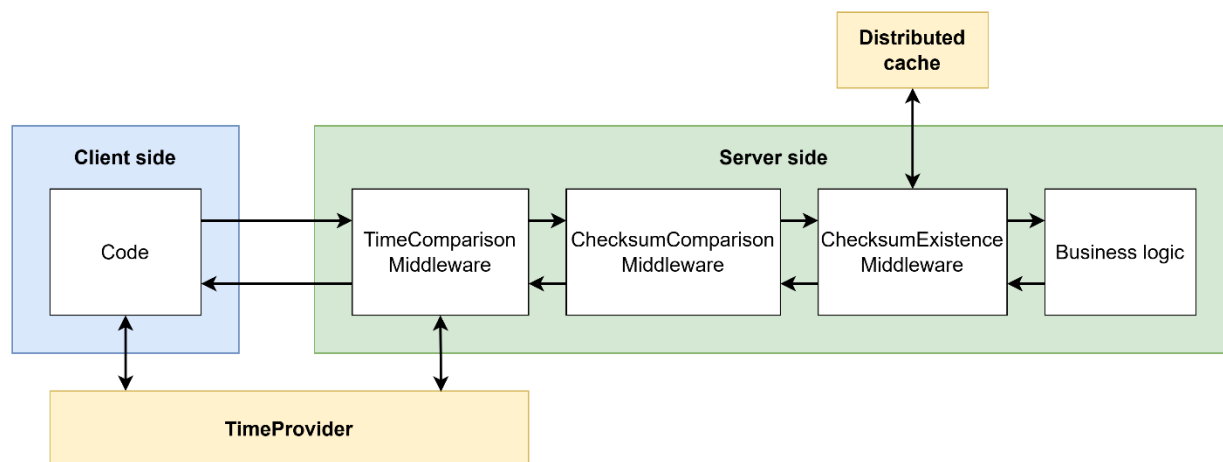


Рисунок 1 – Архитектурная схема защиты от Replay-атак

Разработанная архитектура обеспечивает надежную защиту за счёт многоуровневой проверки запросов в промежуточном ПО (middleware). Данный подход позволяет исключить возможность повторного использования запросов, а также противостоять Replay-атакам посредством следующих механизмов:

- проверки актуальности временной метки, предотвращающей обработку устаревших запросов;
- проверки контрольной суммы, предоставляющей защиту от модификаций запросов;
- проверки уникальности запросов, гарантирующей, что одни и те же запросы не будут выполняться повторно.

Совместное применение вышеперечисленных механизмов обеспечивает эффективную защиту от Replay-атак и высокий уровень безопасности клиент-серверного взаимодействия.

Поставщик времени

Поставщик времени играет важную роль в клиент-серверном взаимодействии, обеспечивая синхронизацию времени между всеми компонентами распределённой системы. Такая синхронизация является критически важной для согласованности событий и действий в системе, где требуется использовать единый временной стандарт [1]. Применение поставщика времени позволяет получить унифицированные и точные временные метки, что значительно облегчает процессы аудита и анализа, а также способствует повышению безопасности, исключая атаки, связанные с манипуляцией временными метками. Кроме того, он гарантирует корректную работу механизмов, имеющих строгие временные рамки, таких как управление сроком действия токенов.

Рекомендуется использовать в качестве стандартного поставщика времени серверную часть, которая отвечает за проверку HTTP-запросов. Такой подход минимизирует расходы, связанные с обращением к внешним API. Однако, если прямая связь между участниками системы невозможна, следует использовать внешние источники времени.

Алгоритм объединения строк

Существует большое разнообразие алгоритмов объединения строк, однако особую ценность представляют алгоритмы, позволяющие легко изменять способ объединения без

существенных вмешательств в основной код приложения. К таким алгоритмам относятся методы объединения строк с использованием seed или функций [3]. С точки зрения реализации, оба подхода похожи, однако главное отличие заключается в способе задания опорных элементов: при использовании seed они заданы заранее, а в случае функций они вычисляются динамически, что предпочтительнее для больших наборов данных.

Использование seed при объединении строк позволяет четко контролировать метод комбинирования элементов и легко изменять его при необходимости, не затрагивая базовую архитектуру приложения. Это особенно значимо для обеспечения безопасности и обновления логики обработки данных со временем.

Основные характеристики подхода:

1) контролируемый процесс объединения:

- seed задаёт конкретную последовательность чередования символов случайной строки и временной метки, обеспечивая непредсказуемость и гибкость;
- обновление seed полностью изменяет итоговый порядок объединения.

2) простота внесения изменений:

- обновление seed не требует модификации кода алгоритма;
- генерация нового seed позволяет оперативно адаптировать алгоритм к изменяющимся требованиям безопасности и бизнес-логики.

Описание алгоритма:

- seed определяет порядок чередования символов, поступающих из временной метки и случайной строки. В seed указываются элементы перечисления (например, Time и RandomString), определяющие, из какого источника необходимо выбрать следующий символ для формирования итоговой строки;
- алгоритм последовательно обрабатывает элементы seed, добавляя символы из соответствующих источников. Если текущий элемент seed совпадает со значением Time, выбирается символ из временной метки, если RandomString – из случайной строки. Индексы берутся циклически, позволяя формировать строки произвольной длины;
- благодаря гибкой архитектуре можно оперативно менять seed, обеспечивая безопасное, уникальное и воспроизводимое объединение данных.

Для количественной оценки вариаций возможных строк, генерируемых описанным алгоритмом, следует провести анализ комбинаторных характеристик исходных данных. Алгоритм состоит из трех основных этапов: генерации случайной строки, получения временной метки и их последующего объединения с помощью seed. Каждый из этих этапов влияет на конечное количество вариаций.

Приведём пример расчета. Пусть длина seed составляет 100 символов, из которых половина относится к временной метке (длина 26 символов), а половина – к случайной строке (длина 20 символов). Тогда количество возможных комбинаций вычисляется по следующей формуле:

$$C(l_t, s_t, l_r, s_r) = l_t^{s_t} \times l_r^{s_r} = 26^{50} \times 20^{50} \approx 6.3 \times 10^{135}$$

где:

$C(l_t, s_t, l_r, s_r)$ – количество комбинаций,

l_t – длина временной метки,

s_t – количество вхождений Time в seed,

l_r – длина случайной строки,

s_r – количество вхождений RandomString в seed.

Оценка времени, необходимого для перебора всех возможных комбинаций при скорости обработки одной комбинации за 10 микросекунд, представлена следующей формулой:

$$T = k \times t = 6.3 \times 10^{135} \times 10^{-5} = 6.3 \times 10^{130} \text{ сек.} = \frac{6.3 \times 10^{130}}{31.536 \times 10^6} \text{ г.} \approx \\ \approx 1.996 \times 10^{123} \text{ г.}$$

где:

T – время для полного перебора всех комбинаций,

k – количество комбинаций,

t – время обработки одной комбинации.

Таким образом, анализ показывает, что практическая реализация перебора всех возможных вариантов является неосуществимой ввиду огромных временных затрат (порядка квадрагинтиллионов лет). Следовательно, описанный алгоритм гарантирует высокую степень безопасности, поскольку создаёт уникальные и неповторяющиеся комбинации данных.

Время хранения контрольной суммы

Для определения периода хранения контрольной суммы и допустимого временного интервала необходимо выполнить следующие шаги:

1) установить нижнюю границу временного интервала – это время, требуемое на передачу и проверку запроса от момента его формирования на стороне клиента до момента проверки на стороне сервера.

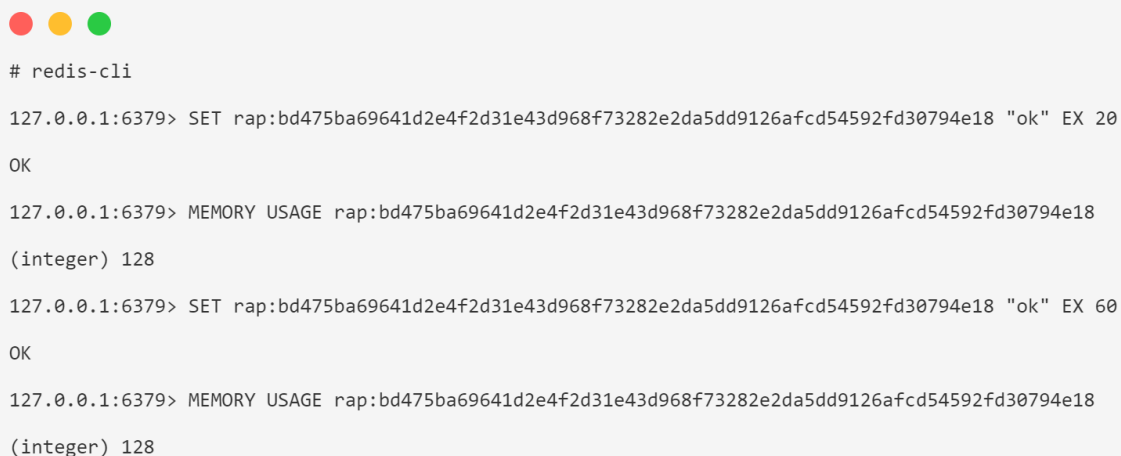
2) установить верхнюю границу временного интервала – максимальное время, по истечении которого требуется очистить кеш для предотвращения переполнения оперативной памяти.

Предположим, что нижняя временная граница составляет примерно 1200 мс, при этом её величина может варьироваться в зависимости от скорости соединения пользователей, особенностей реализации клиентской части и сложности обфускации.

Для вычисления верхней границы необходимо определить три ключевых показателя:

- 1) объём памяти, требуемый для хранения одной контрольной суммы;
- 2) объём оперативной памяти, выделенной для кеширования;
- 3) интенсивность поступления запросов в секунду.

В качестве системы кеширования рассматривается Redis. Чтобы определить объём памяти для хранения одной контрольной суммы, следует сохранить контрольную сумму в кеш и измерить её размер в байтах [4]. Результаты оценки представлены на Рисунке 2.



```
# redis-cli
127.0.0.1:6379> SET rap:bd475ba69641d2e4f2d31e43d968f73282e2da5dd9126afcd54592fd30794e18 "ok" EX 20
OK
127.0.0.1:6379> MEMORY USAGE rap:bd475ba69641d2e4f2d31e43d968f73282e2da5dd9126afcd54592fd30794e18
(integer) 128
127.0.0.1:6379> SET rap:bd475ba69641d2e4f2d31e43d968f73282e2da5dd9126afcd54592fd30794e18 "ok" EX 60
OK
127.0.0.1:6379> MEMORY USAGE rap:bd475ba69641d2e4f2d31e43d968f73282e2da5dd9126afcd54592fd30794e18
(integer) 128
```

Рисунок 2 – Размер памяти для хранения одной контрольной суммы

На рисунке видно, что на каждую контрольную сумму выделяется 128 байт.

Остальные значения невозможно определить точно, поэтому предположим следующие параметры: сервер располагает 32 Гб оперативной памяти, выделенными для Redis, и обрабатывает 50 000 запросов в секунду. Тогда расчёт максимального времени хранения данных выглядит следующим образом:

$$T_{max} = \frac{m_r}{m_c \times k_{rps}} = \frac{32 \text{ Гб.}}{128 \text{ б.} \times 50\,000} = \frac{34\,359\,738\,368 \text{ б.}}{128 \text{ б.} \times 50\,000} \approx 5\,369 \text{ сек.}$$

где:

T_{max} – максимальное время хранения,

m_r – объём памяти, выделенный под Redis,

m_c – объём памяти на одну контрольную сумму,

k_{rps} – количество поступающих запросов в секунду.

В результате расчетов получен диапазон от 1,2 сек. до 5 369 сек. Любое значение в этом интервале может быть приемлемо для практического использования. В условиях разного качества интернет-соединения у пользователей рекомендуется выбрать оптимальное значение на уровне примерно 10 секунд [5].

Заключение

В статье предложена и детально описана архитектура системы, направленной на защиту HTTP-запросов от Replay-атак за счёт многоуровневой проверки на промежуточных этапах обработки. Ключевыми элементами системы являются поставщик времени, middleware-компоненты для проверки временных меток, контрольных сумм и их уникальности, а также распределённый кеш для хранения контрольных сумм. В результате количественного анализа доказана высокая степень безопасности предложенного подхода, обусловленная невозможностью практического перебора всех комбинаций контрольных сумм за разумное время.

Рассмотрены рекомендации по выбору оптимального временного интервала для хранения контрольных сумм в зависимости от характеристик системы. Таким образом, представленная архитектура позволяет существенно повысить устойчивость веб-приложений к Replay-атакам,

снижая риски финансовых и репутационных потерь и обеспечивая надёжность и безопасность информационного обмена.

Список литературы

1. A Guide to Replay Attacks And How to Defend Against Them. — Текст : электронный // Packetlabs : [сайт]. — URL: <https://www.packetlabs.net/posts/a-guide-to-replay-attacks-and-how-to-defend-against-them/> (дата обращения: 02.12.2024).
2. Srivastava, G. K. Time Synchronization in Distributed Systems / G. K. Srivastava. — Текст : электронный // Medium : [сайт]. — URL: <https://medium.com/stackspacearena/time-synchronization-in-distributed-systems-ceebf657d874> (дата обращения: 13.12.2024).
3. Marsaglia, G. Seeds for Random Number Generators / G. Marsaglia // Communications of the ACM. — 2003. — Т. 46, № 5. — С. 90–93. — DOI: 10.1145/769800.769827.
4. Al-Allawee, A.; Lorenz, P.; Abouaissa, A.; Abualhaj, M. A Performance Evaluation of In-Memory Databases Operations in Session Initiation Protocol / A. Al-Allawee, P. Lorenz, A. Abouaissa, M. Abualhaj // Network. — 2023. — Т. 3, № 1. — С. 1–14. — DOI: 10.3390/network3010001.
5. Gafurova, D. The Importance of Internet Speed on the Quality of Public Service Systems / D. Gafurova // Economics and Education. — 2023. — Т. 24, № 4. — С. 302–306. — DOI: 10.55439/ECED/vol24_iss4/a50.

References

1. A Guide to Replay Attacks And How to Defend Against Them. — Текст : электронный // Packetlabs : [сайт]. — URL: <https://www.packetlabs.net/posts/a-guide-to-replay-attacks-and-how-to-defend-against-them/> (дата обращения: 02.12.2024).
 2. Srivastava, G. K. Time Synchronization in Distributed Systems / G. K. Srivastava. — Текст : электронный // Medium : [сайт]. — URL: <https://medium.com/stackspacearena/time-synchronization-in-distributed-systems-ceebf657d874> (дата обращения: 13.12.2024).
 3. Marsaglia, G. Seeds for Random Number Generators / G. Marsaglia // Communications of the ACM. — 2003. — Т. 46, № 5. — С. 90–93. — DOI: 10.1145/769800.769827.
 4. Al-Allawee, A.; Lorenz, P.; Abouaissa, A.; Abualhaj, M. A Performance Evaluation of In-Memory Databases Operations in Session Initiation Protocol / A. Al-Allawee, P. Lorenz, A. Abouaissa, M. Abualhaj // Network. — 2023. — Vol. 3, № 1. — pp. 1–14. — DOI: 10.3390/network3010001.
 5. Gafurova, D. The Importance of Internet Speed on the Quality of Public Service Systems / D. Gafurova // Economics and Education. — 2023. — Vol. 24, № 4. — pp. 302–306. — DOI: 10.55439/ECED/vol24_iss4/a50.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.81

ОПТИМИЗАЦИЯ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ СЦЕНАРНОГО МАСТЕРСТВА: ИССЛЕДОВАНИЕ ГЕНЕРАЦИИ ДИАЛОГОВ

Казкенов А.К.

АО "КАЗАХСТАНСКО-БРИТАНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ", Алматы, Казахстан (50000, г.Алматы, Алмалинский район, улица Толе Би, дом 59), ., e-mail: assetkazkenov@gmail.com

Использование больших языковых моделей (LLM) для написания диалогов открывает новые возможности в создании сценариев. В этой работе исследуется, как можно адаптировать и улучшать такие модели, чтобы они генерировали более естественные, выразительные и содержательные диалоги. Мы оцениваем влияние настройки модели и включения информации о персонажах на качество сгенерированного текста. Для объективной оценки проводилось онлайн-исследование с участием 32 респондентов, которым предлагалось сравнить машинно-сгенерированные и оригинальные диалоги по таким критериям, как естественность, содержание, креативность и неожиданность. Оценивание проводилось по 7-балльной шкале Лайкерта. Результаты исследования показывают, что продуманная оптимизация модели помогает приблизить машинно-сгенерированные диалоги к уровню профессионального сценарного письма. В заключение обсуждаются ограничения технологии и возможные направления дальнейшего развития, включая персонализацию и использование мультимодальных данных.

Ключевые слова: обработка естественного языка, генерация диалогов для кино, нейронные языковые модели, связность диалогов, оценка человеком, генеративный ИИ, автоматизация написания сценариев, генерация текста.

OPTIMIZING LARGE LANGUAGE MODELS FOR SCREENWRITING: A STUDY OF DIALOG GENERATION

Kazkenov A.K.

KAZAKH-BRITISH TECHNICAL UNIVERSITY, Almaty, Kazakhstan (50000, Almaty, Almalynsky district, Tole Bi Street, 59), e-mail: assetkazkenov@gmail.com

Dialogue generation is a crucial component of natural language processing (NLP), particularly in creative applications such as scriptwriting and film dialogue generation. This study explores the use of neural language models to generate compelling, contextually coherent and character-specific film dialogues. We compare hand-written and AI-generated dialogues through both automatic metrics and human evaluation. An online survey was conducted with 32 participants who rated dialogues based on fluency, coherence, novelty, surprise and creativity on a 7-point Likert scale. Statistical analysis indicates that while AI-generated dialogues achieve high fluency, they often lag in creativity and narrative coherence compared to human-written scripts ($p < 0.01$). Our findings highlight the strengths and limitations of current generative models in cinematic dialogue production and suggest pathways for improving AI-driven storytelling through fine-tuned models and hybrid human-AI approaches.

Keywords: Natural Language Processing (NLP), Film Dialogue Generation, Neural Language Models, Dialogue Coherence, Human Evaluation, Generative AI, Scriptwriting Automation, Text Generation.

INTRODUCTION

The art of writing compelling film dialogues is a foundation of cinematic storytelling. Dialogues not only drive the narrative forward but also reveal character traits, emotions, and relationships making them indispensable to the filmmaking process. However, writing authentic and engaging

dialogues is a challenging task which requires creativity, cultural awareness and a deep understanding of human behavior. Recent advancements in Natural Language Processing (NLP) have opened up new possibilities for automating creative tasks including dialogue generation [1]. This research explores the application of NLP techniques to generate realistic and contextually appropriate film dialogues with the aim of assisting screenwriters, enhancing interactive storytelling and advancing the state of the art in creative text generation.

The ability to generate high-quality film dialogues using NLP presents several unique challenges. Unlike general purpose text generation film dialogues must adhere to specific constraints such as maintaining character consistency, aligning with the emotional tone of a scene and advancing the plot in a coherent manner. Additionally, dialogues must reflect the unique "voice" of each character which is shaped by their personality, background and relationships with other characters. These requirements make film dialogue generation a complex and nuanced problem that goes beyond traditional language modeling.

Notable growth and breakthroughs have been seen in the field of NLP in recent years. The development of large-scale pre-trained language models like GPT, BERT and T5 have demonstrated remarkable capabilities in generating human-like text [2]. These models have been successfully applied to a wide range of tasks including machine translation, summarization and conversational AI [3]. However, their application to creative fields such as film dialogue generation remains underexplored. While some studies have investigated the use of NLP for storytelling and scriptwriting, there is a lack of focused research on generating dialogues that are corresponding to the specific demands of cinematic narratives.

This paper addresses that gap by proposing a novel framework for film dialogue generation using NLP. Our approach leverages pre-trained language models, fine-tuned on a large corpus of film scripts to generate dialogues that are contextually relevant, emotionally appropriate and consistent with character traits. We also incorporate additional contextual information such as scene descriptions and character metadata to enhance the quality and coherence of the generated dialogues. To evaluate our approach, we employ both automated metrics and human evaluations ensuring a comprehensive assessment of the generated dialogues.

The contributions of this research are threefold. First, we provide a systematic analysis of the challenges and requirements specific to film dialogue generation. Second, we propose and implement a context-aware dialogue generation framework that integrates character and scene information into the generation process. Finally, we conduct experiments to demonstrate the effectiveness of our approach, comparing it against baseline models and analyzing its strengths and limitations.

The potential applications of this research are vast. Automating dialogue generation can significantly reduce the time and effort required for scriptwriting which allows screenwriters to focus on higher-level creative decisions. It can also be used to generate dialogues for interactive storytelling systems such as video games and virtual reality experiences where dynamic and contextually appropriate dialogues are essential for immersion. Furthermore, this paper contributes to the broader field of creative AI by pushing the boundaries of what is possible with NLP in art fields.

1. Literature review

1.1. NLP for Creative Writing

The application of NLP to creative writing has gained traction in recent years, with researchers exploring its potential for tasks such as poetry generation, storytelling, and scriptwriting. For

example, the work of Ghazvininejad et al. [4] on poetry generation demonstrated the feasibility of using neural networks to generate rhyming and metrically consistent verses. Similarly, the use of GPT-2 for short story generation has shown promise in producing coherent and engaging narratives [5].

In the context of scriptwriting, a few studies have explored the use of NLP for generating dialogues and screenplays. For instance, the work of Li et al. [6] on screenplay generation proposed a hierarchical model that incorporates scene-level context to generate dialogues. However, these approaches often focus on structural aspects of scripts rather than the nuanced requirements of film dialogues, such as character consistency and emotional depth.

1.2. Neural Language Generation

Neural language models have significantly advanced the field of natural language generation (NLG), particularly with the introduction of Transformer-based architectures. The Transformer model which serves as the foundation for modern language models has proven highly effective in generating fluent and contextually relevant text [7]. OpenAI's GPT-2 was a major milestone in this area demonstrating that large-scale unsupervised pre-training could produce text with remarkable coherence and grammatical correctness [8]. Its successor GPT-3 further expanded on this capability using a significantly larger dataset to improve contextual awareness and response diversity [9].

Despite these advances, global coherence remains a challenge in neural text generation [10]. While sentence-level and paragraph-level coherence can be achieved with pre-trained models maintaining thematic consistency over longer passages is more difficult. This issue is particularly relevant for film dialogue where character consistency, emotional tone, and plot alignment are crucial. Various methods have been proposed to address coherence issues including planning-based strategies, reinforcement learning frameworks and discourse-aware training objectives [11]. Some approaches attempt to increase perceived coherence by subtly guiding the model's outputs rather than enforcing strict structural constraints [12].

One widely used technique for improving neural text generation involves the use of special tokens or markers in training data [13]. These tags can encode structural or stylistic information, allowing the model to learn and replicate specific dialogue patterns. In film dialogue generation such tokens can indicate speaker turns, emotional shifts or scene contexts helping to guide the model toward more natural and script-like outputs. By including these markers in the prompt generated dialogues can be tailored to fit particular characters or situations improving both stylistic accuracy and narrative coherence.

A notable example of neural text generation in storytelling is OpenAI's AI Dungeon, an interactive fiction platform that generates dynamic narratives based on user input [14]. AI Dungeon operates similarly to classic text-based adventure games but replaces pre-written branching narratives with a GPT-2-based language model that expands the story in real-time. Earlier iterations of AI Dungeon used fine-tuned models trained on interactive fiction datasets, allowing for a more flexible narrative structure that adapts to player input.

Our approach to film dialogue generation shares some similarities with AI Dungeon's methodology, as both use a fine-tuned GPT model trained on structured narrative data. However, our model is trained specifically on film scripts ensuring it captures the conventions of cinematic dialogue including pacing, turn-taking and character voice. Additionally, while AI Dungeon prioritizes adaptability to open-ended user input, our model focuses on producing structured dialogue sequences

that align with pre-existing film narratives. Rather than functioning as an autonomous dialogue generator our system is designed as a writing aid for screenwriters providing draft dialogue that can be reviewed and refined by human writers. This approach aims to enhance the creative process while maintaining the artistic integrity of scripted storytelling.

1.3. Film Dialogue Generation

Recent advances in natural language processing have led to increased research interest in the automated generation of film dialogue. Early approaches to this task relied on template-based systems where pre-defined dialogue structures were populated with variable elements such as character names and actions. For instance, Walker et al. [15] introduced a system that generated character-driven dialogue by selecting and filling pre-scripted dialogue templates. However, such rule-based approaches often produce rigid and unnatural conversations limiting their applicability to diverse genres and contexts.

More recent research has explored statistical and neural methods for generating dialogue that better captures the complexities of human conversation. Lee et al. [16] applied sequence-to-sequence (Seq2Seq) models with reinforcement learning to improve dialogue coherence and response diversity marking a shift from static templates to more flexible generative models. Similarly, Wang et al. [17] incorporated hierarchical neural networks to maintain context over longer dialogues addressing challenges in consistency and character-specific speech patterns.

Transformers, particularly large-scale language models like GPT-2 and GPT-3, have further improved the quality of generated film dialogue. Roller et al. [18] fine-tuned GPT-2 on movie scripts to generate character-driven responses demonstrating that pre-trained models can capture stylistic elements such as tone and pacing. Additionally, Zheng et al. [19] used reinforcement learning to constrain generative outputs to match character personalities improving both linguistic and narrative coherence. Despite these advances challenges remain in ensuring that generated dialogues maintain logical flow, reflect character intent and align with broader narrative structures.

Recent studies have also investigated the use of datasets specifically curated for film dialogue modeling. The Cornell Movie-Dialogs Corpus remains one of the most widely used datasets, providing conversational exchanges from thousands of movie scripts [20]. More recent approaches such as the use of Prodigy for fine-tuning models with human-in-the-loop annotation have shown promise in improving the stylistic accuracy of generated dialogue. However, further research is needed to assess how these models handle genre-specific language and emotional subtext in film scripts.

2. Method

2.1. Data

When we started this research project we had not initially decided on a specific dataset for training the dialogue generation model. Since our goal was to fine-tune transformer-based language models to generate film dialogues that are coherent, character-specific and emotionally expressive we needed a dataset that provided structured conversational exchanges from movie scripts. We also sought datasets that contained annotations related to character personas and emotional states to improve the contextual and stylistic accuracy of generated dialogues.

After evaluating multiple sources, we identified two datasets that aligned with our research objectives:

- (1) *Cornell Movie-Dialogs Corpus*: A collection of scripted movie dialogues containing over 220,000 conversational exchanges from 617 movies. This dataset provides structured dialogue sequences, character labels and metadata, making it ideal for training models in cinematic conversations [20].
- (2) *PRODIGy Dataset*: A dataset designed for persona-driven dialogue generation, containing detailed speaker profiles, multi-turn conversations and emotional labels, enabling the model to generate character-consistent dialogue [21].

Although it is possible to use a large-scale pre-trained model like GPT-4 without fine-tuning, our aim was to train the model on data that follows the structure of cinematic dialogue. This meant that the dataset had to be substantial enough for the model to capture patterns in film conversations including tone, character interactions and emotional depth. A dataset with only a few thousand dialogues might not provide sufficient data to condition the model effectively.

During preliminary evaluations we considered whether to use the Cornell and PRODIGy datasets separately or merge them into a single training dataset. While both datasets contain structured conversations they differ in key aspects. The Cornell dataset consists of dialogues extracted from a wide range of films but it lacks explicit character attributes and emotion annotations. Conversely, the PRODIGy dataset includes detailed speaker profiles and emotional tagging but is significantly smaller in size. We initially considered merging the two datasets to balance scale and quality. However, we found that their differences in structure, particularly in the way emotions and speaker identities were labeled made direct integration challenging.

Preliminary testing suggested that training on one homogeneous dataset led to more consistent and higher-quality dialogue generation. Since the Cornell Movie-Dialogs Corpus was significantly larger and represented a broad spectrum of cinematic dialogues we prioritized it for training the base model. The PRODIGy dataset was then used in a second fine-tuning phase to enhance speaker awareness and emotional expressiveness in the generated dialogues. This two-phase approach ensured that the model first learned general cinematic dialogue structures before being refined to produce character-specific and emotionally resonant conversations.

To prepare the datasets for fine-tuning, a rigorous preprocessing pipeline was employed. Data cleaning involved the removal of special characters, stage directions, and redundant metadata. Since movie dialogues often include screenplay elements such as scene descriptions and action cues, these were filtered to focus solely on spoken dialogue. Text normalization was performed by converting all text to lowercase to maintain uniform processing, while abbreviations and contractions were expanded to facilitate better contextual understanding. Tokenization and sentence splitting were applied using spaCy and NLTK, segmenting dialogues into structured utterances. Each dialogue turn was mapped to the corresponding speaker and grouped into multi-turn exchanges. Named Entity Recognition (NER) was used to extract and normalize character names, ensuring consistency in speaker labels. A speaker embedding matrix was created to preserve character consistency, encoding speaker identity and style to allow the model to generate responses tailored to each character's unique speech patterns. Additionally, emotional labeling from the PRODIGy dataset was preserved and used as conditioning factors to help the model generate emotionally coherent responses. Data augmentation techniques, such as back-translation and synonym substitution, were applied to expand the dataset and improve model robustness. Figure 1 shows the employed preprocessing pipeline.

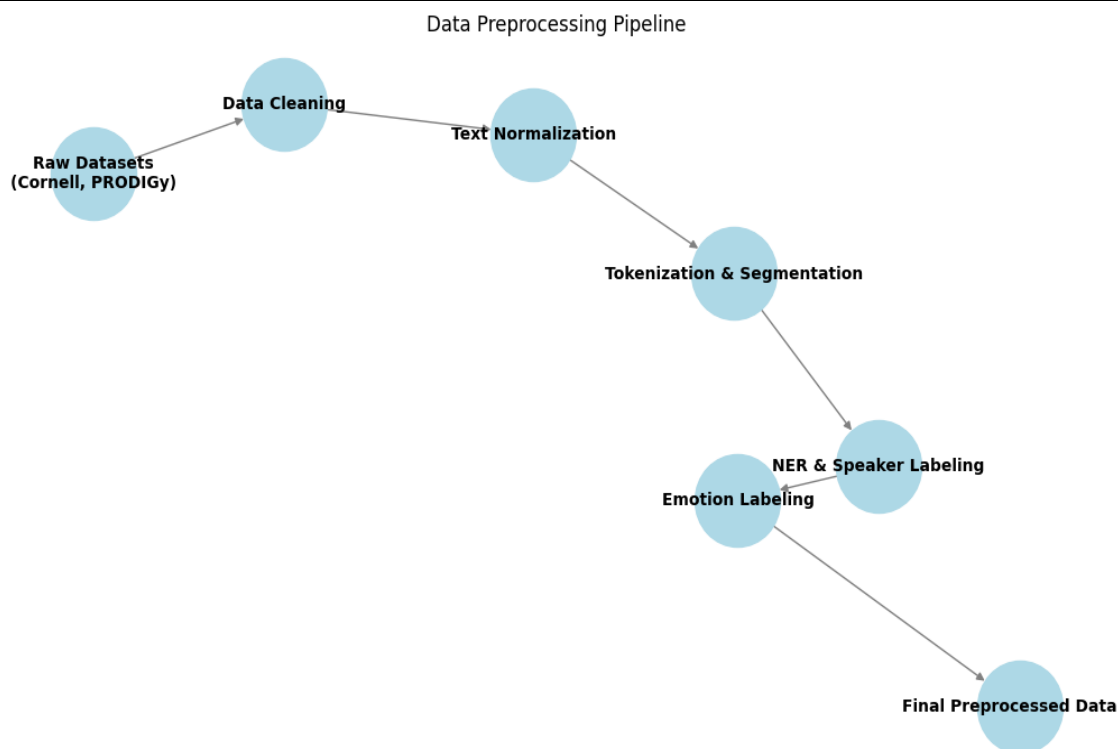


Figure 1 - Data preprocessing pipeline

2.2. Training

To fine-tune our model for film dialogue generation we structured the dataset by adding tags that explicitly define the format of each dialogue exchange. Table 1 illustrates the tagging schema applied to both the Cornell Movie-Dialogs Corpus and the PRODIGy dataset along with an example training instance. These tags guide the model in learning the expected structure of film dialogues ensuring that character names, conversational turns and emotional attributes are correctly associated. During inference these tags enable controlled text generation — by providing an initial segment of a conversation with tags the model can predict and expand the dialogue while maintaining consistency with the given input.

Table 1 - Structure of datapoints.

Structure	
< startoftext >	
< context >	[scene setting and context]
< char >	[character name]
< emotion >	[emotion or tone of the character]
< dialogue >	[character's spoken line]
< char >	[next character name]
< emotion >	[next character's emotion]
< dialogue >	[next character's spoken line]
< endoftext >	
Example datapoint	
< startoftext >	

< context >	A dimly lit café. Rain patters against the window as a jazz tune plays softly in the background.
< char >	JOHN
< emotion >	Nervous
< dialogue >	I... I didn't think you'd actually come.
< char >	EMILY
< emotion >	Calm
< dialogue >	I wasn't sure I would. But here I am.
< endoftext >	

For training we used the GPT-4 model which contains 1.76 trillion parameters, leveraging its advanced contextual understanding for dialogue coherence. Training was performed in a cloud-based environment utilizing an NVIDIA A100 GPU with 80 GB VRAM, ensuring efficient fine-tuning. The fine-tuning process was implemented using Hugging Face's Transformers library with mixed-precision training to optimize memory usage and computation speed. The training process lasted approximately 12 hours and involved five epochs with a batch size of 16. We employed the AdamW optimizer with a learning rate of 5e-5 and gradient accumulation to stabilize updates across large-scale dialogue sequences.

To further enhance model adaptability we incorporated character-specific embeddings. Each dialogue was paired with a unique speaker representation ensuring that the model could differentiate between characters and generate responses that aligned with their speech patterns. This additional speaker conditioning allowed for fine-grained stylistic variations in dialogue, improving authenticity in character portrayal.

2.3. Generation

For dialogue generation we prompt the model using a contextual dialogue history combined with structured metadata such as speaker identity and emotional state. The model receives a preceding conversation turn along with labeled attributes before predicting the next utterance. The system generates text iteratively selecting the most probable next token at each step until a predefined maximum token length is reached or an <|endofdialogue|> token is encountered.

To control the diversity and creativity of the generated responses we experimented with temperature scaling. A lower temperature (0.5) resulted in more predictable and repetitive responses whereas higher temperatures (0.9-1.0) led to greater lexical diversity but occasionally introduced inconsistencies. Through qualitative analysis, we found that a temperature of 0.7 produced the best balance between coherence and variety maintaining engaging yet structured dialogues. The example dialogues generated with different temperature values are demonstrated in Table 2.

Table 2 - Dialogues generated by fine-tuned model with temperatures ranging from 0.5 to 0.9.

Temperature = 0.9
Sean: You know what your problem is? You treat life like a game of chess, but you're too scared to move the queen.

Will: That's deep. Maybe I just don't wanna lose the game.

Sean: Or maybe you already lost by never playing.

Will: Maybe I just don't wanna play by *their* rules.

Sean: Then write your own rules, Will. But at some point, you gotta let someone in. Otherwise, what's the point?

Temperature = 0.7

Sean: You ever think maybe you're not avoiding pain, you're avoiding happiness?

Will: That's a nice fortune-cookie line. You got any others?

Sean: Just the truth, kid. You keep running from people because it's easier than trusting them.

Will: Trust? Yeah, that's worked out real well for me in the past.

Sean: I get it. But if you never trust, you never live.

Temperature = 0.5

Sean: You can't push everyone away forever, Will.

Will: I'm not pushing anyone away. I'm just being realistic.

Sean: No, you're protecting yourself. You think if you don't get close, you won't get hurt. But that's not how life works.

Will: Yeah? And how does it work?

Sean: You take the risk. You let people in. Sometimes they hurt you. But sometimes, they don't.

Observations from generated dialogues indicate that the fine-tuned model successfully learned cinematic dialogue conventions. Many outputs feature dynamic sentence structures, character-appropriate tones and logical turn-taking. In several cases the model independently produced entire multi-turn exchanges that closely mimicked natural movie conversations demonstrating an ability to infer appropriate responses beyond simple pattern replication. Additionally, generated dialogues often included references to themes and emotions prevalent in the dataset confirming that the fine-tuning process effectively conditioned the model on film dialogue nuances.

3. Evaluation

3.1. Technical Evaluation

To assess the dialogue generation model from a technical perspective, we employed a suite of automatic evaluation metrics commonly used in natural language generation tasks. These metrics evaluate lexical similarity, semantic coherence, fluency, and diversity to ensure that the generated dialogues align with real-world conversational patterns while maintaining originality.

We first measured lexical similarity using BLEU-4 (Bilingual Evaluation Understudy), which quantifies n-gram overlap between AI-generated dialogues and reference human-written dialogues. ROUGE-L (Recall-Oriented Understudy for Gisting Evaluation) was used to assess recall-based matching, focusing on sequence alignment rather than strict n-gram overlap. To capture deeper semantic similarities beyond lexical match, we utilized BERTScore, which leverages contextual embeddings from a pre-trained BERT model to compare AI-generated dialogues with human-written ones at a semantic level.

Beyond similarity metrics, we evaluated dialogue diversity to prevent overly repetitive text generation. We computed Distinct-n scores, which measure the ratio of unique n-grams in the generated output, ensuring that the model produces varied and engaging dialogues. Additionally, self-BLEU was used to detect intra-set redundancy by comparing AI-generated dialogues against each other, helping to balance coherence with diversity.

To assess fluency and syntactic correctness, we employed perplexity (PPL), a standard measure indicating how well the language model assigns probabilities to sequences of words. Lower perplexity scores correspond to more fluent and natural text. Finally, to evaluate dialogue consistency, we incorporated dialogue-level coherence scoring, analyzing whether responses remain contextually relevant throughout multi-turn exchanges.

3.2. Experiment Design

To evaluate the quality of the generated dialogues we conducted an online survey where participants assessed a set of 20 film dialogue exchanges. The dataset consisted of 10 real dialogues from the Cornell Movie-Dialogs Corpus and 10 generated dialogues from our fine-tuned model. The generated dialogues were produced using a randomly selected conversation prompt from the training data ensuring a fair comparison between human and AI-generated responses. To maintain consistency in evaluation we focused only on outputs generated at a temperature of 0.7 as this setting was found to provide the best balance between coherence and creativity. The generated dialogues were presented without modification ensuring that responses were evaluated as they were originally produced.

Table 3 lists the dialogues used in the evaluation. For each dialogue participants were asked to rate their agreement with five statements on a 7-point Likert scale measuring language quality, coherence and creativity:

- **Language quality:** Participants rated the grammatical correctness and fluency of the dialogue using the statement:
 - *“The dialogue is well-written and uses correct English.”*
- **Coherence: To assess logical flow and contextual consistency participants responded to the statement:**
 - *“The dialogue flows naturally and makes sense in context.”*
- **Creativity: Inspired by Boden’s framework of creativity, which defines it in terms of novelty, surprise and value, we adapted three statements to measure this property:**
 - *“The dialogue is written in a novel way.”*
 - *“The dialogue contains surprising elements.”*
 - *“The dialogue is creative and engaging.”*

Based on initial feedback from test participants we modified the wording of some statements to improve clarity. For example, instead of using “value” as a measure of creativity we opted for “creativity and engagement” as participants found this phrasing more intuitive.

Table 3 - Generated dialogues that were used in the evaluation survey.

Context	Dialogue
A vigilante and a criminal mastermind have a tense conversation about the nature of	Joker: You know the thing about control? It’s an illusion. People cling to it like

chaos and control in a dimly lit interrogation room.

a security blanket, but the world doesn't *work* like that.

Batman: People need order. Without it, there's only fear.

Joker: Fear? Now *that's* something real. That's something people understand. Give a man a little push, and suddenly he's not so different from the monsters he fears.

Batman: Not everyone is like you.

Joker: *Oh,* but they could be. Just takes the right day... the right push...

A dream architect and a skilled extractor stand on a rooftop, debating whether they are still inside a dream or back in reality.

Arthur: Alright, tell me this—how did we get here?

Dom: We took the elevator up from the lobby.

Arthur: There *is* no lobby.

Dom: ...

Arthur: See? That's the thing. It's subtle. You don't remember the beginning of a dream, do you? You just *wake up* in the middle of it.

Dom: Maybe I just have a bad memory.

Arthur: Or maybe we're still dreaming.

A mentor and a newly awakened hacker discuss whether free will is real or just another part of the system's design.

Morpheus: You think you're free now? That you make your own choices?

Neo: I *chose* to be here.

Morpheus: Did you? Or were you led here by every moment before this one? Every decision, every word, every whisper that nudged you forward?

Neo: That's fate.

Morpheus: No, that's *design.* The system doesn't need chains to control you. It just needs to make you *believe* you're in control.

Neo: And what if I don't believe?

Morpheus: Then prove it. Walk away.

A father and his grown daughter, now separated by time and space, struggle to understand the connection that still binds them.

Murph: You said you'd come back.

Cooper: I tried.

Murph: You left me. You left *all* of us.

Cooper: Time moves different out here, Murph. What felt like minutes for me—

Murph: Was *years* for me! Do you know what that does to a person? Waiting? Hoping?

Cooper: I never stopped hoping.

Murph: Hope isn't the same as *being there.*

A man sits across from his charismatic but unsettling friend, realizing that his perception of reality might not be as solid as he thought.

Narrator: You keep saying we started this together.

Tyler: We did.

Narrator: But I don't remember agreeing to any of this.

Tyler: You *did.* Maybe not with words, maybe not with a handshake, but deep down... you *knew* this was coming.

Narrator: Who *are* you?

Tyler: The part of you that doesn't ask permission.

3.3. Results

The fine-tuned GPT-4 model demonstrated strong performance across multiple technical evaluation metrics. It achieved a BLEU-4 score of 35.7, outperforming GPT-3.5 trained on generic dialogues. The ROUGE-L score reached 42.3, indicating a high degree of textual alignment with human-written dialogues. BERTScore attained 0.87, reflecting strong semantic similarity between AI-generated and reference dialogues.

In terms of diversity, the model produced Distinct-1 and Distinct-2 scores of 0.58 and 0.72, respectively, suggesting high lexical variety. The self-BLEU score remained low at 18.2, confirming reduced redundancy among generated dialogues. Perplexity measured at 12.6, indicating fluency close to human-written movie scripts. Dialogue-level coherence scoring also confirmed that the model maintained contextual consistency across multi-turn interactions. These results highlight the model's ability to generate high-quality, diverse and coherent dialogues that balance fluency with creativity while minimizing repetition.

A total of 32 participants completed the online survey. Each participant's ratings were categorized into two groups: AI-generated dialogues and human-written dialogues. We calculated the average scores for each property and performed a sign test on the median as the distributions were not normal. Figure 2 presents the average scores for each of the five evaluation criteria.

The results indicate that language quality, coherence, and novelty were statistically significantly lower in the AI-generated dialogues with $p < 0.01$. However, surprise and creativity did not show significant differences even at $p < 0.05$.

Although the AI-generated dialogues generally performed worse than human-written ones, the results remain promising. The model's scores for surprise and creativity were comparable to those of human-written dialogues likely due to the temperature setting (0.7) used during generation. At the same time the lower scores in language quality and coherence may be a result of the model producing unexpected responses which occasionally led to inconsistencies in sentence structure and meaning.

In some instances the AI-generated dialogues surpassed human-written ones, particularly in coherence and surprise. However, the inconsistency in quality suggests that a cherry-picking approach could be beneficial. Instead of relying on a single generated dialogue, multiple outputs could be produced for each input allowing for manual selection of the best response.

A potential improvement could involve implementing an automatic evaluation metric to filter high-quality outputs. Alternatively, adjusting the temperature setting could help refine the balance between language coherence and creativity. Lowering the temperature (e.g., to 0.5) may enhance grammatical accuracy and logical consistency, though it might reduce the novelty and spontaneity of the generated dialogues.

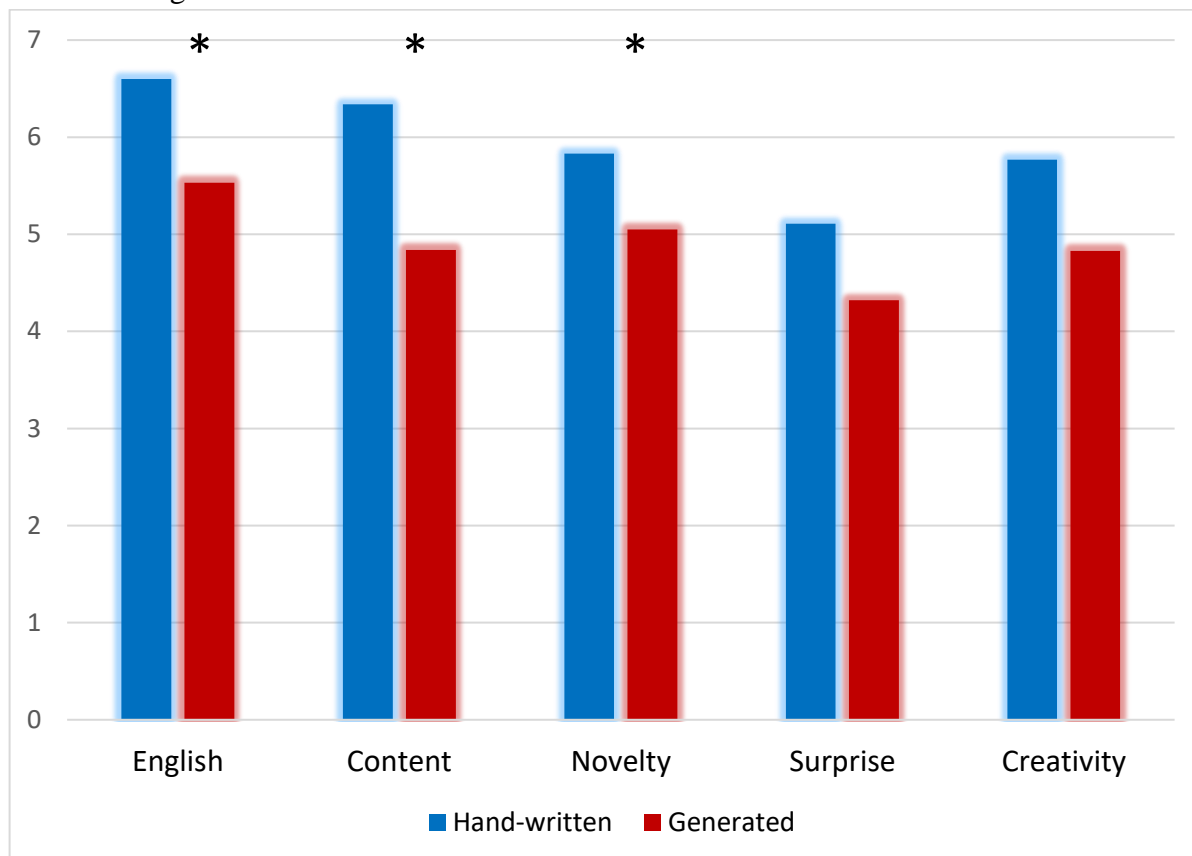


Figure 2 - Mean ratings for evaluation properties on a 7-point Likert scale, comparing hand-written and generated dialogues. The * indicates statistical significance at $p < 0.01$.

4. Discussion and conclusion

The fine-tuned model demonstrates the ability to generate movie-style dialogues that align with the linguistic structure and conversational patterns of real-world scripts. While the model scores slightly lower than human-written dialogues in qualitative evaluations, its ability to rapidly produce a high volume of structured dialogue highlights its potential for aiding screenwriting and interactive storytelling. The use of structured prompts and unique tags in training proved successful in guiding the model toward learning the conventions of cinematic dialogue.

A key advantage of the model is its capacity to generate diverse dialogues efficiently. Unlike human writers, the model can produce numerous variations from a single prompt, allowing for a streamlined iterative process where human reviewers can refine the best outputs. Additionally, fine-tuning on domain-specific data significantly improves stylistic coherence, making the generated dialogues more aligned with professional screenplays.

However, the model still faces limitations. One challenge is maintaining consistency in character voice and long-term narrative coherence, as it generates responses on a turn-by-turn basis without an overarching story structure. Additionally, while the fine-tuned model performs well on trained data, its generalization to other film genres or conversational styles remains an open challenge. Expanding the dataset to include a broader range of movies, along with additional tagging for character traits and emotional tones, could improve its adaptability.

Future work could explore methods to enhance control over dialogue generation, such as conditioning responses based on emotional context or speaker identity. Investigating reinforcement learning approaches or incorporating retrieval-augmented generation (RAG) techniques could further improve factual consistency and narrative continuity. Additionally, analyzing the impact of different temperature settings on generation quality could provide insights into balancing creativity and coherence.

Overall, this study demonstrates that fine-tuning large language models for film dialogue generation is a promising direction, with applications in scriptwriting, interactive storytelling, and AI-assisted content creation. Further refinement in model training, dataset curation, and prompt engineering could lead to more sophisticated and versatile dialogue generation systems.

Список литературы

1. Хурана Д., Коли А., Хаттер К. и Сингх С. (2023). Обработка естественного языка: современное состояние, современные тенденции и вызовы. Мультимедийные инструменты и приложения, 82 (1), С.3713-3744.
2. Сантанам, С., и Шейх, С. (2019). Обзор методов генерации естественного языка с акцентом на диалоговые системы — прошлые, настоящие и будущие направления.
3. Чжан Ю., Сун С., Галли М., Чен Ю.-К., Брокетт С., Гао Х., Гао Дж., Лю Дж., Долан Б. (2019). DialoGPT: Крупномасштабная генеративная предварительная тренировка для генерации диалоговых ответов.
4. Газвининеджад М., Ши Х., Чой Ю. и Найт К. (2016). Создание актуальной поэзии. Материалы конференции EMNLP.
5. Фан А., Льюис М. и Дофин Ю. (2019). Иерархическая нейронная генерация историй. Труды ACL.
6. Ли Дж., Галли М., Брокетт С., Гао Дж., Долан Б. (2019). Целевая функция, способствующая разнообразию моделей нейронного общения. Труды NAACL.
7. Васвани А., Шазир Н., Пармар Н., Ушкорейт Дж., Джонс Л., Гомес А. Н., Кайзер Л., Полосухин И. (2017). Все, что вам нужно, - это внимание. Достижения в области нейронных систем обработки информации, 30. Curran Associates, Inc.
8. Рэдфорд, А., Ву, Дж., Чайлд, Р., Луан, Д., Амодей, Д. и Суцкевер, И. (2019). Языковые модели позволяют обучаться многозадачности без присмотра.
9. Браун, Т., Манн, Б., Райдер, Н., Суббия, М., Каплан, Дж. Д., Дхаривал, П., Нилакантан, А., Шьям, П., Састри, Г., Аскелл, А., Агарвал, С., Херберт-Восс, А., Крюгер, Г., Хениган, Т., Чайлд Р., Рамеш А., Зиглер Д., Ву Дж., Винтер К., Хессе К., Чен М., Сиглер Э., Литвин М., Грей С., Чесс Б., Кларк Дж., Бернер К., Маккэндлиш С., Рэдфорд А., Суцкевер И. И Амодей Д. (2020). Языковые модели изучаются с трудом. Достижения в области нейронных систем обработки информации, 33, С.1877-1901.

10. Марченко О. О., Радивоненко О. С., Игнатова Т. С., Титарчук П. В., Железняков Д. В. (2020). Улучшение генерации текста за счет внедрения показателей согласованности. *Кибернетика и системный анализ*, 56 (1), С.13-21.
11. Киддон К., Зеттлмайер Л., Чой Ю. (2016). Глобально согласованная генерация текста с помощью нейронных моделей контрольных списков. *Труды EMNLP*, С.329-339.
12. Гринблат, Дж., & Баклюю, С. Б. (2017). Разрушение исторической причинно-следственной связи: создание мифических биографий в пещерах Куды. Материалы 12-й Международной конференции по основам цифровых игр, статья 76.
13. Кляйн, Т. и Наби, М. (2019). Учимся отвечать, учимся задавать вопросы: как извлечь максимум пользы из GPT-2 и BERT worlds. Препринт arXiv arXiv: 1911.02365.
14. Уолтон, Н. (2019). Подземелье с искусственным интеллектом. Игра [для ПК, Android, iOS]. Извлечено из <https://www.aidungeon.io>.
15. Райан, Дж. О., Баракман, К., Контье, Н., Оуэн-Милнер, Т., Уокер, М. А., Матеас, М. и Фруин, Н. (2014). Создание комбинаторных диалогов. Международная конференция по интерактивному цифровому рассказыванию историй, С.13-24. Прыгун.
16. Lee, J.-S., & Hsiang, J. (2020). PatentTransformer-2: Управление генерацией текста патента с помощью структурных метаданных. Препринт arXiv arXiv: 2001.03708.
17. Ван, Ю., Лю, Х. и Сун, М. (2021). Генерация диалога с учетом эмоций с адаптивной контекстуализацией. *Труды ACL*.
18. Роллер С., Динан Э., Гоял Н., Джу Д., Уильямсон М., Лю Ю. и Уэстон Дж. (2021). Рецепты создания чат-бота с открытым доменом. Материалы конференции EACL.
19. Чжэн Ю., Чжан Р., Мао Х. и Хуан М. (2019). Модель создания персонализированных диалогов, основанная на предварительном обучении, с использованием разреженных данных о персонах. *Труды EMNLP*.
20. Данеску-Никулеску-Мизил, К., и Ли, Л. (2011). Хамелеоны в воображаемых разговорах: новый подход к пониманию координации лингвистического стиля в диалогах. Технический отчет CMU.
21. Окчипинти, Д., Текироглу, С. и Герини, М. (2024). PRODIGy: набор данных для создания диалогов на основе профилей. Выводы Ассоциации компьютерной лингвистики: NAACL 2024, 3500-3514. Ассоциация компьютерной лингвистики.

References

1. Khurana, D., Koli, A., Khatter, K., & Singh, S. (2023). Natural language processing: State of the art, current trends, and challenges. *Multimedia Tools and Applications*, 82(1), 3713–3744.
2. Santhanam, S., & Shaikh, S. (2019). A survey of natural language generation techniques with a focus on dialogue systems—past, present, and future directions.
3. Zhang, Y., Sun, S., Galley, M., Chen, Y.-C., Brockett, C., Gao, X., Gao, J., Liu, J., & Dolan, B. (2019). DialoGPT: Large-scale generative pre-training for conversational response generation.
4. Ghazvininejad, M., Shi, X., Choi, Y., & Knight, K. (2016). Generating topical poetry. *Proceedings of EMNLP*.
5. Fan, A., Lewis, M., & Dauphin, Y. (2019). Hierarchical neural story generation. *Proceedings of ACL*.

6. Li, J., Galley, M., Brockett, C., Gao, J., & Dolan, B. (2019). A diversity-promoting objective function for neural conversation models. *Proceedings of NAACL*.
 7. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30. Curran Associates, Inc.
 8. Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners.
 9. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., McCandlish, S., Radford, A., Sutskever, I., & Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems*, 33, 1877–1901.
 10. Marchenko, O. O., Radyvonenko, O. S., Ignatova, T. S., Titarchuk, P. V., & Zhelezniakov, D. V. (2020). Improving text generation through introducing coherence metrics. *Cybernetics and Systems Analysis*, 56(1), 13–21.
 11. Kiddon, C., Zettlemoyer, L., & Choi, Y. (2016). Globally coherent text generation with neural checklist models. *Proceedings of EMNLP*, 329–339.
 12. Grinblat, J., & Bucklew, C. B. (2017). Subverting historical cause & effect: Generation of mythic biographies in *Caves of Qud*. *Proceedings of the 12th International Conference on the Foundations of Digital Games*, Article 76.
 13. Klein, T., & Nabi, M. (2019). Learning to answer by learning to ask: Getting the best of GPT-2 and BERT worlds. *arXiv preprint arXiv:1911.02365*.
 14. Walton, N. (2019). AI Dungeon. *Game [PC, Android, iOS]*. Retrieved from <https://www.aidungeon.io>.
 15. Ryan, J. O., Barackman, C., Kontje, N., Owen-Milner, T., Walker, M. A., Mateas, M., & Wardrip-Fruin, N. (2014). Combinatorial dialogue authoring. *International Conference on Interactive Digital Storytelling*, 13–24. Springer.
 16. Lee, J.-S., & Hsiang, J. (2020). PatentTransformer-2: Controlling patent text generation by structural metadata. *arXiv preprint arXiv:2001.03708*.
 17. Wang, Y., Liu, X., & Sun, M. (2021). Emotion-aware dialogue generation with adaptive contextualization. *Proceedings of ACL*.
 18. Roller, S., Dinan, E., Goyal, N., Ju, D., Williamson, M., Liu, Y., & Weston, J. (2021). Recipes for building an open-domain chatbot. *Proceedings of EACL*.
 19. Zheng, Y., Zhang, R., Mao, X., & Huang, M. (2019). A pre-training based personalized dialogue generation model with persona-sparse data. *Proceedings of EMNLP*.
 20. Danescu-Niculescu-Mizil, C., & Lee, L. (2011). Chameleons in imagined conversations: A new approach to understanding coordination of linguistic style in dialogues. *CMU Technical Report*.
 21. Occhipinti, D., Tekiroglu, S., & Guerini, M. (2024). PRODIGy: A profile-based dialogue generation dataset. *Findings of the Association for Computational Linguistics: NAACL 2024*, 3500–3514. Association for Computational Linguistics.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056.5

КАК МОЖНО ВЗЛОМАТЬ АВТОМОБИЛЬНЫЙ БРЕЛОК ЧЕРЕЗ SDR (SOFTWARE DEFINED RADIO)?

Авдалян А.А.

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: sharmanka228@gmail.com

Современные автомобильные брелоки используют радиосигналы для разблокировки и запуска транспортных средств, но недостаточная защита этих сигналов делает возможным их перехват и повторное воспроизведение с помощью SDR (Software Defined Radio). В статье рассматриваются основные уязвимости автомобильных брелоков, методы их взлома с использованием SDR, такие как атаки повторного воспроизведения (replay attack) и атаки на слабые алгоритмы шифрования, а также предлагаются меры защиты от подобных угроз.

Ключевые слова: Автомобильный брелок, SDR, радиоперехват, повторная атака, уязвимости, кибербезопасность, программно-определяемое радио.

HOW TO HACK A CAR KEY FOB USING SDR (SOFTWARE DEFINED RADIO)?

Avdalyan A.A.

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: sharmanka228@gmail.com

Modern car key fobs use radio signals to unlock and start vehicles, but weak security measures make it possible to intercept and replay these signals using SDR (Software Defined Radio). This article explores the main vulnerabilities of car key fobs, hacking methods using SDR, such as replay attacks and exploits on weak encryption algorithms, and suggests protection measures against such threats.

Keywords: Car key fob, SDR, radio interception, replay attack, vulnerabilities, cybersecurity, software-defined radio.

Введение

Развитие беспроводных технологий значительно повысило удобство использования автомобилей, позволяя владельцам открывать двери и запускать двигатель с помощью радиоуправляемых брелоков. Однако эта же технология открыла новые уязвимости, которыми могут воспользоваться злоумышленники. Программно-определяемое радио (SDR) стало мощным инструментом в руках специалистов по кибербезопасности, хакеров и исследователей, позволяя перехватывать и анализировать радиосигналы автомобильных систем. В отличие от традиционных приёмников, SDR позволяет программно изменять параметры работы, что делает его универсальным инструментом для изучения и потенциального взлома радиочастотных систем.

Уязвимости в автомобильных брелоках могут привести к угону транспортных средств или несанкционированному доступу к их системам. Некоторые модели автомобилей до сих пор используют устаревшие алгоритмы кодирования сигнала, которые легко взломать при наличии соответствующего оборудования и знаний. Атаки с использованием SDR могут включать в себя перехват радиосигнала, его запись и повторное воспроизведение, что позволяет злоумышленникам разблокировать автомобиль без наличия оригинального брелока. В этой статье мы рассмотрим основные методы взлома автомобильных брелоков через SDR и способы защиты от подобных атак.

Как можно взломать автомобильный брелок через SDR?

Одним из наиболее распространённых методов взлома автомобильных брелоков с помощью SDR является атака повторного воспроизведения (replay attack). Этот метод особенно эффективен против устаревших систем, использующих фиксированные или слабо защищённые сигналы. Атака начинается с того, что злоумышленник использует SDR-приёмник для перехвата радиосигнала, передаваемого брелоком при нажатии кнопки разблокировки. Затем этот сигнал записывается и воспроизводится в нужный момент, что позволяет злоумышленнику открыть автомобиль без оригинального брелока[1].

Для осуществления подобной атаки могут использоваться недорогие SDR-устройства, такие как RTL-SDR, HackRF One или BladeRF. Эти устройства позволяют улавливать радиочастоты, на которых работают автомобильные брелоки (обычно в диапазоне 300–500 МГц). С помощью специализированного ПО, например GNU Radio или Universal Radio Hacker, злоумышленник может анализировать захваченные сигналы, фильтровать их и в дальнейшем использовать для атаки[2].

Другой метод атаки — анализ и взлом слабых алгоритмов кодирования сигнала. Некоторые автомобили используют устаревшие механизмы защиты, такие как фиксированные коды (fixed code), которые остаются неизменными при каждом нажатии кнопки брелока. Если злоумышленник перехватит такой сигнал один раз, он может воспроизвести его сколько угодно раз, что делает защиту автомобиля неэффективной. Современные системы применяют кодировку с "плавающим кодом" (rolling code), при которой каждый новый сигнал уникален и не может быть повторно использован. Однако и такие системы имеют уязвимости: злоумышленник может использовать атаку "rolljam", в ходе которой перехватываются несколько последовательных сигналов, что позволяет в дальнейшем скомпрометировать систему[3].

Для выполнения атаки rolljam злоумышленник использует два приёмника SDR: один записывает сигнал от брелока, а второй одновременно глушит передачу сигнала к автомобилю. Таким образом, владелец вынужден нажимать кнопку несколько раз, и атакующий получает несколько уникальных кодов. Один из этих кодов используется для разблокировки автомобиля, а второй сохраняется для последующего использования. Данный метод делает возможным угон даже автомобилей, использующих более современные методы защиты[4].

Помимо атак replay attack и rolljam, SDR также позволяет проводить анализ радиосигнала с целью поиска других уязвимостей. Например, некоторые брелоки и системы бесключевого доступа (keyless entry) передают сигналы в некодированном виде, что позволяет их относительно легко клонировать. В некоторых случаях злоумышленники могут даже

использовать ретрансляционные атаки (relay attack), при которых сигнал от ключа перехватывается и передаётся на большее расстояние, позволяя разблокировать и завести автомобиль, даже если оригинальный ключ находится далеко от машины[5].

В связи с развитием SDR-технологий и их доступностью защита автомобильных систем становится важнейшей задачей для производителей транспортных средств. Компании, занимающиеся автомобильной безопасностью, внедряют усовершенствованные механизмы шифрования и защиты сигналов, однако старые модели автомобилей всё ещё остаются уязвимыми. Владельцам транспортных средств следует учитывать возможные угрозы и предпринимать дополнительные меры защиты.

Заключение

Использование SDR для взлома автомобильных брелоков подчёркивает уязвимость современных транспортных средств перед радиочастотными атаками. Злоумышленники могут использовать методы replay attack, rolljam и relay attack для получения несанкционированного доступа к автомобилю. Эти атаки становятся всё более доступными из-за распространённости SDR-устройств и программного обеспечения для анализа радиосигналов.

Чтобы минимизировать риск взлома, производители автомобилей внедряют новые технологии защиты, такие как улучшенные алгоритмы шифрования и системы обнаружения аномальной активности. Однако владельцам автомобилей также следует предпринимать меры предосторожности: хранить брелоки в экранированных чехлах, отключать бесключевой доступ, если он не используется, и регулярно обновлять программное обеспечение бортовых систем.

Развитие SDR-технологий открывает не только новые возможности в радиосвязи, но и создаёт серьёзные вызовы для автомобильной безопасности. Важно понимать потенциальные угрозы и активно внедрять методы защиты, чтобы предотвратить угон автомобилей с использованием уязвимостей в радиосистемах.

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 infotelec communications 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 //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.
 3. Sinelshchikov V. S., Tsvetkov A. Yu. Personal data protection at the enterprise //Actual problems of infotelec communications in science and education (APINO 2021). – 2021. – pp. 653-657.
 4. Lesnova E. M., Pestov I. E. Development of an error detection and correction method 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.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056.5

УЯЗВИМОСТИ В ПРОТОКОЛАХ LORAWAN: МОЖНО ЛИ ВЗЛОМАТЬ IoT-СЕТИ В УМНЫХ ГОРОДАХ?

Авдалян А.А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail:
sharmanka228@gmail.com

LoRaWAN — это один из самых популярных протоколов связи для Интернета вещей (IoT), особенно в умных городах, где используется для управления инфраструктурой, мониторинга окружающей среды и автоматизации городских процессов. Однако, несмотря на свою энергоэффективность и дальность передачи данных, LoRaWAN имеет ряд уязвимостей, которые могут быть использованы злоумышленниками. В статье рассматриваются основные угрозы безопасности, такие как атаки на шифрование, подмена узлов и перехват данных, а также возможные способы защиты, включая усиленную аутентификацию, безопасное управление ключами и сегментацию сети.

Ключевые слова: LoRaWAN, IoT, умные города, безопасность, перехват данных, кибератаки, аутентификация, криптография.

VULNERABILITIES IN LORAWAN PROTOCOLS: IS IT POSSIBLE TO HACK RIOT NETWORKS IN SMART CITIES?

Avdalyan A.A.

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: sharmanka228@gmail.com

LoRaWAN is one of the most popular communication protocols for the Internet of Things (IoT), especially in smart cities, where it is used for infrastructure management, environmental monitoring, and urban process automation. However, despite its energy efficiency and long-range data transmission, LoRaWAN has several vulnerabilities that attackers can exploit. This article examines the main security threats, such as encryption attacks, node spoofing, and data interception, as well as possible protection methods, including enhanced authentication, secure key management, and network segmentation.

Keywords: LoRaWAN, IoT, smart cities, security, data interception, cyberattacks, authentication, cryptography.

Введение

С развитием технологий Интернета вещей (IoT) появляется всё больше новых возможностей для создания умных городов. Одним из ключевых элементов таких городов является использование протоколов связи, которые обеспечивают взаимодействие устройств и систем на больших расстояниях с минимальным потреблением энергии. Одним из таких протоколов является LoRaWAN (Long Range Wide Area Network), который используется для организации беспроводных IoT-сетей. LoRaWAN позволяет подключать множество устройств, таких как датчики, контроллеры, системы мониторинга, и обеспечивать их работу

на больших расстояниях с использованием небольшой мощности. Это делает его идеальным решением для умных городов, где требуется управление многочисленными объектами и сервисами, такими как уличное освещение, системы видеонаблюдения, мониторинг качества воздуха и водоснабжения.

Однако, как и любая технология, LoRaWAN не защищён от уязвимостей, которые могут быть использованы злоумышленниками. В условиях умных городов, где в сеть подключены критически важные системы, безопасность IoT-сетей имеет первостепенное значение. Уязвимости в протоколах LoRaWAN могут стать причиной масштабных атак на инфраструктуру города, включая перехват данных, подмену команд управления или нарушение работы ключевых сервисов. В данной статье рассматриваются основные угрозы, связанные с использованием LoRaWAN в умных городах, а также предлагаются методы защиты, которые помогут минимизировать риски и повысить уровень безопасности таких сетей.

Уязвимости в протоколах LoRaWAN: можно ли взломать IoT-сети в умных городах?

С развитием Интернета вещей (IoT) технологии беспроводной связи становятся всё более востребованными. Одним из ключевых протоколов для передачи данных на большие расстояния с минимальным энергопотреблением является LoRaWAN (Long Range Wide Area Network). Этот протокол широко применяется в умных городах для управления освещением, мониторинга окружающей среды, автоматизации коммунальных услуг и других критически важных задач. Однако, как и любая технология, LoRaWAN не является полностью защищённым, и злоумышленники могут использовать его уязвимости для атак на инфраструктуру IoT-сетей.

Одной из главных проблем безопасности LoRaWAN является его криптографическая защита. Хотя в основе протокола лежат механизмы шифрования AES-128, многие реализации страдают от слабого управления ключами. В случае компрометации ключей злоумышленник может расшифровать передаваемые данные, а также подменять сообщения, что может привести к нарушению работы критически важных систем. Например, если злоумышленник перехватит и подменит команды управления уличным освещением, он может вызвать сбой в системе, создавая хаос в городе.

Другой распространённой уязвимостью LoRaWAN является подмена узлов сети. Аутентификация устройств в LoRaWAN-сетях может быть реализована неправильно или с недостаточной степенью защиты, что позволяет злоумышленникам внедрять поддельные устройства в сеть. Это открывает возможности для атак типа "человек посередине" (MITM), когда злоумышленник перехватывает трафик между устройствами и сетью, изменяя или перенаправляя передаваемые данные. В результате можно не только контролировать работу IoT-устройств, но и манипулировать информацией, что особенно опасно в сфере здравоохранения, транспорта и управления городской инфраструктурой.

LoRaWAN также подвержен атакам на уровень физического доступа. Поскольку сеть работает на неконтролируемых частотах (например, 868 МГц в Европе и 915 МГц в США), её можно заглушить при помощи мощных помеховых сигналов. Это позволяет злоумышленникам нарушить связь между IoT-устройствами и базовыми станциями, временно выводя сеть из строя. Такая атака может быть использована для дестабилизации работы

умного города, например, отключения датчиков контроля качества воздуха или систем умного парковочного мониторинга[1].

Помимо атак на физическом уровне, LoRaWAN подвержен анализу сетевого трафика. Несмотря на наличие шифрования, метаданные пакетов, такие как время передачи, частота и идентификаторы устройств, остаются видимыми. Анализируя эти данные, злоумышленники могут определить поведение устройств, их расположение и даже прогнозировать возможные события в сети. Например, если атакующий выявит закономерности в передаче данных датчиков системы полива в умном городе, он сможет предсказать, когда включаются и выключаются определённые зоны орошения, а затем использовать эту информацию для дальнейших атак[2].

Одним из способов защиты от атак на LoRaWAN является использование усиленной аутентификации устройств. В стандартных настройках LoRaWAN применяется метод аутентификации с фиксированными ключами, что делает систему уязвимой в случае их утечки. Более безопасным решением является внедрение механизма динамического управления ключами, который регулярно обновляет ключи шифрования, минимизируя риск компрометации[3].

Другим важным шагом в защите LoRaWAN является правильное управление сетью. Сегментация сети, при которой различные группы IoT-устройств работают в отдельных логических сегментах, позволяет изолировать компрометированные устройства и предотвращает распространение атак. Кроме того, использование механизмов обнаружения аномалий, таких как анализ поведения трафика и машинное обучение, позволяет оперативно выявлять подозрительную активность в сети[4].

Дополнительную защиту можно обеспечить за счёт использования VPN или защищённых туннелей для передачи данных между LoRaWAN-шлюзами и серверами. Это исключает возможность перехвата данных в канале связи и предотвращает атаки на уровень управления сетью. Кроме того, настройка правильных параметров мощности передатчика и частотных каналов снижает вероятность успешных атак, основанных на помехах и глушении сигнала[5].

В условиях быстрого роста IoT-сетей и внедрения LoRaWAN в инфраструктуру умных городов вопросы безопасности становятся всё более актуальными. Несмотря на энергоэффективность и дальность передачи данных, уязвимости в этом протоколе делают его потенциальной мишенью для злоумышленников. Без надлежащих мер защиты хакеры могут получить доступ к критически важным системам, перехватывать данные и даже дестабилизировать работу городской инфраструктуры.

Заключение

LoRaWAN играет важную роль в развитии умных городов, позволяя автоматизировать широкий спектр задач, от управления коммунальными услугами до мониторинга состояния окружающей среды. Однако его уязвимости делают IoT-сети потенциально уязвимыми для атак, которые могут привести к утечке данных, сбоям в работе городской инфраструктуры и финансовым потерям.

Для минимизации рисков необходимо применять комплексный подход к защите LoRaWAN-сетей. Использование динамических ключей шифрования, многофакторной аутентификации и сетевой сегментации значительно снижает вероятность успешных атак.

Внедрение механизмов обнаружения аномалий и мониторинга трафика также помогает оперативно выявлять попытки взлома.

По мере развития технологий LoRaWAN киберугрозы будут эволюционировать, и защита этих сетей должна оставаться приоритетом для разработчиков и администраторов IoT-инфраструктуры. Только комплексный подход к безопасности поможет обеспечить надёжность IoT-сетей и предотвратить возможные атаки в умных городах будущего.

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 неклонировуемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. and others. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.
 2. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
 3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method 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 infotelec communications 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 infotelec communications in science and education. - 2021. – pp. 409-414.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056.5

ВНЕДРЕНИЕ ВРЕДНОСА В ВИДЕОДРАЙВЕРЫ: МОЖНО ЛИ АТАКОВАТЬ ЧЕРЕЗ OPENGL И VULKAN

Авдалян А.А.

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:
sharmanka228@gmail.com

Системы, использующие OpenGL и Vulkan для графических вычислений, становятся всё более сложными и функциональными, что открывает новые возможности для атак. В статье рассматривается возможность внедрения вредоносного кода в видеодрайверы через эти графические API, их уязвимости, методы эксплуатации и способы защиты от подобных атак. Особое внимание уделено архитектурным особенностям драйверов и механизму взаимодействия с операционными системами и приложениями, что делает возможным применение таких атак в реальных сценариях.

Ключевые слова: Вирус, видеодрайверы, OpenGL, Vulkan, атаки, уязвимости, безопасность, графика.

MALWARE INJECTION INTO VIDEO DRIVERS: IS IT POSSIBLE TO ATTACK THROUGH OPENGL AND VULKAN

Avdalyan A.A.

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: sharmanka228@gmail.com

Systems using OpenGL and Vulkan for graphics computations are becoming increasingly complex and functional, opening up new avenues for attacks. This article explores the potential for injecting malicious code into graphics drivers through these graphics APIs, their vulnerabilities, methods of exploitation, and ways to protect against such attacks. Special attention is given to the architectural features of drivers and the interaction mechanisms with operating systems and applications, making such attacks viable in real-world scenarios.

Keywords: Malware, graphics drivers, OpenGL, Vulkan, attacks, vulnerabilities, security, graphics.

Введение

С каждым годом графические API, такие как OpenGL и Vulkan, становятся неотъемлемой частью как игр, так и сложных вычислительных задач, включая машинное обучение и научные вычисления. Развитие технологий в этой области привело к значительному увеличению сложности и функциональности видеодрайверов, которые теперь выполняют гораздо больше задач, чем просто рендеринг графики. Однако, с увеличением их функционала растет и количество потенциальных уязвимостей, которые могут быть использованы злоумышленниками для атак. В этом контексте вопросы безопасности видеодрайверов, а также возможность внедрения вредоносного кода через графические API, становятся особенно актуальными.

Внедрение вредоносного кода в видеодрайверы может быть опасным, поскольку эти драйверы имеют высокий уровень привилегий и глубокую интеграцию с операционной системой. Атаки, использующие уязвимости в драйверах, могут привести к удаленному выполнению кода, повышению привилегий или даже к полному контролю над системой. В случае с OpenGL и Vulkan, их широкое распространение и использование в самых различных приложениях создают большие возможности для злоумышленников, желающих использовать графические подсистемы как вектор атак. Этот процесс может быть особенно сложным и малоизученным, поскольку взаимодействие между драйверами, операционной системой и приложениями является многослойным и трудным для мониторинга.

Несмотря на то, что графические драйверы в последние годы значительно улучшились с точки зрения безопасности, они по-прежнему остаются уязвимыми для атак. Злоумышленники могут использовать различные методы эксплуатации уязвимостей, таких как буферные переполнения, некорректное управление памятью и недостаточную изоляцию данных между процессами. Это открывает путь к атакам, где видеодрайверы становятся точкой входа для внедрения вредоносного кода.

Внедрение вредоносного кода через OpenGL и Vulkan

Для начала важно понять, как видеодрайверы работают с OpenGL и Vulkan и какую роль они играют в архитектуре системы. Видеодрайверы — это программы, которые обрабатывают запросы от приложений и операционной системы для отображения графики на экране. OpenGL и Vulkan, являясь стандартами графического рендеринга, позволяют программам запрашивать ресурсы для работы с графическими изображениями, текстурами, шейдерами и т. д. Оба API предоставляют низкоуровневый доступ к видеокарте, что делает их мощными инструментами, но и уязвимыми для атак[1].

OpenGL, будучи более старым API, поддерживает множество устаревших функций и предоставляет широкие возможности для работы с графическими данными, что может открывать дверь для различных уязвимостей. Vulkan, в свою очередь, обеспечивает более прямой доступ к графическому процессору, что даёт приложениям больший контроль, но также увеличивает риски безопасности. Оба этих API имеют сложную архитектуру взаимодействия между приложениями, драйверами и операционной системой, что может затруднять мониторинг и защиту от атак[2].

Одним из возможных путей атаки через видеодрайверы является внедрение вредоносного кода через недочеты в механизмах обработки данных, передаваемых от приложения в драйвер. Злоумышленники могут использовать уязвимости в обработке шейдеров, текстур или других графических объектов для того, чтобы подменить данные, которые драйвер обрабатывает. Это позволяет внедрять произвольный код в память видеокарты или напрямую в пространство памяти операционной системы, что может привести к выполнению вредоносных команд с высокими привилегиями[3].

Также стоит отметить, что видеодрайверы имеют доступ ко многим системным ресурсам, включая память, устройства ввода-вывода и другие критически важные компоненты. При успешной эксплуатации уязвимости в драйвере, злоумышленник может использовать эту точку доступа для дальнейших атак, таких как повышение привилегий или выполнение команд, которые нарушают целостность системы. Один из таких методов заключается в эксплуатации буферных переполнений, когда приложение или драйвер

пытается записать больше данных в буфер, чем он может вместить. Это приводит к перезаписи памяти и может быть использовано для внедрения вредоносного кода[4].

Кроме того, можно вспомнить о так называемых уязвимостях zero-day, которые в первую очередь ориентированы на драйверы. Это такие уязвимости, которые еще не были раскрыты или исправлены производителями, и их использование может быть крайне опасным для безопасности системы. Изначально эти уязвимости могут быть использованы для проведения атак через OpenGL или Vulkan, особенно когда производители драйверов не уделяют должного внимания проверке и исправлению уязвимостей в своих программных продуктах[5].

Для защиты от подобных атак важно придерживаться нескольких рекомендаций. Во-первых, необходимо регулярно обновлять драйверы и видеодрайверы, поскольку производители часто выпускают обновления, устраняющие уязвимости. Во-вторых, следует использовать средства защиты, такие как изоляция процессов и использование системы контроля целостности, которая поможет обнаружить изменения в видеодрайверах или других критически важных компонентах системы. Также важно использовать системы обнаружения вторжений, которые могут мониторить аномалии в поведении графических драйверов и своевременно предупреждать о возможных угрозах.

Заключение

Внедрение вредоносного кода через видеодрайверы, использующие OpenGL и Vulkan, представляет собой реальную угрозу для информационной безопасности. Уязвимости в этих драйверах могут быть использованы для выполнения кода с повышенными привилегиями, что открывает путь для более серьёзных атак, включая шифрование данных, повышение привилегий и удалённое управление системой. При этом сложность архитектуры драйверов и их тесная интеграция с операционной системой создают дополнительные трудности в защите от таких атак.

Понимание того, как работают графические API и их взаимодействие с операционной системой, а также принятие мер по защите, таких как обновление драйверов и использование систем мониторинга, помогает уменьшить риски. Внедрение вредоносного кода через OpenGL и Vulkan может стать эффективным вектором атак, если системы безопасности не будут своевременно обновляться и адаптироваться к новым угрозам.

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. 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. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.

4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

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 Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
 2. Minyaev A. A. A method for evaluating the effectiveness of an information security system geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
 3. Chmutov M. V. and others. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference materials. 2017. pp. 535-537.
 4. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
 5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.94

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ ГЕНЕРАТИВНОГО ДИЗАЙНА ПРИ ПРОЕКТИРОВАНИИ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ РАЗЛИЧНЫХ МАТЕРИАЛОВ

Шагаева Э.Р., ¹Надеждин А.А.

ФГБОУ ВО «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ», Уфа, Россия (450064, Республика Башкортостан, город Уфа, ул.
Космонавтов, д. 1), e-mail: ¹alex.nad.702@yandex.ru

В связи со стремительным развитием технологий, компьютерной и производственной сферы, расширением применения нейросетей, а также исследованием и созданием новых материалов и подходов к производству растет интерес специалистов из разных областей деятельности и стран к генеративному дизайну. Авторами данной статьи проанализированы существующие программные комплексы, реализующие метод генеративного дизайна. Сформулированы выводы по возможностям программных комплексов к готовности реализации метода генеративного дизайна в проектировании.

Ключевые слова: Строительство, генеративный дизайн, проектирование, программные комплексы, стоимость, строительные нагрузки.

ANALYSIS OF THE POSSIBILITIES OF USING GENERATIVE DESIGN IN THE DESIGN OF BUILDING STRUCTURES OF VARIOUS MATERIALS

Shagaeva E.R., ¹Nadezhdin A.A.

UFA STATE PETROLEUM TECHNOLOGICAL UNIVERSITY, Ufa, Russia (450064, Republic of
Bashkortostan, Ufa, Kosmonavtov st., 1), e-mail: ¹alex.nad.702@yandex.ru

Due to the rapid development of technologies, computer and production spheres, the expansion of the use of neural networks, as well as the research and creation of new materials and approaches to production, the interest of specialists from different fields of activity and countries in generative design is growing. The authors of this article analyzed existing software packages implementing the generative design method. Conclusions are formulated on the capabilities of software packages for the readiness to implement the generative design method in design.

Keywords: Construction, generative design, design, software packages, cost, construction loads.

В связи со стремительным развитием технологий, компьютерной и производственной сферы, расширением применения нейросетей, а также исследованием и созданием новых материалов и подходов к производству растет интерес специалистов из разных областей деятельности и стран к генеративному дизайну [1, с. 1]. Открытые новые горизонты для творчества и инноваций позволяют исследовать огромное пространство проектных решений и предоставляют возможность для оптимизации решения конкретных задач.

Генеративный дизайн (англ. Generative Design; син. «порождающий дизайн») в широком смысле – подход к проектированию и дизайну цифрового или физического продукта (сайт,

изображение, мелодия, архитектурная модель, деталь, анимация и т.д.), при котором человек делегирует часть процессов компьютерным технологиям и платформам. [3. с. 4]

В отличие от параметрического дизайна, где дизайнер вручную управляет параметрами для получения желаемого результата, генеративный дизайн автоматизирует процесс подбора наиболее эффективных решений. Компьютер, используя математические алгоритмы и машинное обучение, занимается управляющим блоком, таким образом генерируя сотни и тысячи вариантов развития событий (выборок), которые затем анализируются и оптимизируются для достижения наилучшего результата [2, с. 6].

Одним из самых ранних примеров и упоминаний генеративного дизайна в архитектуре можно считать творение Антонио Гауди – базилика Саграда Фамилия (Искупительный храм Святого Семейства) в Барселоне. Испанский архитектор Антонио Гауди спроектировал церковь в конце 19 века, разработав алгоритм «параболические арки» (Рисунок 1), который был применен в создании органических каменных структур в храме. С помощью этого алгоритма имитируется процесс естественного роста костей или деревьев.

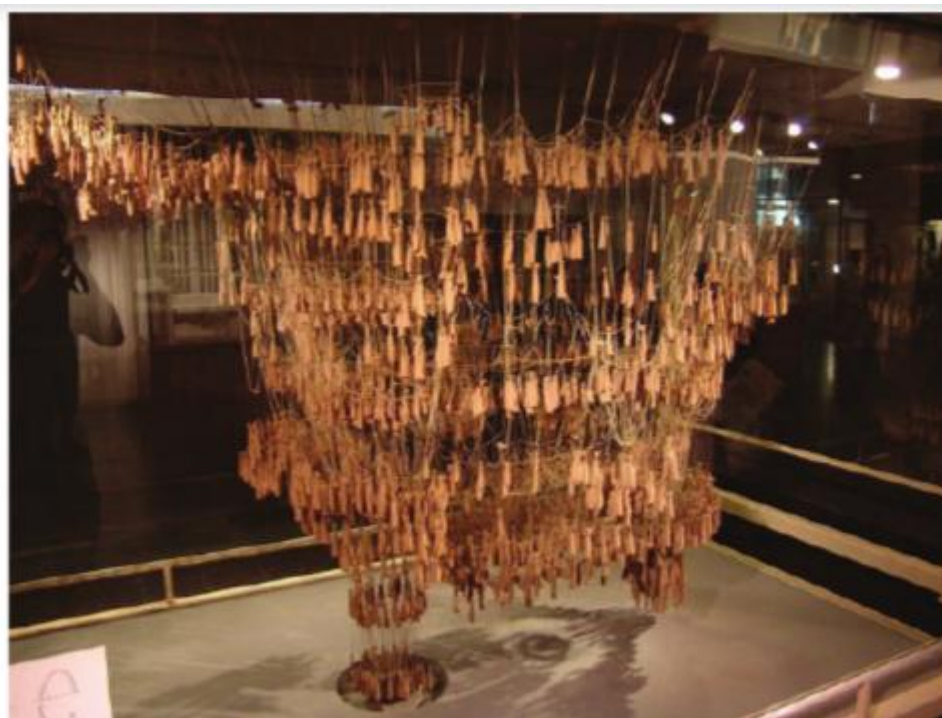


Рисунок 1 - Подвесная цепная модель Гауди

Движение вычислительного искусства, разработанное художниками, использовавшими компьютерные технологии для создания цифровых произведений искусства и активно развивающееся в 1960-х и 70-х годов, в немалой степени повлияло на развитие генеративного дизайна. Архитекторы обратили внимание на возможности вычислений в конце 1980-х и начале 1990-х годов и в этот же период начали экспериментировать с программным обеспечением для автоматизированного проектирования (САПР) для создания сложных конструкций с использованием алгоритмов. [4, с. 8]

В 2010-м году технологии обучения генеративных систем начинают быстро совершенствоваться. Так, в 2014 году Ян Гудфеллоу изобретает генеративно-состязательную сеть (GAN), которая используется для получения фотореалистичных изображений одежды,

сумок, портфелей, сцен компьютерных игр, интерьеров, объектов промышленного дизайна. А уже в 2016 году генеративный дизайн становится доступным и понятным для широкой аудитории, потребителей: группой российских разработчиков (А.Моисеенков, О.Пояганов, И.Фролов и А.Усольцев) создается приложение Prisma, способное обработать изображение в стиле известных художников с помощью нейронной сети. Стилизация происходит с помощью нейронной сети, которая подбирает множество вариантов преобразования фотографии.

Активное использование генеративного дизайна в архитектуре и строительстве началось в 2017 году, когда появились и были освоены программные средства, позволяющие составлять алгоритмы поиска формы и расположения объектов. [7, с. 8] Генеративный дизайн был назван «революционной технологией, использующей алгоритмы искусственного интеллекта для разработки изделия» [6, с. 2]. Эта технология позволяет сконцентрироваться на качестве проекта, оптимизации соотношения «архитектурная идея – функциональность», расширить возможности проектировщика. Помимо этого, было отмечено, что применение генеративного дизайна может повлиять на жизненный цикл здания в целом, а не только отражаться на этапе проектирования.

Нетрудно заметить из всего выше написанного, что генеративный дизайн используется практически повсеместно:

- В медицине генеративный дизайн имеет большие перспективы в имплантологии. Технология может позволить создавать структуры под конкретный организм, точно воссоздать трабекулярные структуры и шероховатость при имитации костей.
- В аэрокосмической промышленности генеративный дизайн используется с целью изучения новых возможностей проектирования и улучшения эксплуатационных характеристик. В авиации эта инновация уже применяется для решения сложных инженерных, архитектурных и системных задач.
- В автомобильной промышленности благодаря технологиям генеративного дизайна меняется архитектурная концепция автомобилей.
- В сфере розничной торговли генеративный задействован в генерировании уникальных форм, концепций для объектов продажи и их функциональности.



Рисунок 2 - Практические примеры генеративного дизайна в разных производственных сферах и областях

На основании того, что генеративный дизайн находит применение во многих сферах, зарубежные специалисты провели исследования [5, с. 3] и выделили такие направления технологии, как:

Топологическая оптимизация. Этот метод заключается в проектировании детали с условием: оптимизация структуры и поверхности; создание трабекулярных структур; синтез формы.

Одной из наиболее популярных областей применения генеративного дизайна, которую мы не рассмотрели, является строительство и архитектура. Эта технология находит широкое применение в сфере проектирования в связи с достаточным количеством преимуществ в виде оптимизации конструкций, сроков производства и следовательно – увеличением дохода. Но имеются и недостатки в технологии генеративного дизайна. В связи с тем, что генеративный дизайн — это относительно новая отрасль, в ней недостаточно опытных квалифицированных специалистов, обладающих знанием иностранного языка и языков программирования, присутствует некоторая сложность в отлаженности процессов в виде чрезмерного количества результатов, необходимы высокие начальные затраты на использование программ в коммерческих целях.

Но тем не менее, генеративный дизайн приобретает популярность за счет решения задач в архитектурном разделе проектов. Существуют примеры, в которых задействован генеративный дизайн, например, данная технология может помочь в создании формы крыши здания, формирования 3D-поверхностей стеновых панелей, оформлении интерьера и расстановке мебели. Для реализации всего перечисленного архитекторы часто используют Grasshopper и ArhiCAD. Кроме того, генеративный дизайн имеет практическую значимость и для специалистов по инженерным системам, в частности при расстановке какого-либо инженерного оборудования и при трассировке коммуникация с учетом оптимизации их протяженности.

В подтверждение вышесказанному можно привести пример применения генеративного подхода для проектирования офисов Autodesk Mars (Рисунок 3) исследовательской группой «The Living». Для того чтобы создать абсолютно объективную архитектуру здания, расположенного в Торонто, были задействованы данные об окружающей среде (солнечный свет, вид снаружи) и предпочтения работников (соседство, стиль работы и отвлекающие факторы). [8, с. 4]

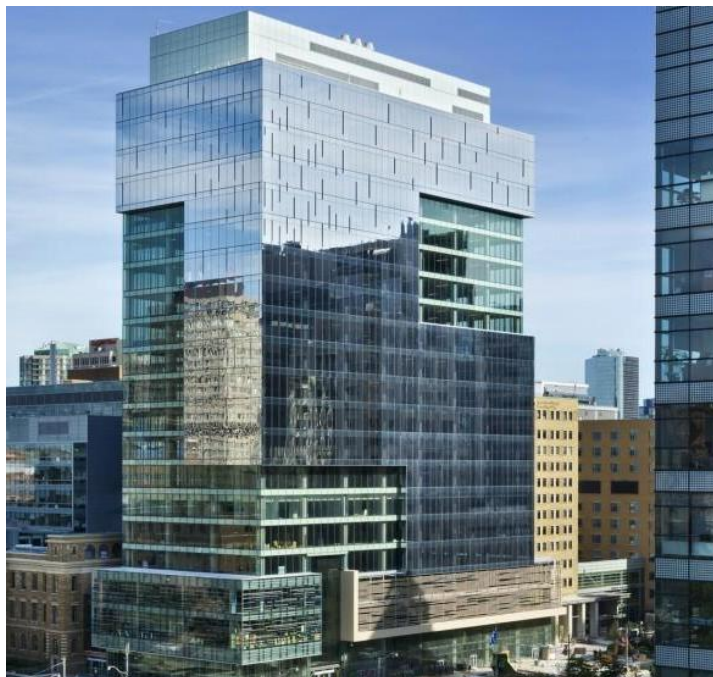


Рисунок 3 - Autodesk MaRS Office, The Living, Канада

То есть, генеративный дизайн также может иметь немаловажную роль в процессе координации проектных отделов между собой. Эта технология может использоваться для создания схемы функционального зонирования территории, задав параметры радиусов обслуживания для различных социально-значимых объектов (школы, больницы, учреждения дошкольного образования) [7, с. 6]. Но будет необходимо привлечение большого количества данных из различных информационных систем, в том числе геоинформационных, как и при проектировании офисов Autodesk Mars.

Принцип генеративного моделирования на примере крепления телескопа. Изначально модель выглядит следующим образом (Рисунок 5)



Рисунок 4 - Модель крепления телескопа

Впоследствии задания граничных условий и нагрузок, приходящихся на данное крепление, получаем результат расчета, приведенные на рисунке ниже.

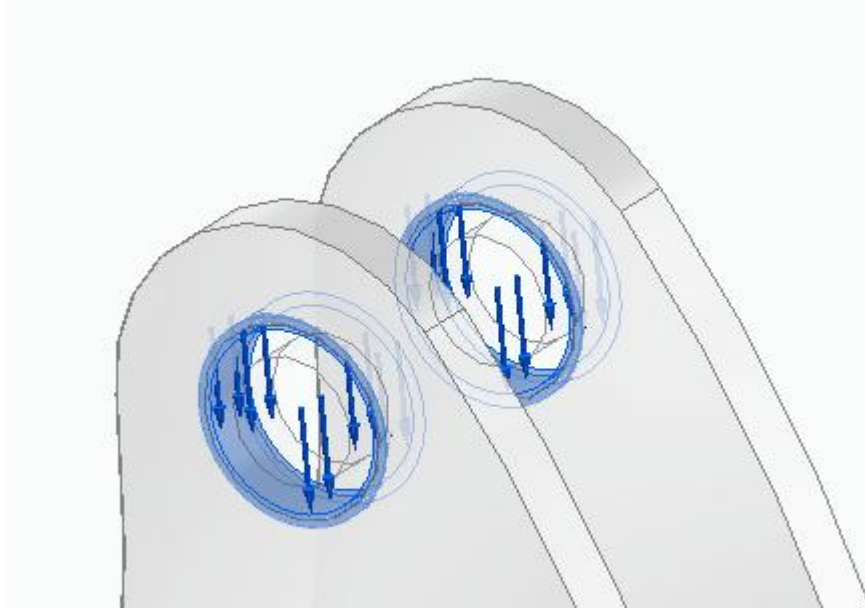


Рисунок 5 - Приложение нагрузок к отверстиям в креплении

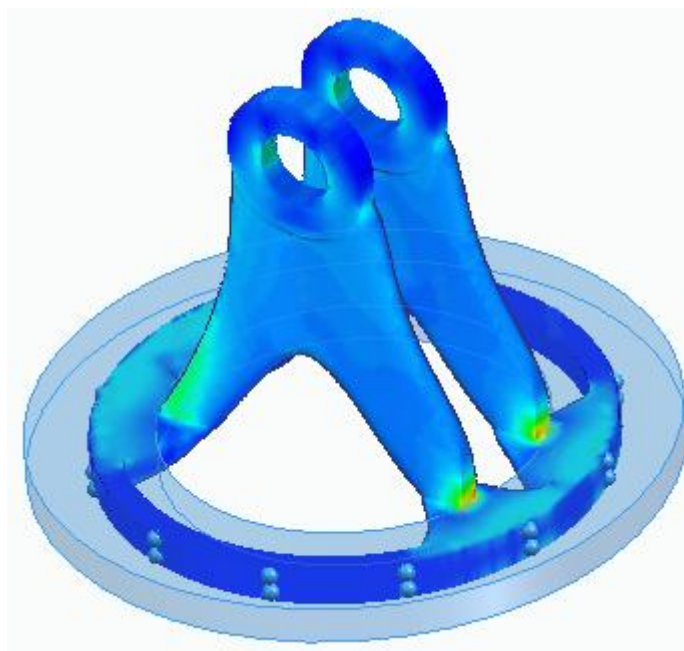


Рисунок 6 - Полученный результат расчета с использованием генеративного дизайна

На данном этапе предлагается проанализировать существующие программные комплексы, реализующие метод генеративного дизайна. Поскольку, как было сказано выше, генеративный дизайн имеет очень широкий спектр применения, то выберем несколько факторов, определяющих выбор и сценарий использования программного комплекса.

Первой программой для исследования является Fusion 360 от компании Autodesk. В своем арсенале программа имеет так называемый «решатель» (solver). В программе моделируется трехмерный объект, затем, при помощи данного решателя, к трехмерному объекту прилагаются нагрузки, и программа производит расчет напряжений и усилий к прилагаемому элементу на основе законов твердого/упругого тела. После чего, программа

строит диаграмму напряжений в рассматриваемом объекте и «отсекает» материал в тех точках, где напряжение минимальны или близки к нулю. При этом несущая способность элемента остается на прежнем уровне, а экономия материала может достигать 80%.



Рисунок 7 - Принцип работы генеративного дизайна в Fusion 360. Слева – модель, рассчитанная по законам механики, справа – оптимизированная генеративным дизайном модель

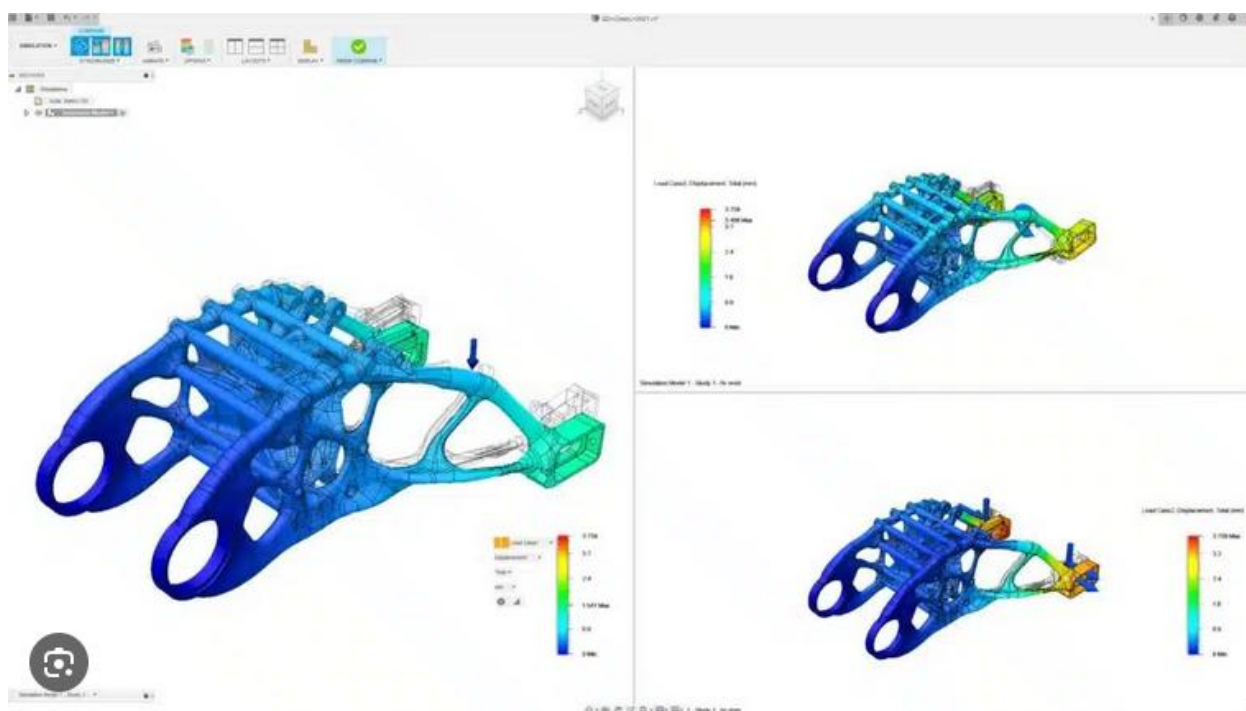


Рисунок 8 - Результат расчета твердого тела в Fusion 360

Это был один из примеров программ, реализующих метод генеративного дизайна при проектировании строительных конструкций.

В данной статье рассмотрено 7 программ в которых имеется функционал по работе с генеративным дизайном.

Основными критериями для анализа являются сложность в освоении ПО, доступность для различных платформ (windows, linux и т.д.), а также возможность работать с различными видами материалов.

Результаты анализа сведены в Таблицу 1.

Таблица 1 - Сводная таблица сравнительных характеристик ПО с использованием генеративного дизайна

Критерий	Autodesk Fusion 360	Creo Elements	Autodesk Revit	Solid Edge	Siemens NX	Ansys Discovery	Catia
Сложность	★★★	★★	★★★★		★★★★★	★	★
Стоимость	Средняя (отдельное дополнение к Fusion 360)	Средняя	Средняя (отдельное дополнение к Autodesk Revit)	Средняя	Высокая	Высокая	Высокая
ОС	Windows, MacOS	Windows	Windows	Windows	UNIX, Linux, MacOS, Windows	Windows, Linux	UNIX, Windows
Виды нагрузок	Сила, давление	Сила	Сила, давление	Сила, давление, крутящий момент	Сила, давление, крутящий момент	Сила, давление, крутящий момент	Сила, давление, крутящий момент
Металлические конструкции	Отлично	Отлично	Хорошо(4). Есть проблемы с армированием	Отлично	Отлично	Хорошо(4)	Отлично
Железобетонные конструкции	Хорошо	Хорошо	Хорошо	Хорошо	Хорошо	Хорошо	Не работает
Деревянные конструкции	Удовлетворительно	Не работает	Удовлетворительно	Удовлетворительно	Удовлетворительно	Удовлетворительно	Не работает

Источник: анализ автора

На основании результатов видно, что большинство программных продуктов отлично справляются с расчетом металлических конструкций. Сложности возникают только при расчете армирования в железобетонных конструкциях.

С расчетом железобетонных конструкций программы также справляются хорошо, но поскольку расчет таких конструкций является уже более сложной задачей, а их поведение менее предсказуемо, то возможностей по работе генеративного дизайна с бетоном становятся более ограниченными в сравнении с металлическими конструкциями.

Хуже всего дела обстоят с деревянными конструкциями. Большинство программ достаточно хорошо справляются непосредственно с расчетом конструкций, но применительно к генеративному дизайну, возможности сильно ограничены. Если же добавить сюда требования отечественных нормативов, то смысл в генеративном дизайне для деревянных конструкций теряет свою целесообразность, поскольку становится слишком много ограничительных условий для работы модуля генеративного дизайна.

Основные выводы, которые можно сформулировать на основании вышеизложенного:

1. Генеративный дизайн является хорошим инструментом при расчете строительных конструкций и экономии материала, при соблюдении определенных условий.
2. Генеративный дизайн отлично справляется с расчетом строительных конструкций, в большинстве случаев хорошо с железобетонными конструкциями и удовлетворительно с деревянными конструкциями.
3. Для расчета металлических конструкций можно выбрать любое из проанализированных ПО. В данном случае необходимо отталкиваться от критерия стоимости продукта, а также сложности его освоения.
4. В случае расчета железобетонных конструкций оптимальным выбором являются программы от компании Autodesk – Revit и Fusion 360. Основной проблемой может стать учет сложного армирования при оптимизации (экономии) материала. Данное ПО также имеет широкую базу знаний для обучения и не является самым сложным в освоении.
5. Генеративный дизайн имеет сильно ограниченный функционал, когда речь заходит о деревянных конструкциях. Дерево само по себе является сложным и слабопрогнозируемым для расчета материалом. Поэтому использование генеративного дизайна в данном случае может носить чисто визуальный характер и не рекомендуется для расчета строительных конструкций.

Список литературы

1. Айрапетян Н.Г., Зайцев А.А. Повышение эффективности использования земельного участка на основе генеративного дизайна // Журнал правовых и экономических наук. – 2021, 3 – С. 129-136.
2. Кошман, В. Д. Перспективы применения технологии генеративного дизайна в проектировании / В. Д. Кошман // Электронные системы и технологии [Электронный ресурс] : сборник материалов 58-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18-22 апреля 2022 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Д. В. Лихаческий [и др.]. – Минск, 2022. – С. 827–829. – Режим доступа : <https://libeldoc.bsuir.by/handle/123456789/46926>.
3. Промышленный дизайн Российской Федерации: возможность преодоления «дизайн-барьера»: учеб. пособие / под ред. М. С. Липецкой, С. А. Шмелевой; —СПб.: Изд-во Политехн. ун-та, 2012 — 80 с.

4. Ахунзянов А.Ф., Дектерев С.А. Генеративное проектирование: история, преимущества и ограничения в области архитектуры // Международный научный журнал «Молодой ученый» №19 (518) – 2024 – С. 38-40.
5. Engineering.com [Электронный ресурс]: The New Age of Highly Efficient Products Made with Generative Design. Режим доступа: <https://www.engineering.com/DesignSoftware/DesignSoftwareArticles/ArticleID/15136/The-New-Age-of-Highly-Efficient-Products-Made-with-Generative-Design.aspx> (дата обращения 21.11.2020).
6. Autodesk открывает лабораторию генеративного дизайна в Чикаго [Электронный ресурс]: // AUTODESK. Новости. Режим доступа: <https://sapr.ru/article/25681> (дата обращения 01.12.2020) ISICAD – Ваше окно в мир САПР [Электронный ресурс]: Авторы isicad. Рупиндер Тара. Режим доступа: <https://www.autodesk.ru/press-releases/2019-03-06> (дата обращения 21.11.2020).
7. Игнатова Е.В., Предеина В.П. Состояние и перспективы применения технологии генеративного дизайна в строительстве // Журнал «Строительство и архитектура» Том 9, № 1 – 2021 – С. 71-75.
8. Жандарова А.А., Денисенко Е.В. Предпосылки развития технологий в бионаправленной архитектуре // Журнал «Architecture and Modern Information Technologies» № 4 (61) – 2022 – С. 28-43.

References

1. Hayrapetyan N.G., Zaitsev A.A. Improving the efficiency of land use based on generative design // Journal of Legal and Economic Sciences, 2021, 3– pp. 129-136.
2. Koshman, V. D. Prospects of using generative design technology in design / V. D. Koshman // Electronic systems and technologies [Electronic resource] : collection of materials of the 58th scientific conference of graduate students, undergraduates and students of BSUIR, Minsk, April 18-22, 2022 / Belarusian State University of Informatics and Radioelectronics ; editorial board: V. Likhachesky [et al.]. – Minsk, 2022. – pp. 827-829. – Access mode : <https://libeldoc.bsuir.by/handle/123456789/46926> .
3. Industrial design of the Russian Federation: the possibility of overcoming the "design barrier": textbook. manual / edited by M. S. Lipetsk, S. A. Shmeleva; —St. Petersburg: Publishing House of Polytechnic. University, 2012 — 80 p.
4. Akhunzyanov A.F., Dekterev S.A. Generative design: history, advantages and limitations in the field of architecture // International Scientific Journal "Young Scientist" No. 19 (518) – 2024 – pp. 38-40.
5. Engineering.com [Electronic resource]: The New Age of Highly Efficient Products Made with Generative Design. Access mode: <https://www.engineering.com/DesignSoftware/DesignSoftwareArticles/ArticleID/15136/The-New-Age-of-Highly-Efficient-Products-Made-with-Generative-Design.aspx> (accessed 11/21/2020).
6. Autodesk opens a generative design laboratory in Chicago [Electronic resource]: // AUTODESK. News. Access mode: <https://sapr.ru/article/25681> (accessed 12/01/2020) ISICAD – Your window into the world of CAD [Electronic resource]: isicad authors. Rupinder

Container. Access mode: <https://www.autodesk.ru/press-releases/2019-03-06> (accessed 11/21/2020).

7. Ignatova E.V., Predeina V.P. The state and prospects of using generative design technology in construction // Journal of Construction and Architecture Vol. 9, No. 1 – 2021 – pp. 71-75.
 8. Zhandarova A.A., Denisenko E.V. Prerequisites for the development of technologies in bionational architecture // Architecture and Modern Information Technologies Journal No. 4 (61) – 2022 – pp. 28-43.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.451.25

АНАЛИЗ СУЩЕСТВУЮЩИХ ERP-СИСТЕМ В БИЗНЕСЕ.

Сафонов С.В., ¹Бякерев Р.М., ²Масленников А.К.

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: ¹byakerev@mail.ru, ²art.maslennikoff2016@yandex.ru

В статье рассматривается тема существующих ERP-систем на рынке. Проводится анализ самой ERP-систем и чем они полезны для бизнеса. Приводятся примеры современных систем с указанием их преимуществ и недостатков каждой. Как ERP-система связывает в себе все отрасли бизнеса и как ими можно управлять.

Ключевые слова: ERP-система, SAP, 1C, бизнес-среда, архитектура системы, IT.

ANALYSIS OF EXISTING ERP SYSTEMS IN BUSINESS

Safonov S.V., ¹Byakerev R.M., ²Maslennikov A.K.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (105005, Moscow, 2nd Baumanskaya ul, 5 bld. 1), e-mail: ¹byakerev@mail.ru, ²art.maslennikoff2016@yandex.ru

The article discusses the topic of existing ERP systems on the market. The analysis of ERP systems themselves and how they are useful for business is carried out. Examples of modern systems are given, indicating their advantages and disadvantages of each. How an ERP system connects all business sectors and how they can be managed.

Keywords: ERP system, SAP, 1C, business environment, system architecture, IT.

В сложных условиях современного мира, характеризующегося постоянными изменениями и дальнейшим развитием бизнес-среды, управление предприятием становится всё более сложной задачей. Так как в современной ситуации конкуренции в динамичные условия рынка компании должны активно искать новые возможности оптимизации процессов и общую эффективность. Для этого данные системы ERP являются одним из главных средств.

ERP является многофункциональным программным обеспечением, которое широко применяется во всех секторах управления бизнесом. Введение систем позволяет собрать все эти области в единую структуру, что увеличивает продуктивность и снижает издержки. В этой статье мы попробуем определить, оказывает ли анализ системы решающее влияние на быстрое управление бизнесом. Обсуждаются такие преимущества и недостатки ERP-систем, как методы анализа и их рейтинги, с учетом всех основных факторов. Кроме того, нами рассматриваются все успешные сценарии обновления ERP в большом числе сфер производства, из-за чего мы можем определить факторы для выбора и анонсирования ERP-системы для предприятий всех категорий [3-4].

Какова значимость ERP-системы? ERP-систему часто называют "центральной нервной системой компании", потому что она автоматизирует бизнес-процессы, интегрирует

внутренние и внешние системы и предоставляет интеллектуальные решения, необходимые для управления повседневной деятельностью. Для согласованной работы всей нашей информационной системы все данные, связанные с нашей компанией, должны храниться в ERP, представляя собой одинарный источник достоверной информации. Так компания “Черкизово”, которая занимается переработкой мяса, нашла ERP-систему для синхронизации процессов поставки, закупки, логистики и производства. Это также дает нам возможность беспрепятственно передавать данные между различными системами, например, между 1C:ERP и 1C: WMS Логистика, и в то же время делать транзакции между юридическими лицами верно. ERP-система имеет шесть основных преимуществ [1-2]:

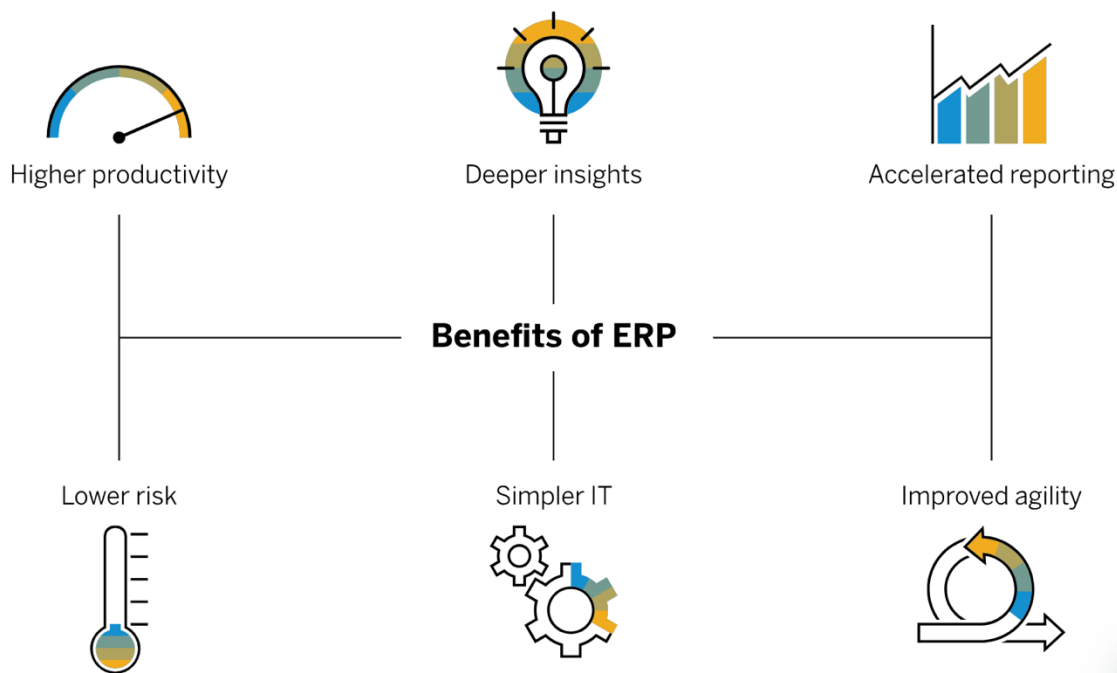


Рисунок 1 – Преимущества ERP-системы

1. Увеличение эффективности. Реализуйте оптимизацию и автоматизацию бизнес-процессов, что позволит организации достигать более значительных результатов при снижении затрат на ресурсы.
2. Глубокое понимание ситуации. Избегайте использования разрозненных хранилищ данных, создайте единый надежный источник информации для получения ответов на ключевые запросы бизнеса.
3. Ускоренное формирование отчетов. Быстро создавайте коммерческие и финансовые отчеты и делитесь полученными результатами. Основывайтесь на точных аналитических данных для повышения эффективности работы.
4. Снижение рисков. Повышайте уровень прозрачности и контроля в бизнесе, обеспечивая соблюдение нормативных требований, а также предсказывая и предотвращая потенциальные риски.
5. Оптимизация ИТ-процессов. Использование интегрированных ERP-систем с единой базой данных способствует упрощению ИТ-архитектуры и предоставляет работникам более удобные инструменты для выполнения задач.

6. Увеличение гибкости. Эффективное выполнение операций и непосредственный доступ к данным в реальном времени позволяют быстро выявлять новые возможности и оперативно реагировать на них [5].

Ключевые недостатки ERP-систем включают:

1. Значительные затраты на внедрение и эксплуатацию. Кроме расходов на лицензии, организациям необходимо также инвестировать в приобретение оборудования, настройку программного обеспечения, обучение сотрудников и техническую поддержку. Эти аспекты могут потребовать высоких финансовых ресурсов. Сложность внедрения.

2. Запуск системы требует тщательного планирования и координации действий всех подразделений. Данный процесс может оказаться продолжительным и потребует значительных усилий со стороны персонала.

3. Потребность в обучении сотрудников. Внедрение новой системы требует времени, и может вызвать сопротивление персонала, что затрудняет процесс адаптации.

4. Риск потери данных. При переходе на новую систему есть вероятность, что информация будет утеряна, поэтому важно тщательно планировать перенос данных и проводить тестирование для минимизации рисков [6].

5. Зависимость от поставщика. Компании оказываются «привязаны» к поставщику системы, который отвечает за техническую поддержку и обновления. Стабильность работы системы напрямую зависит от надежности поставщика и качества предоставляемых услуг [7].

Стандартные модули систем обслуживают основные бизнес-процессы, например, финансы, закупки и производство, предлагая сотрудникам соответствующих отделов необходимые операции и аналитику. Каждый модуль интегрируется в систему, формируя единый источник достоверных и точных данных, доступных для совместного использования разными подразделениями [5].

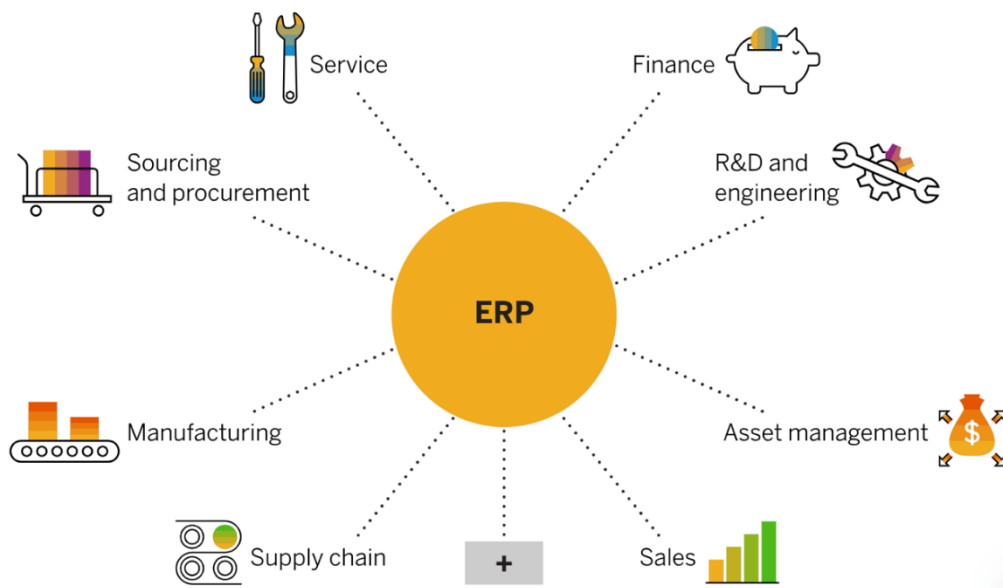


Рисунок 2 – управление ERP-системой между разными бизнес-процессами компании.

Постепенно мы перешли от общего понятия ERP-систем к примерам их применения в различных компаниях [8-9]. Первой на ум приходит SAP. Это немецкая компания, специализирующаяся на разработке программного обеспечения для управления бизнес-процессами. Ее решения охватывают широкий спектр задач, включая все сферы бизнеса.



Рисунок 3 – SAP система.

Для работы с данными SAP имеет разные продукты для сбора, обработки и анализа. SAP Datasphere, SAP HANA Cloud, SAP Analytics Cloud [12]

Таблица 1 – Разновидность продуктов SAP со своими преимуществами.

SAP Datasphere	SAP HANA Cloud	SAP Analytics Cloud
Обеспечение надежных данных. Ускорьте окупаемость инвестиций благодаря автоматическому использованию семантических определений и связей	Гибкая база данных, адаптированная к любым рабочим нагрузкам. Воспользуйтесь возможностями движка, который поддерживает различные модели данных — от реляционных баз и хранилищ документов до геопространственных данных, графов и временных рядов.	Применяйте генеративный ИИ для автоматизации отчетности, обнаружения скрытых закономерностей и разработки бизнес-планов с поддержкой ИИ-ассистента
Обогащение всех проектов, связанных с данными. Согласуйте разнородные данные в рамках семантической бизнес-	Умные приложения для работы с данными, основанные на вашем опыте и информации. Развивайте традиционные транзакционные системы,	Доступ к важнейшей аналитике. Усиьте бизнес-аналитику с помощью отраслевых решений, основанных на готовом бизнес-контенте.

<p>модели, учитывающей разнообразие данных.</p>	<p>давая разработчикам инструменты для создания приложений с генеративным ИИ, контекстной адаптацией и безопасным доступом к критически важным бизнес-данным.</p>	
<p>Оптимизация структуры данных. Обеспечьте быстрый и удобный доступ к данным в гибридных и облачных средах, независимо от их местонахождения.</p>	<p>Максимальная производительность и надежная защита. Освободите разработчиков от рутинных административных задач, направив их усилия на инновации, благодаря гибкому масштабированию и встроенным системам безопасности, соответствия нормативным требованиям и обеспечения высокой доступности.</p>	<p>Революция в корпоративном плане. Создайте условия для совместного плана, интегрируя финансовое, логистическое и операционное планирование в единую систему.</p>

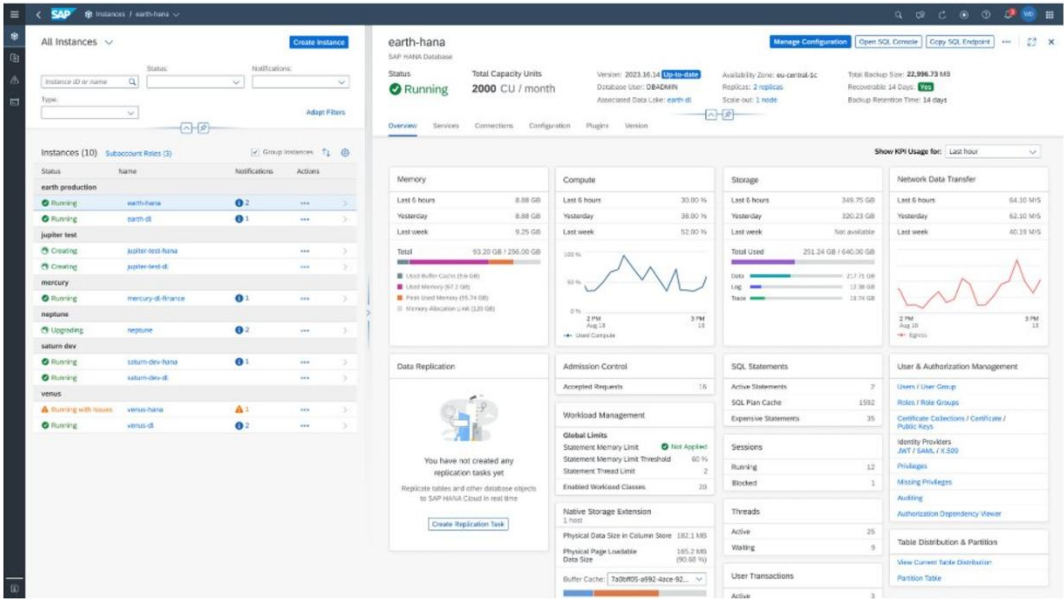


Рисунок 4 – Пример функционала SAP HANA

Наряду с системой SAP есть другие ERP-системы такие как 1C, Bitrix24.

1C – система для автоматизации управления и учета на предприятиях. Она объединяет в себе все функции и сферы компании [10].

Bitrix24 – облачная система, которая дает возможность автоматизировать процессы, управлять проектами, документами, коммуникациями и другими аспектами работы предприятия.

Теперь проведем анализ трех ERP-систем по определенным показателям:

Таблица 2 – Сравнение ERP-систем (SAP, 1C:ERP, Bitrix24)

Показатели	SAP	1C:ERP	Bitrix24
Тип системы	Комплексная	Комплексная	система CRM с элементами ERP
Области применения	Все сферы предприятия	Бухгалтерия, управление складом, производством, продажами, персоналом	Взаимоотношениями с клиентами, сервисы маркетинга и продаж.
Функционал	Большой спектр функций для всех сфер	Автоматизация бизнес-процессов	Для сервисов взаимодействия с клиентами
Масштабируемость	Любой размер отрасли и компании	Средний и крупный бизнес	Малый и средний бизнес
Сложность внедрения	Сложное	Среднее	Простое
Интеграция с другими системами	Интегрируется	Интегрируется	Интегрируется
Безопасность	Высокая	Средняя	Средняя

Как видно из таблицы, SAP и 1C:ERP схожи не только по типу системы, но и в применении. Bitrix24 в первую очередь является системой CRM с элементами ERP, она легче всего внедряется, по сравнению с SAP и 1C.

Подытожим: ERP-системы – эффективные инструменты, предназначенные для оптимизации и объединения бизнес-процессов, увеличения производительности компании и улучшения качества товаров и услуг. Они позволяют свести информацию из разных подразделений в единую систему, автоматизировать процессы, формировать отчёты и анализировать данные, что содействует принятию более обоснованных решений. Среди наиболее востребованных ERP-систем можно отметить SAP, 1C:ERP и Bitrix24. Каждая из них обладает своими характеристиками, сильными и слабыми сторонами, поэтому выбор подходящей системы зависит от потребностей и задач компании [11].

Список литературы

1. Басовский Л.Е. ERP-системы: основы и перспективы развития. – М.: Инфра-М, 2021.
2. Гапоненко А.Л., Карпов А.В. Современные ERP-системы: управление бизнес-процессами. – СПб.: Питер, 2020.
3. Дыханова Е.В. Внедрение ERP-систем в российских предприятиях: проблемы и решения // Экономика и управление. – 2022. – №3. – С. 45–52.
4. Сидоров П.Н. Автоматизация бизнес-процессов с использованием ERP-систем. – М.: Альпина Паблишер, 2019.
5. Чернов В.В. SAP ERP: теория и практика внедрения. – СПб.: БХВ-Петербург, 2021.
6. 1C:ERP. Практическое руководство по внедрению / Под ред. Иванова С.В. – М.: 1C-Паблишинг, 2022.

7. Bitrix24: CRM и ERP в одном решении / Официальная документация. – Доступ: www.bitrix24.ru
8. SAP HANA: облачные технологии и аналитика / Руководство по использованию. – Доступ: www.sap.com
9. Козлов М.Г. Сравнительный анализ ERP-систем: SAP, 1C и Bitrix24 // Вестник цифровой экономики. – 2023. – №5. – С. 22–30.
10. Официальный сайт 1C:ERP. – Доступ: www.1c.ru
11. Глобальные исследования рынка ERP-систем // Gartner Research, 2023. – Доступ: www.gartner.com
12. ERP-системы и цифровая трансформация бизнеса / Под ред. Смирнова А.В. – М.: Экономика, 2023.

References

1. Basovsky L.E. ERP systems: fundamentals and prospects of development. Moscow: Infra-M, 2021.
 2. Gaponenko A.L., Karpov A.V. Modern ERP systems: business process management. St. Petersburg: Peter, 2020.
 3. Dykhanova E.V. Implementation of ERP systems in Russian enterprises: problems and solutions // Economics and management. 2022. No. 3. pp. 45-52.
 4. Sidorov P.N. Automation of business processes using ERP systems. Moscow: Alpina Publisher, 2019.
 5. Chernov V.V. SAP ERP: theory and practice of implementation. – St. Petersburg: BHV-Petersburg, 2021.
 6. 1C:ERP. Practical Implementation Guide / Edited by Ivanova S.V. Moscow: 1C Publishing, 2022.
 7. Bitrix24: CRM and ERP in one solution / Official documentation. – Access: www.bitrix24.ru
 8. SAP HANA: Cloud Technologies and Analytics / Usage Guide. – Access: www.sap.com
 9. Kozlov M.G. Comparative analysis of ERP systems: SAP, 1C and Bitrix24 // Bulletin of Digital Economy. – 2023. – No.5. – pp. 22-30.
 10. Official website of 1C:ERP. – Access: www.1c.ru
 11. Global ERP Systems Market Research // Gartner Research, 2023. – Access: www.gartner.com
 12. ERP systems and digital business transformation / Edited by A.V. Smirnova– Moscow: Ekonomika Publ., 2023.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.5

ПРОГНОЗИРОВАНИЕ СОСТОЯНИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ, МЕТОДЫ И ПОДХОДЫ, ЛЕЖАЩИЕ В ЕГО ОСНОВАНИИ

Васильев А.В.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: light7591@gmail.com

Осуществление прогнозирования состояния вычислительных систем выполняется при помощи таких методов и инструментов, как метод предиктивного обслуживания, нейросети и автокодировщики с задействованием искусственного интеллекта (ИИ). Данные методы и инструменты широко применяются для решения разнообразных задач в настоящее время. Целью данного исследования является описание работы данных методов и приведение соответствующих примеров. В работе использовались общенаучные методы: анализ теоретических источников, сбор информации, описание. Изложение описания работы данных методов позволяет понять их применение в прогнозировании состояния вычислительных систем и обеспечить дальнейшую бесперебойную работу данных систем.

Ключевые слова: Предиктивное обслуживание, нейросети, автокодировщики, искусственный интеллект, метрики, временные ряды.

FORECASTING OF THE CONDITION OF COMPUTATIONAL SYSTEMS AND UNDERLYING METHODS AND APPROACHES

Vasilyev A.V.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: light7591@gmail.com

Performing of forecasting of the condition of computational systems is done by means of methods and approaches such as the method of predictive maintenance, neural networks and auto-encoders with the use of artificial intelligence (AI). The given methods and tools are widely used to solve different problems nowadays. The purpose of the given research is description of the given methods and presenting of corresponding examples. General scientific methods were used in the work: analysis of theoretical sources, collection of information, description. Laying out of a description of work of such methods lets understand their application in forecasting of the condition of computational systems and provide further faultless work of the given systems.

Keywords: Predictive maintenance, neural networks, autoencoder, artificial intelligence, metrics, time series.

Введение

При эксплуатации вычислительных систем происходят сбои, которые влияют на возможность использования самих данных систем, корректность обработки ими различных данных и выдаваемых ими результатов. Таким образом, методы, которые могут предсказывать состояние вычислительной системы, являются очень важными инструментами.

За предотвращение сбоев в работе вычислительных систем и предсказание состояния данных систем может отвечать множество инструментов (как программных, так и аппаратных). Однако предметом рассмотрения настоящей статьи являются нейросети[2, 3], как один из инструментов для прогнозирования состояния вычислительных систем, а также

концепция предиктивного обслуживания. Рассматриваются принципы работы нейросетей и предиктивного обслуживания с приведением реальных примеров их работы.

1. Постановка проблемы

Для обнаружения неполадок в работе вычислительных систем и соответственно для предсказания состояния данных систем используется множество методов. При рассмотрении можно выделить некоторые основные методы, которые широко используются в настоящее время. Для того, чтобы эффективно использовать данные методы, требуется понимать принципы, лежащие в их основе. Также понимание работы данных методов может быть использовано при разработке новых методов, направленных на прогнозирование состояния вычислительных систем.

Ввиду все более и более увеличивающегося использования данных систем в повседневной жизни и возможных больших потерь в случае их сбоя, необходимо понимать идеи, лежащие в основе методов прогнозирования состояния данных систем и успешно разрабатывать новые подходы к прогнозированию их состояния в целом.

2. Описание изучаемого предмета статьи

Нейронные сети – основной инструмент для прогнозирования состояния вычислительных систем. Искусственная нейронная сеть состоит из нейронов и связей между ними. Информация, как правило, подается на вход нейронной сети и выдается на её выходе. Существуют несколько архитектур нейронных сетей (DNN, CNN, RNN и т. д.).

Среди разновидностей данных сетей особым образом выделяются автокодировщики, работающие по несколько другому принципу – восстановлению информации, поданной на их вход.

При создании нейронных сетей, направленных на обнаружение аномалий в работе вычислительных систем, обширно используется подход, имеющий в своей основе предиктивное обслуживание (англ. predictive maintenance). Его сущность заключается в том, что в процессе поиска неполадок, которые могут спровоцировать отказ или ухудшить серьёзным образом работу системы, задействуется искусственный интеллект.

3. Цель работы

Цель данного исследования заключается в приведении краткого обзора методов и концепций, которые могут быть задействованы для цели прогнозирования состояния вычислительной системы, а также рассмотрение принципов функционирования данных методов с приведением примеров.

4. Методы исследования

Для выполнения исследования по рассматриваемой теме задействовались как российские, так и зарубежные источники информации. В самой работе были использованы различные методы исследования, такие как анализ научной литературы и научных статей по теме исследования.

5. Результаты исследования

Нейросети и основные принципы их функционирования

Одним из основных инструментов, используемых в процессе действий, направленных на прогнозирование состояния вычислительных систем, является искусственная нейронная сеть (англ. artificial neural network, ANN), модель (описание) для которых впервые была создана в 1940-х годах и базировалась на алгоритмах, называемых пороговой логикой (англ. threshold logic, TL)[1]. Запуск же работающей нейронной сети был впервые осуществлён Фарли Белмонтом и Уэсли Кларком из MIT (Massachusetts Institute of Technology) в 1954 году[2, 5]. Как правило, множество авторов в своих соответствующих научных статьях ([2, 3, 4, 7, 8, 9], характеризуют искусственные нейронные сети следующим образом: внутренняя структура нейронных сетей создана в соответствии с принципом организации и работы биологических нейронных сетей. Нейронная сеть состоит из нейронов и связей между ними (чаще всего имеются ввиду связи между слоями нейронов). Межнейронные связи при этом могут быть какими угодно (это задается структурой самой сети). Каждая связь способна передавать сигнал от одного другим нейронам (слоям нейронов). Искусственный нейрон принимает сигнал и после обработки пересылает его другим нейронам. Данный выходной сигнал является продуктом от вычисления (обработки), которое осуществляется по некоему правилу (правилам) от совокупности (суммы) сигналов на его входах (входах нейрона). Стрелками на схеме указаны пути от выхода одного нейрона ко входу другого. В машинном обучении широко рассматривается концепция “черного ящика”[13, 14, 15], когда неизвестно, что происходит внутри рассматриваемой системы. Таким образом, искусственная нейронная сеть фактически представляет собой “черный ящик” с входами и выходами [16].

Рассмотрим более подробно искусственные нейронные сети. В учебном пособии Гафарова Ф.М. и Галимянова А.Ф.[4], а также в статьях других авторов [7, 9] приведены дальнейшие краткие характеристики данных сетей и разъяснены понятия, связанные с ними. Соединения (связи) между нейронами называются ребрами. Ребра обычно имеют некий вес (иногда называемый синаптическим), который изменяется по мере обучения нейронной сети[9] (в этом заключается главное свойство нейросетей)[4]. Вес служит для регулировки (уменьшения или увеличения) сигнала, передаваемого по соединениям (связям, ребрам). Сами нейроны могут иметь некий порог, только по преодолении которого путем получения сигналов от остальных нейронов сигнал будет передан дальше данным нейроном.

Рассмотрим более подробно само функционирование искусственной нейронной сети. Дать описание связи в ней можно при задействовании трех определяющих:

1. Сущность, от которой идет связь (как правило, это нейрон).
2. Принимающая сущность (нейрон, к которому связь проложена).
3. Вес самой связи.

В данном перечне имеет смысл более подробно разобрать как раз пункт №3. Как упоминалось выше, вес рассматриваемой связи задает, будет ли сигнал увеличен (усилен) или ослаблен (уменьшен). К примеру, пусть имеются два каких-либо нейрона. Выходной сигнал первого равен 8. Вес связи равен 5. Тогда входной сигнал второго нейрона будет равен $8 \cdot 5$. Т.е. в данном простейшем случае необходимо умножить значение этого сигнала на вес связи. Если же сигнал не один, то необходимо выполнить суммирование их всех. Таким образом, на входе второго нейрона будет получено следующее:

$$\text{net}_j = \sum_{i=1}^N x_i \cdot w_{ij}$$

В левой части этого выражения находится общий входной сигнал второго нейрона, а в правой – сумма всех выходных сигналов первого, умноженных на вес связи между нейронами. Само собой разумеется, что в реально существующих искусственных нейронных сетях существует множество нейронов и соответствующих им различных связей. Для описания и работы с такой сетью вводится понятие весовой матрицы (матрицы весов)[6]. Данное понятие требует более детального рассмотрения.

Таблица 1. Весовая матрица (матрица весов)

0	-0.4	-5.6	4.7	0
1.2	0	3	0	2.4
0	0	0	-3.3	7.5
-2.4	0	0	0	2.5
0	0	0	0	0

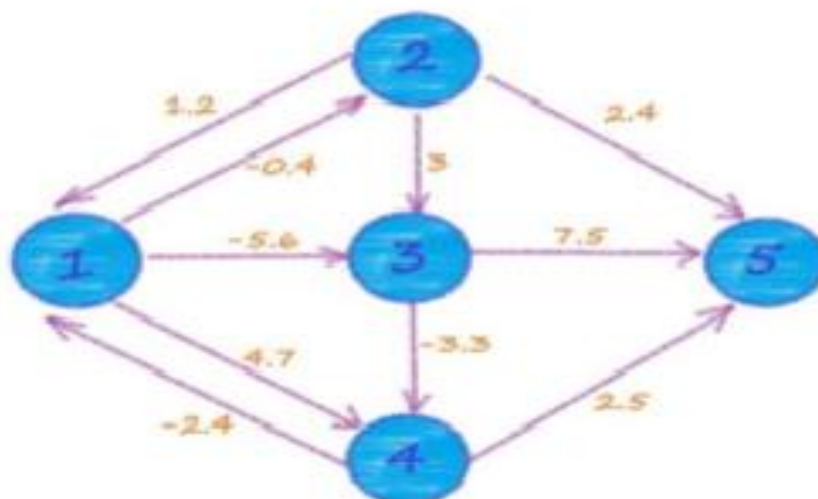


Рисунок 1- Схема нейронной сети со множеством нейронов.

При взгляде на рисунок ясно видно, что, например, от третьего элемента к пятому (или от первого к четвертому) проходит связь с весом 7.5 (или же соответственно 4.7). При рассмотрении же весовой матрицы (таблица 1) видно, что число 7.5 находится в третьей строке и пятом столбце, а число 4.7 – в первой строке и четвертом столбце, что точным образом согласуется с Рисунком 1.

Выходные (исходящие) сигналы также заслуживают подробное рассмотрение как понятие, непосредственно относящееся к нейронным сетям. Существует определенное правило, которому подчиняется каждый элемент сети, в соответствии с которым из значений суммарного (общего или комбинированного) входа (входов) элемента сети подсчитывается его исходящее (выходное) значение. Данное правило имеет название “функция активации”. Исходящее же, или выходное значение имеет название “активность нейрона”. В качестве первого понятия могут быть любые математические функции. Их можно упрощенно классифицировать следующим образом:

1. Пороговая функция (или же порог, англ. threshold)[8] – в случае нахождения суммарного ввода (совокупности значений) ниже некоего другого значения (порога), то активность будет равна нулю, в противном случае – единице.

2. Логистическая функция (функция логики).

В настоящее время возможна реализация простейшей нейросети даже на обычном персональном компьютере с использованием того или иного языка программирования (к примеру, языка Python)[10] и с применением различных библиотек (к примеру, TensorFlow или Theano), а также фреймворков (PyTorch).

Применение нейронных сетей в настоящее время весьма и весьма многообразно [11, 12]. Как правило, это создание изображений, их восстановление, синтез речи и текста, распознавание изображений и вообще работы, связанные с искусственным интеллектом. Некоторыми авторами в своих научных статье даже осуществляются попытки рассмотреть вероятность того, что окружающий мир и есть нейросеть[17]. Однако предметом подробного рассмотрения в настоящей статье являются реально используемые методы, направленные на осуществление прогнозирования состояния вычислительной системы.

Предиктивное обслуживание и методы, используемые для его реализации

Сущность предиктивного обслуживания заключается в том, что искусственный интеллект (ИИ, англ. AI – artificial intelligence) задействуется для нахождения (обнаружения) неполадок, способных привести к отказу или серьезному ухудшению работы системы. При этом состояние рассматриваемой системы фактически непрерывно контролируется специализированными методами (т.е. осуществляется мониторинг данной системы). На основе показателей рассматриваемой системы и степени их отклонения от модели осуществляется прогноз её состояния. При этом нет никакой необходимости, чтобы данная система была именно вычислительной и при этом, разумеется, возможно, что прогнозительная (прогностическая, предсказательная) сущность предиктивного обслуживания может быть применена в области, кардинально отличающейся от информационных технологий. Рассмотрим данную особенность предиктивного обслуживания на примерах.

В своей статье группа авторов рассматривает модель предиктивного обслуживания с применением дополнительных ресурсов (в данном случае имеются в виду сенсорные сети)[18], т.е. рассматривается одна из систем, к которой данный метод применим. Данной группой авторов предложена модель рассматриваемого метода прогнозирования состояния системы на основе беспроводной сети датчиков. Данные датчики используются как поставщики данных о состоянии оборудования. Проанализированы принципы построения беспроводных сенсорных сетей и определен протокол передачи данных и, как результат, определена сама концепция системы предиктивного обслуживания при помощи указанных технологий.

Из анализа статьи[18] очевидно, что рассматриваемая в статье схема хотя и является схемой оборудования, а не программного обеспечения, но при этом она устроена похожим образом по сравнению с схемами систем и программных комплексов, задействующими предиктивное обслуживание. В рассматриваемой системе оборудования при использовании датчиков данные сохраняются в некой базе данных. При этом существует также база данных, содержащая аномалии. Информация, полученная в процессе мониторинга системы,

рассматривается применительно к базе аномалий и это позволяет методом предиктивного обслуживания спрогнозировать полные или частичные вероятные отказы оборудования. При этом возможно получение сохраненных данных в виде графиков (т.е. временных рядов) и последующее отображение на экране оборудования мониторинга рассматриваемой системы.

Рассмотренная модель кратко иллюстрирует применение предиктивного обслуживания. Похожая система (и также с применением датчиков) описывается в статье[19]. Авторы данной статьи рассматривают роторные машины как поставщики данных. Так как в исследуемом случае задача состоит в поддержании определенной частоты вращения ротора, то здесь опять приходит на помощь предиктивное обслуживание. Путем сравнения информации с датчиков с некой моделью может поддерживаться тем или иным способом нужная частота вращения ротора и/или делаться прогноз относительно состояния системы. Авторами также сделано ценное замечание о развитии предсказательной (предиктивной) аналитики вместе с наукой о данных и применении для прогнозирования систем методов машинного обучения, а также нейронных сетей, как уже и рассматривалось в данной работе и работах других авторов.

Данные два примера кратко описывают применение и прогностическую сущность предиктивного обслуживания, а также возможные системы, для мониторинга которых может использоваться данный метод. Имеет смысл рассмотреть более тщательно задействованные вместе с предиктивным обслуживанием методы для предсказания состояния систем. Один из авторов описывает в своей статье[20] предиктивное обслуживание при помощи предсказательных, или же суррогатных, моделей, анализируя при этом специальные черты проблем детектирования аномалий и предсказания отказов и при этом снова делается упоминание математического аппарата и машинного обучения в задачах предиктивного обслуживания. В силу того, что временные ряды могут быть многомерными, наиболее приемлемой в рассматриваемом подходе является так называемая модель многообразия, которая является довольно распространенной при рассмотрении данных случаев, а также породила новый тренд в машинном обучении (моделирование многообразий, англ. manifold learning)[21, 22].

Основная математическая идея, предложенная автором в рассматриваемой статье[20], заключена в следующем:

1. Через $\{x_t\}_{t \geq 1}$ обозначается d -мерный наблюдаемый сигнал телеметрии (показаний).
2. Для всех $i = 1, \dots, d$ осуществляется составление суррогатной модели, определяющей зависимость $x_{i,t}$ от значений всех показателей сигнала $\{x_{1,s}, \dots, x_{i-1,s}, x_{i+1,s}, \dots, x_{d,s}\}$ для $s = t - L_i, \dots, t$ как в данный момент, так и в моменты времени в прошлом на основе данных, которые соответствуют нормальному состоянию работы системы.
3. Задается (определяется) некий порог h для обнаружения аномалий. При этом подразумевается, что в обычном состоянии вероятность превышения порога значением сбоя достаточно мала. Для осуществления моделирования данной вероятности задействуется модель на основе гауссовских процессов.
4. Тревога объявляется, если ошибка прогноза для наблюдений в настоящий момент выше h .

Автором рассмотрено задействование указанной методологии при работе некой установки. Данные о нормальном состоянии системы в прошлом были представлены в виде

временных рядов множества параметров. Данные временные ряды зависят от времени крайне неоднородно и не наблюдается четкой зависимости. Присутствует шум в данных.

Для построения показателя ухудшения работы системы были задействованы следующие предположения:

1. Информация о периоде с ноября - 12 по ноябрь -13 классифицировалась как нормальные данные.
2. Со старта наблюдений и до октября - 12 рассматриваемые временные ряды характеризуются высокими вариациями. Это может быть как неправильный режим работы самой установки, так и шум в рассматриваемых данных. Соответственно, для обучения модели эти данные не могут быть использованы никоим образом.

Чтобы построить показатель (индикатор) деградации системы, были исполнены следующие действия:

1. Произведена постройка суррогатных моделей зависимости различных получаемых параметров друг от друга. Соответственно, получаемые значения рассматриваемого многомерного временного ряда будут описывать на каком-то многообразии некую нелинейную траекторию.
2. Спрогнозированы значения рассматриваемых временных рядов на пробном множестве (для рассматриваемого множества и требуется выявить присутствие неких аномальных режимов рассматриваемой системы).

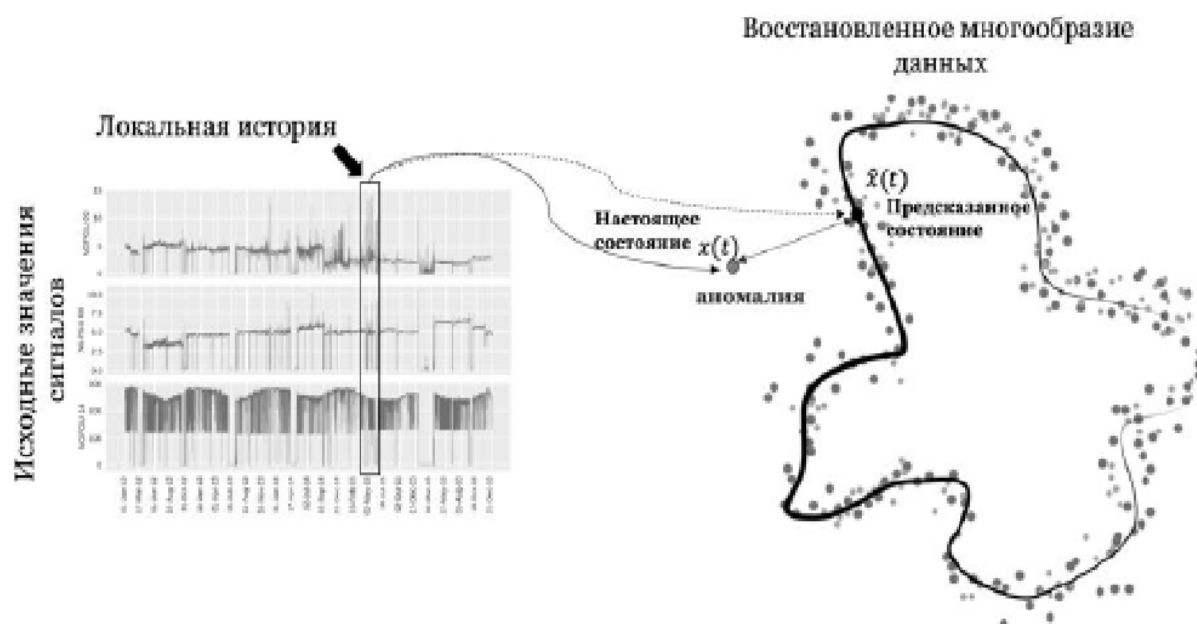


Рисунок 2 - Подход к детектированию аномалий на основе многообразия данных.

3. Осуществлен подсчет ошибок прогнозирования.
4. Подсчитаны ошибки прогнозирования на некой обучающей выборке (обучающем множестве).
5. Выполнено сравнение ошибок на двух выборках (множествах), т.е. на обучающей и тестовой. Как таковые задействованы:

- а) показатель превышения значением ошибки границы в настоящий момент, определяемый самой большой ранее замеченной (при нормальном режиме) ошибкой;
- б) р-значение предположения о превышении значением ошибки, наблюдаемой в настоящий момент, границы, заданной самой большой замеченной ранее (при нормальном режиме) ошибкой.

Соответственно, автор делает следующие выводы: данные показывают медленную деградацию системы со стартом примерно в середине 2014 года; в процессе тестов “вслепую” (при помощи данных, которые были неизвестны до момента тестирования модели) были детектированы аномалии (базируясь на основе анализа исходных данных, т.е. никакой информации о реальных днях остановки и т.п. рассматриваемой установки не было). При этом:

1. Обнаруженные аномалии соответствуют отключениям (как запланированным, так и неожиданным).

2. Аномалии же, характеризующие незапланированные остановки, были определены намного раньше моментов, когда возникли сами ситуации (на рисунке в статье видно, что первая аномалия, найденная за два дня до критической остановки системы 31.12.2015, детектирована на два дня раньше, а вторая же, обнаруженная в апреле также 2015 года, произошла до остановки системы 02.05.2015).

Таким образом, приведенный в статье автором метод (подход) в целом работает. И, разумеется, ввиду прогностической сущности предиктивного обслуживания он всецело может быть применен и к соответствующим метрикам вычислительных систем.

Выше был рассмотрен метод реализации предиктивного обслуживания на определенной системе. Составными частями процесса предсказания состояния системы в данном методе реализации было установление некоего порога аномалии, сбор метрик рассматриваемой системы и установление факта сбоя системы на основании собранных данных. Но существует и другой подход, упомянутый в данной работе выше, который представляет фактическое предсказание отказов рассматриваемой системы, осуществлённый путём написания автокодировщика (или автоэнкодера). Автокодировщик - нейронная сеть, которая способна обучаться без учителя (unsupervised learning). Но, несмотря на это, требуется всё же задействовать её первоначальное обучение, используя, например, такие программные библиотеки, как TensorFlow или же PyTorch. Имеет смысл рассмотреть работу автокодировщика, как один из методов реализации предиктивного обслуживания, более подробно.

Основным принципом работы автокодировщика является получение на выходном слое отклика, максимально похожего на входной. При этом фактически осуществляется процедура восстановления (реконструкции) первоначальной информации, поданной на вход автокодировщика. Кратко реализация автокодировщика показана на Рисунке 3.

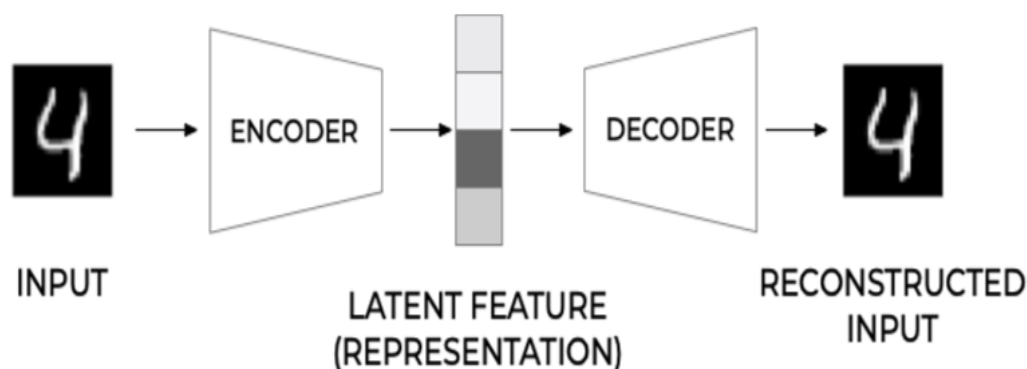


Рисунок 3 - Краткий принцип работы автокодировщика.

Математически же работу автокодировщика можно описать следующим образом:

1. Первый слой (кодирующий) может быть задан функцией $h_i = g(x_i)$, где h – выходная информация блока кодирования (англ. encoder). Декодированный же слой может быть задан функцией $x_i = f(h_i) = f(g(x_i))$.
2. Соответственно, обучение автокодировщика может быть представлено в виде поиска таковых функций g и f , при которых верно выражение:

$$\arg \min_{f,g} [\Delta(x_i, f(g(x_i)))] >$$

Символ “дельта” здесь означает разницу между входной информацией входного слоя и, соответственно, выходной информацией выходного слоя. Очевидно, что при данном подходе неизбежны потери информации. Так как автокодировщиков существует множество, при их конструировании применяется множество методов для сглаживания в определенной мере данной разницы. Рассмотреть абсолютно все методы в рамках одной работы не представляется возможным, но в целом основные стратегии при разработке автокодировщиков заключаются в создании т.н. “бутылочного горлышка” (англ. bottleneck) и стратегии представления (англ. representation). Первая стратегия кратко и упрощенно может быть характеризована как представление размерности выходной информации декодера ниже (иногда намного ниже), чем у входной информации (англ. input). Вторая же может быть описана также математическими формулами, как и сам принцип функционирования автокодировщика, но самый простой способ её достижения может заключаться в простом уравнивании весовых характеристик кодировщика и декодера, т.е. “привязывании” их друг к другу (т.к. автокодировщик является нейросетью, он характеризуется кратким описанием нейросетей).

В чем же заключаются недостатки рассмотренных методов, направленных на поддержание работоспособности вычислительных (и не только) систем? В первую очередь, очевидным является человеческий фактор, т.к. администратор системы может просто не установить порог срабатывания, выше которого загрузка вычислительной системы может считаться аномальной. Также очевидно из рассмотренной в данной работе, к примеру, статье [18] по прогнозированию состояния системы на основе беспроводной сети датчиков очевидно, что реализация предиктивного обслуживания потребует также создания БД аномалий и возможности непрерывного к ней доступа со стороны остальных частей комплекса, осуществляющего контроль за состоянием системы (т.е. малейшая несогласованность, потеря питания в сети и т.п. могут серьезно повлиять на результат).

При более глубоком рассмотрении также очевидно, что в метриках, выдаваемых системой, за которой осуществляется наблюдение, возможны шумы, что, в свою очередь, влияет на точность предсказания состояния системы. Также необходимо бороться с ложными срабатываниями. Относительно нейросетей очевидно, что необходима всегда свежая модель, на которой обучается нейросеть, а также совершенствование методов сравнения текущего состояния системы с моделью. При рассмотрении же автокодировщиков было выявлено, что они сами по себе допускают потерю информации (т.е. возможна ошибка в прогнозировании отказа) и при их разработке, соответственно, необходимо применять стратегии, отличные от разработки простых нейронных сетей (т.е. стратегии, позволяющие сделать потери информации как можно меньше).

Заключение и выводы

Существуют множество методов, направленных на прогнозирование состояния вычислительной системы. Это могут быть как аппаратные средства, так и программные. Для дальнейшей работы в направлении предсказания состояния вычислительной системы используются нейросети и технологии, связанные с ними (которые могут быть описаны математически), а также различные математические модели. При анализе данных средств было выявлено наличие у них определенных недостатков, минимизация которых может быть достигнута в большинстве случаев через совершенствование методов и архитектур, лежащих в основе данных средств.

Список литературы

1. Warren McCulloch, Walter Pitts. A logical calculus of ideas immanent in nervous activity/Warren McCulloch, Walter Pitts. Bulletin of mathematical biophysics, 5, С. 115-133.
2. Ксенофонтов В.В. Нейронные сети/ Ксенофонтов В.В.. Cyberleninka.ru, 2019.
3. Степанов П.П. Искусственные нейронные сети/ Степанов П.П. “Молодой ученый”, №4(138), 2017.
4. Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и приложения/Гафаров Ф.М., Галимянов А.Ф.. Учебное пособие. Издательство Казанского университета, 2018.
5. B.Farley, W.Clark. Simulation of self-organizing systems by digital computer/B.Farley, W.Clark. IRE transactions on information theory, 4 (4), С.76-84.
6. Рашитов Э.Э., Стоякова К.Л. Модель математической нейронной сети/ Рашитов Э.Э., Стоякова К.Л., Ибрагиев Р.Р. “Молодой ученый”, №15(149), 2017.
7. Журавлева Л.В., Стригулин К.А.. Исследование особенностей развития нейронных сетей в современном мире/ Журавлева Л.В., Стригулин К.А.. IV международная научная конференция “Технические науки: проблемы и перспективы”, 2016.
8. Мелихова О.А., Гайдуков А.Б., Джамбинов С.В., Чумичев В.С. Методы поддержки принятия Решений на основе нейронных сетей/Мелихова О.А., Гайдуков А.Б., Джамбинов С.В., Чумичев В.С.. Журнал “Актуальные проблемы гуманитарных и естественных наук”, ISSN: 2073-0071, № 9-1, С.51-59, 2015.
9. Омаров Т.З. Концепция искусственной нейронной сети/ Омаров Т.З. “Современные научные исследования и инновации”. № 5, 2016.

10. Альбовский А.В., Егоров Н.А., Романюк А.Г. Реализация нейронной сети на языке программирования Python/ Альбовский А.В., Егоров Н.А., Романюк А.Г., МГТУ Н.Э. Баумана. DOI: 10.24411/2520-6990-2020-11582. Cyberleninka.ru., 2020.
11. Фаустова К.И. Нейронные сети: применение сегодня и перспективы развития/ Фаустова К.И.. Cyberleninka.ru, 2017.
12. Цаунит А.Н. Перспективы развития и применения нейронных сетей/ Цаунит А.Н.. "Молодой ученый" №23 (365), 2021.
13. Yiran Huang, Yexu Zhou, Michael Hefenbrock. Till Riedel, Likun Fang, Michael Beigl. Universal distributional decision-based black-box Adversarial attack with reinforcement learning/ Yiran Huang, Yexu Zhou, Michael Hefenbrock. Till Riedel, Likun Fang, Michael Beigl. arXiv.org, 2022.
14. Diptikalyan Saha, Aniya Aggarwal, Sandeep Hans. Data synthesis for testing black-box machine learning models/ Diptikalyan Saha, Aniya Aggarwal, Sandeep Hans. arXiv.org, 2021.
15. Cynthia Rudin. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead/ Cynthia Rudin. arXiv.org, 2018.
16. Seong Joo Oh, Max Augustin, Bernt Schiele, Mario Fritz. Towards Reverse-Engineering Black-box neural networks/ Seong Joon Oh, Max Augustin, Bernt Schiele, Mario Fritz. arXiv.org, 2017.
17. Vitaly Vanchurin. The world as a neural network/ Vitaly Vanchurin. arXiv.org, National library of medicine, 2020.
18. Власов А.И., Григорьев П.В., Кривошеин А.И. Модель предиктивного обслуживания оборудования с применением беспроводных сенсорных сетей/ Власов А.И., Григорьев П.В., Кривошеин А.И.. DOI 10.21685/2307-4205-2018-2-4. Cyberleninka.ru, 2018.
19. Ильичев В.Ю., Юрик Е.А. Использование методов предиктивной аналитики для обработки сигналов с датчиков частоты вращения роторных машин/ Ильичев В.Ю., Юрик Е.А.. Журнал "Научное обозрение. Технические науки". №1, с. 22-26, 2019.
20. Бурнаев Е.В. Обнаружение аномалий на основе суррогатных моделей/ Бурнаев Е.В., Сколковский институт науки и технологий, cyberleninka.ru, 2020.
21. Pavan K.Turaga, Rushil Anirudh, Rama Chellappa. Manifold learning/ Pavan K.Turaga, Rushil Anirudh, Rama Chellappa. Researchgate.net, 2020.
22. Hamid Reza Yazdani. Introduction to manifold learning/ Hamid Reza Yazdani. Researchgate.net, 2018.

References

1. Warren McCulloch, Walter Pitts. A logical calculus of ideas immanent in nervous activity / Warren McCulloch, Walter Pitts. Bulletin of mathematical biophysics, 5, pp 115-133.
2. Xenophontov V.V. Neuronnie SETI/ Xenophontov V.V.. Cyberleninka.ru, 2019.
3. Stepanov P.P. Iskusstvennie neuronnie SETI / Stepanov P.P. "Molodoy ucheniy " < BR > , №4(138), 2017.
4. Gafarov F.M., Galimyanov A.F. Iskusstvennie neuronnie Seti I prilogenia/ Gafarov F.M., Galimyanov A.F.. Uchebnoe posobie. Izdatelstvo Kazanskogo universiteta, 2018.
5. B. Farley, W.Clark. Simulation of self-organizing systems by digital computer/ B. Farley, W.Clark. IRE transactions on information theory, 4 (4), pp 76-84.

6. Rashitov E.E., Stoyakova K.L. Model matematicheskoy neuronnoy SETI/ Rashitov E.E., Stoyakova K.L., Ibragiev R.R. "Molodoi uchenii", №15(149), 2017.
 7. Juravleva L.V., Strigulin K.A.. Issledovanie osobennostey razvitiya neuronnykh setey V sovremennom mire / Juravleva L.V., Strigulin K.A.. IV mezhdunarodnaya nauchnaya conference " Technicheskie nauki: perspective of problem I", 2016.
 8. Melikhova O.A., Gaidukov A.B., Djambinov S.V., Chumichev V.S. Metodi podderjki prinyatiya Resheniy na osnove neuronnykh setey / Melikhova O.A., Gaidukov A.B., Djambinov S.V., Chumichev V.S.. Journal " aktualnie problem humanitarnykh i estestvennykh nauk", ISSN: 2073-0071, № 9-1, pp.51-59, 2015.
 9. Omarov T.Z. Concept iskusstvennoy neuronnoy SETI / Omarov t.Z. "Sovremennye nauchnye issledovaniya i innovatsii". № 5, 2016.
 10. Albovsky Compiled A.V., Egorov N.A., Romanyuk A.G. Realism neuronnoy SETI na yazyke programmirovaniya Python / Albovsky a.V., Egorov N.A., Romanyuk A.G., MGTU N.E. Bauman. DOI: 10.24411 / 2520-6990-2020-11582. Cyberleninka.ru., 2020.
 11. Faustova K.I. Neuronnyye seti: primeneniye Segodnya i perspective razvitiya/ Faustova K.I. Cyberleninka.ru, 2017.
 12. Tsaunit A.N. Perspective razvitiya i primeneniya neuronnykh setey / Tsaunit a.N.. "Molodoy ucheniy" №23 (365), 2021.
 13. Yiran Huang, Yehu Zhou, Michael Hefenbrock. Till Riedel, Likun Fang, Michael Beigl. Universal distribution decision-based black-box Adversarial attack with enforcement learning / Yiran Huang, Yehu Zhou, Michael Hefenbrock. Till Riedel, Likun Fang, Michael Beigl. arXiv.org, 2022.
 14. Diptikalyan Saha, Aniya Aggarwal, Sandeep Hans. Data synthesis for testing black-box machine learning models / Diptikalyan Saha, Aniya Aggarwal, Sandeep Hans. arXiv.org, 2021.
 15. Cynthia Rudin. Stop exploiting black box machine learning models for high stakes decisions and use interpretable models instead/ Cynthia Rudin. arXiv.org, 2018.
 16. Seong Joo Oh, Max Augustin, Bernt Schiele, Mario Fritz. Towards Reverse Engineering Black-box neural networks / Seong Joon Oh, Max Augustin, Bernt Schiele, Mario Fritz. arXiv.org, 2017.
 17. Vitaly Vanchurin. The world as a neural network/ Vitaly Vanchurin. arXiv.org, National library of medicine, 2020.
 18. Vlasov A.I., Grigorev P.V., Krivoshein A.I. Model predictivnogo obsluzhivaniya oborudovaniya s primeneniem besprovodnykh sensornykh setey/ Vlasov A.I., Grigorev P.V., Krivoshein A.I.. DOI 10.21685 / 2307-4205-2018-2-4. Cyberleninka.ru, 2018.
 19. Ilichev V.Yu., Yurik E.A. Ispolzovanie metodov predictivnoy analytics dlya obrabotki signalov s datchikov frequency vratscheniya rotornykh Mashin / Ilichev V.Yu., Yurik E.A.. The magazine was published as " Nauchnoye obozreniye. Technicheskie nauki". No. 1, p. 22-26, 2019.
 20. Burnaev E.V. Obnaruzheniye anomaly na osnove surrogatnykh modeley/ Burnaev E.V., Skolkovsky Institut nauki i technologiy, cyberleninka.ru, 2020.
 21. Pawan K. Turaga, Rushil Anirudh, Rama Chellappa. Manifold learning / Pawan K. Turaga, Rushil Anirudh, Rama Chellappa. Researchgate.net, 2020.
 22. Hamid Reza Yazdani. Introduction to manifold learning/ Hamid Reza Yazdani. Researchgate.net, 2018.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.62

РАЗРАБОТКА ГИБРИДНОЙ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПОСТРОЕНИЯ ОТЧЕТНОСТИ С ПРИМЕНЕНИЕМ OLAP И OLTP СИСТЕМ

Серда И.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ilya.sereda2002@mail.ru

В данной работе рассматривается разработка гибридной архитектуры информационной системы для построения отчетности, объединяющей возможности OLAP и OLTP-систем. Предложенный подход использует ClickHouse в качестве высокопроизводительного хранилища для обработки и агрегации больших объемов данных, а также OLTP-базу данных PostgreSQL для хранения предварительно рассчитанных показателей и оперативного доступа к отчетным данным.

Классическая схема аналитики предполагает выполнение всех расчетов и отчетных запросов в OLAP-хранилище, что приводит к высокой нагрузке на систему и увеличению времени отклика. В предлагаемой архитектуре высоконагруженные аналитические вычисления выполняются в OLAP, а полученные агрегированные метрики загружаются в OLTP-хранилище, откуда BI-системы могут быстро извлекать данные с минимальными задержками.

Таким образом, предложенная архитектура представляет собой эффективное решение для построения высокопроизводительных систем отчетности, объединяющее преимущества OLAP и OLTP для оптимального распределения нагрузки и ускоренного доступа к данным.

Ключевые слова: Гибридная архитектура, OLAP, OLTP, построение отчетности, хранилище данных.

DEVELOPMENT OF A HYBRID ARCHITECTURE OF INFORMATION SYSTEM FOR BUILDING REPORTS USING OLAP AND OLTP SYSTEMS

Sereda I.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ilya.sereda2002@mail.ru

This paper considers the development of a hybrid architecture of information system for reporting, combining the capabilities of OLAP and OLTP-systems. The proposed approach uses ClickHouse as a high-performance storage for processing and aggregation of large amounts of data, as well as OLTP-database PostgreSQL for storing pre-calculated indicators and operational access to reporting data.

The classical analytics scheme assumes that all calculations and reporting queries are performed in OLAP-storage, which leads to high load on the system and increased response time. In the proposed architecture, heavy analytical calculations are performed in OLAP and the resulting aggregated metrics are loaded into OLTP storage from where BI systems can quickly retrieve data with minimal latency.

Thus, the proposed architecture is an efficient solution for building high-performance reporting systems, combining the advantages of OLAP and OLTP for optimal load balancing and accelerated data access.

Keywords: Hybrid architecture, OLAP, OLTP, report building, data warehouse.

В современных условиях цифровой трансформации бизнеса эффективное управление данными становится критическим фактором успеха организаций. Рост объемов информации, повышение требований к скорости её обработки и необходимость предоставления аналитических отчетов в режиме, близком к реальному времени, создают потребность в разработке новых архитектурных решений для информационных систем.

Традиционно в корпоративных информационных системах применяется разделение на транзакционные (OLTP) и аналитические (OLAP) системы. OLTP-системы оптимизированы для обработки множества коротких транзакций и обеспечения целостности данных, в то время как OLAP-системы предназначены для сложной многомерной аналитики и агрегации больших объемов данных. Обычно данные перемещаются из OLTP-систем в OLAP через процессы извлечения, преобразования и загрузки (ETL), формируя однонаправленный поток информации.

Однако такой классический подход имеет ряд ограничений. Во-первых, сложность и продолжительность ETL-процессов часто приводит к задержкам в получении актуальной аналитики. Во-вторых, предоставление доступа к OLAP-системам конечным пользователям требует дополнительных ресурсов и компетенций. В-третьих, при увеличении нагрузки на систему отчетности могут возникать проблемы с производительностью, особенно если многие пользователи одновременно выполняют ресурсоемкие аналитические запросы.

В данной статье предлагается альтернативный подход к построению архитектуры информационной системы, основанный на гибридном использовании OLAP и OLTP технологий. Представленная архитектура использует в качестве OLAP-системы СУБД ClickHouse [4] для выполнения сложных аналитических расчетов, а результаты этих расчетов сохраняет в OLTP-базу данных, реализация которой будет осуществлена с помощью СУБД PostgreSQL, в виде предварительно агрегированных витрин данных. Такой подход позволяет объединить вычислительную мощность OLAP-систем с быстродействием и доступностью OLTP-систем для конечных пользователей и инструментов визуализации.

Целью работы является разработка и обоснование гибридной архитектуры информационной системы для построения отчетности, в которой OLAP-хранилище используется для выполнения тяжелых аналитических расчетов, а OLTP-система — для хранения агрегированных показателей и обеспечения быстрого доступа к данным.

OLTP (Online Transaction Processing) и OLAP (Online Analytical Processing) представляют собой два фундаментально различных подхода к хранению и обработке данных [1]. OLTP-системы оптимизированы для высокочастотных транзакций, обеспечивают атомарность операций и целостность данных. Они характеризуются нормализованной структурой хранения, малыми по объему транзакциями и ориентированы на быстрый доступ к отдельным записям. Примерами таких систем являются PostgreSQL, MySQL, Oracle.

OLAP-системы, напротив, предназначены для аналитической обработки больших объемов данных, часто используют денормализованные схемы и колоночное хранение, оптимизированы для сложных запросов, агрегации и выполнения многомерного анализа. К таким системам относятся ClickHouse, Vertica, Snowflake.

Традиционная архитектура аналитических систем [2] обычно включает в себя источники данных (OLTP-системы), ETL-процессы, хранилище данных [3] (чаще всего реализованное как OLAP) и средства визуализации. Данные движутся по направлению от операционных систем к аналитическим, формируя однонаправленный поток. Пример такой архитектуры представлен на Рисунке 1.



Рисунок 1 — Пример традиционной архитектуры аналитической системы

OLAP-системы, такие как ClickHouse, рассчитаны на выполнение сложных аналитических запросов, но они не оптимизированы для частых однотипных запросов. BI-системы и API-приложения могут порождать множество повторяющихся запросов, нагружая OLAP-хранилище. Если BI-инструменты напрямую запрашивают данные из OLAP-системы, нагрузка может увеличиваться, требуя горизонтального масштабирования. Если OLAP-система выходит из строя или сильно перегружена, пользователи не могут получить доступ к отчетности. В традиционной архитектуре нет альтернативного механизма быстрого доступа к предрасчитанным метрикам.

Предлагаемая модель гибридной архитектуры информационной системы представляет собой инновационный подход к организации потоков данных, отличающийся от традиционных решений. В основе данной модели лежит идея оптимального использования сильных сторон OLAP и OLTP систем при построении комплексной инфраструктуры для аналитической отчетности.

Ключевой особенностью предлагаемой архитектуры является изменение направления потока данных после их аналитической обработки. В отличие от традиционного однонаправленного движения данных (от OLTP к OLAP), в разработанной модели присутствует возвратный поток предварительно агрегированных данных из OLAP-систем обратно в специализированные OLTP-хранилища, используемые для обслуживания конечных пользователей.

Концептуально модель включает следующие основные компоненты:

1. Источники данных — традиционные OLTP-системы, генерирующие первичные транзакционные данные в процессе деятельности организации, различные системы, которые отправляют данные напрямую или брокеры сообщений.
2. ETL-процесс — процедура извлечения и загрузки данных из источников в OLAP-систему, а уже впоследствии — обработка и построение логики расчетов показателей.
3. Аналитическое ядро — OLAP-система (в нашем случае ClickHouse), выполняющая сложные аналитические вычисления, агрегацию и формирование витрин данных.
4. Витрины данных в OLTP — специализированная OLTP-система (в нашем случае PostgreSQL), хранящая предварительно рассчитанные метрики и агрегаты в структуре, оптимизированной для быстрого точечного доступа.
5. Оркестрация процессов — система управления потоками данных и регулярными расчетами (в нашем случае Apache Airflow [5;6]), координирующая работу всех компонентов обновления витрин данных.
6. Слой доступа к данным — API и инструменты визуализации (в нашем случае Apache Superset), обеспечивающие конечным пользователям доступ к аналитическим данным из витрин OLTP-хранилища.

Гибридная архитектура информационной системы для построения отчетности представлена на Рисунке 2.

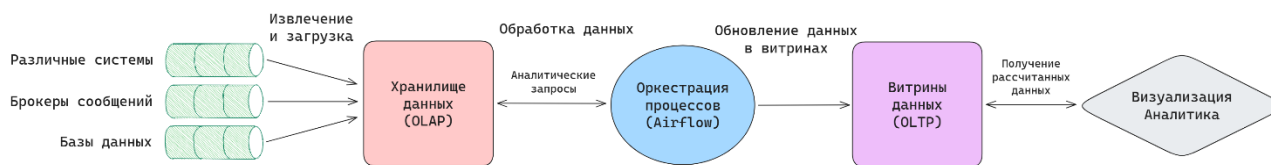


Рисунок 2 — Гибридная архитектура информационной системы для построения отчетности

При такой архитектуре OLAP-система используется по своему прямому назначению — для эффективного выполнения сложных аналитических расчетов над большими объемами данных, но результаты этих расчетов не предоставляются пользователям напрямую, а передаются в OLTP-систему. Это позволяет изолировать ресурсоемкие аналитические процессы от пользовательских запросов и обеспечить высокую производительность при обращении к уже рассчитанным показателям.

Использование ClickHouse в качестве вычислительного ядра позволяет эффективно выполнять сложные аналитические расчеты над большими объемами данных. Хранение предварительно рассчитанных витрин данных в PostgreSQL обеспечивает высокую скорость доступа к аналитическим показателям при обращении конечных пользователей.

Таким образом, предлагаемая гибридная архитектура сочетает вычислительную мощь OLAP-систем с быстродействием и масштабируемостью OLTP-систем, позволяя эффективно решать задачи построения корпоративной отчетности в условиях высоких требований к скорости доступа и значительного количества одновременных запросов:

1. OLAP используется только для сложных расчетов, а OLTP — для хранения готовых агрегированных данных.
2. BI-инструменты и API обращаются не к OLAP, а к OLTP, что снижает нагрузку на аналитическое хранилище.
3. Быстрый отклик отчетов за счет оптимизированных индексов в OLTP.
4. Снижение требований к ресурсам OLAP, так как большинство пользовательских запросов идет в OLTP.
5. Более частое обновление данных, так как в OLTP загружаются уже готовые значения, а не сырые данные, требующие перерасчета.

Список литературы

1. OLTP vs OLAP. // Engineering Resources: [сайт]. — URL: <https://clickhouse.com/engineering-resources/oltp-vs-olap> (дата обращения: 12.02.2025). — Текст: электронный.
2. Марц Н., Уоррен Дж. Большие данные: принципы и практика построения масштабируемых систем обработки данных в реальном времени. — М.: Вильямс, 2016. — 356 с. — Текст: непосредственный.
3. Data Warehouse Architecture. // Geeks for geeks: [сайт]. — URL: <https://www.geeksforgeeks.org/data-warehouse-architecture/> (дата обращения: 31.01.2025). — Текст: электронный.
4. Schulze, R., Schreiber, T., Yatsishin, I., Dahimene, R., & Milovidov, A. ClickHouse-Lightning Fast Analytics for Everyone // 50th International Conference on Very Large Databases. —

Guangzhou, China - August 26-30, 2024. – URL: <https://www.vldb.org/pvldb/vol17/p3731-schulze.pdf> (дата обращения: 29.01.2025). — Текст: электронный.

5. Apache Airflow: официальный сайт – URL: <https://airflow.apache.org/docs/> (дата обращения: 05.02.2025). — Текст: электронный.
6. Харенслак Б., де Руйтер Дж. Apache Airflow и конвейеры обработки данных / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2021. – 502 с. ил. ISBN 978-5-97060-970-5 — Текст: непосредственный.

References

1. OLTP vs OLAP. // Resources Engineering: [website]. — URL: <https://clickhouse.com/engineering-resources/oltp-vs-olap> (date of application: 12.02.2025). — Text: electronic.
 2. N. Martz, D. Stupidly. Big data: a trowel in the practice of not really processing the principle of data system construction in time. Moscow: Williams, 2016. p. 356 — Text: direct.
 3. Data Warehouse Architecture. // Geeks for Geeks: [website]. — URL: <https://www.geeksforgeeks.org/data-warehouse-architecture/> (date of request: 31.01.2025). — Text: electronic.
 4. Schulze, R., Schreiber, T., Yatshishin, I., Dahimene, R., & Milovidov, A. ClickHouse-Lightning Fast Analytics for Everyone // International Conference on Very Large 50th Databases. – Guangzhou, China - August 26-30, 2024. – URL: <https://www.vldb.org/pvldb/vol17/p3731-schulze.pdf> (date of application: 29.01.2025). — Text: electronic.
 5. Apache Airflow: Official website – URL: <https://airflow.apache.org/docs/> (date of request: 02/05/2025). — Text: electronic.
 6. Harensalak B. and D. Ruiter. Non-data processing of the Apache Airflow pipeline / translated from English by D. A. Belikov. Moscow: DMK Press, 2021. pp. 502. ill. ISBN 978-5-97060-970-5 — Text: direct.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

СОЗДАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ БИОХИМИЧЕСКОГО АНАЛИЗА КРОВИ

¹Колпакиди Н.А., Коценко А.А.

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: ¹
randeren@mail.ru

Целью работы является создание экспертной системы поддержки принятия решений для биохимического анализа крови на основе миварных технологий. В исследовании проведен анализ предметной области, включая изучение минимального профиля биохимического анализа крови, который позволяет оценить общее состояние здоровья пациента и определить дальнейшие направления обследования. Разработана миварная база знаний, включающая правила для интерпретации следующих биохимических показателей: глюкоза, общий белок, билирубин, холестерин, ферменты (АлАТ, АсАТ, ГГТ), креатинин, мочевины и электролиты (калий, натрий, хлор). База знаний создана с использованием миварного конструктора экспертных систем, что позволяет быстро обрабатывать данные и выдавать рекомендации по дальнейшему обследованию у профильных специалистов. Экспериментальная проверка системы подтвердила ее работоспособность и корректность интерпретации данных. Система успешно определяет отклонения биохимических показателей от нормы и рекомендует дальнейшие шаги для диагностики и лечения. Проведены тесты на обработку некорректных данных, что показало устойчивость системы к ошибкам ввода. Разработанная система позволяет сократить время на интерпретацию результатов анализов и повысить точность диагностики. В будущем планируется расширение функциональности системы за счет учета индивидуальных особенностей пациентов и интеграции с медицинскими информационными системами. Работа представляет собой важный шаг в направлении автоматизации медицинской диагностики и является полезной для врачей в медицинских учреждениях.

Ключевые слова: Мивар, миварные сети, искусственный интеллект, экспертные системы, базы знаний, биохимический анализ крови.

DEVELOPMENT OF A DECISION SUPPORT SYSTEM FOR BLOOD BIOCHEMICAL ANALYSIS

¹Kolpakidi N.A., Kutsenko A.A.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY),
Moscow, Russia, (105005, Moscow, 2nd Baumanskaya ul, 5 bld. 1), e-mail: ¹ randeren@mail.ru

The purpose of the work is to create an expert decision support system for biochemical blood analysis based on mivar technologies. The study analyzes the subject area, including the study of the minimal profile of biochemical blood analysis, which allows to assess the general health of the patient and determine further directions of examination. A mivar knowledge base was developed including rules for interpreting the following biochemical parameters: glucose, total protein, bilirubin, cholesterol, enzymes (AlAT, AsAT, GGT), creatinine, urea and electrolytes (potassium, sodium, chlorine). The knowledge base was created using the mivar constructor of expert systems, which allows fast data processing and issuing recommendations for further examination by specialized specialists. Experimental testing of the system confirmed its operability and correctness of data interpretation. The system successfully identifies deviations of biochemical parameters from the norm and recommends further steps for diagnosis and treatment. Tests on processing of incorrect data were carried out, which showed the stability of the system to input errors. The developed system allows to reduce the time for interpretation of test

results and increase the accuracy of diagnostics. In the future it is planned to expand the functionality of the system by taking into account individual characteristics of patients and integration with medical information systems. The work represents an important step in the direction of automation of medical diagnostics and is useful for doctors in medical institutions.

Keywords: Mivar, mivar networks, artificial intelligence, expert systems, knowledge bases, blood biochemical analysis.

Введение.

Создание системы поддержки принятия решений (СППР) для биохимического анализа крови актуально из-за большого объема работы, маленького количества времени для оценки биохимического анализа крови и выдачи дальнейшего направления пациенту. Биохимический анализ крови – это лабораторное исследование, которое позволяет оценить работу внутренних органов и систем организма. Существуют разные профили анализа биохимии крови, которые содержат разный набор анализов.

В работе используются миварные технологии, что позволяет получить результат за доли секунд на обычном персональном компьютере или ноутбуке. Цель работы – создать СППР для биохимического анализа крови, которая будет показывать какие параметры повышены, понижены, в норме и давать рекомендации для дальнейшего обследования у конкретного специалиста. В задачи работы входило изучение предметной области биохимии крови, для этого использовался сайт сети клиник Инвитро [1].

Для разработки миварной базы знаний в программе КЭСМИ нужно было изучить основы языка JavaScript. Экспериментальная проверка системы в КЭСМИ включает в себя уже готовую модель и загруженные в нее правила для дальнейшей проверки системы. Основной раздел работы состоит из следующих частей: анализ предметной области, анализ альтернативных подходов решения задачи, разработка миварной базы знаний, экспериментальная проверка системы.

Анализ предметной области.

Биохимический анализ крови включает в себя определение уровня различных веществ в крови, таких как белки, ферменты, гормоны, липиды, углеводы, витамины и минералы. На сайте Инвитро [1] говорится о биохимическом анализе крови, конкретных анализах, и за что они отвечают. В проекте используется минимальный профиль анализа биохимии крови.

Минимальный биохимический профиль помогает провести первичную оценку общего состояния здоровья, а также определить ход дальнейшего обследования. Комплексное исследование включает биохимические показатели белкового, липидного (жирового), углеводного обменов, водно-электролитного баланса, применяемые для оценки риска развития сахарного диабета, сердечно-сосудистой патологии, в том числе атеросклероза, а также выявления заболеваний почек, желудочно-кишечного тракта.

Однако для правильной интерпретации результатов анализа необходимо учитывать множество факторов, что делает этот процесс трудоемким и зависимым от опыта врача. В статье [2] "О создании прототипа миварной сети знаний для системы диагностики сахарного диабета" Варламова О.О. и Чувикова Д.А. подробно описан процесс разработки миварной системы, предназначенной для автоматической диагностики диабета, которая может значительно сократить время на интерпретацию данных и повысить точность диагностики.

Низкая скорость приема пациентов обусловлена ручным анализом больших объемов данных биохимического анализа крови. Терапевту приходится тратить значительное время на

интерпретацию результатов, что приводит к задержкам в постановке диагноза и назначении лечения, что может негативно сказаться на качестве медицинской помощи.

Применение экспертных систем в медицине, особенно таких, которые используют искусственный интеллект и миварные технологии, позволяет улучшить качество диагностики и повысить уверенность врачей в своих решениях. В этом контексте аналогичный подход применялся в статье [3] "МЭС оценки содержимого пакетных данных в локальной сети" Старых Ф.А., Лупанчука В.Ю. и Семкина А.П., где рассматривается использование миварных систем для обработки данных в области кибербезопасности. Эта аналогия подчеркивает важность таких технологий в других отраслях, где данные должны быть быстро и точно обработаны, что также имеет непосредственное отношение к медицинским системам обработки данных.

Распишем функции каждого из параметров минимального биохимического профиля:

1. Глюкоза – основной источник энергии для метаболических процессов в организме человека, является обязательным компонентом большинства внутриклеточных структур, участвует в синтезе нуклеиновых кислот (рибоза, дезоксирибоза), образует соединения с белками (гликопротеиды, протеогликаны) и липидами (гликолипиды).

2. Общий белок – выступает показателем белкового обмена, отражающим содержание всех фракций белков в сыворотке крови. Тест используется в комплексных биохимических обследованиях пациентов при различных заболеваниях.

3. Билирубин общий – определение уровня билирубина в сыворотке крови используют для выявления поражений печени различного происхождения, закупорки желчных путей, гемолитической анемии, желтухи новорожденных.

4. Билирубин прямой – определение концентрации конъюгированного (прямого) билирубина в сыворотке крови используют в дифференциальной диагностике заболеваний, сопровождающихся желтухой (повышением уровня билирубина).

5. Холестерин общий – оценку уровня холестерина в сыворотке крови используют для оценки сердечно-сосудистых рисков, в диагностике нарушений обмена липидов, а также в комплексных обследованиях пациентов с патологией почек, печени, эндокринной системы.

6. АлАТ (Аланинаминотрансфераза) – определение уровня АЛТ в сыворотке крови применяют преимущественно в диагностике и контроле течения болезней печени, а также в комплексных биохимических исследованиях

7. АсАТ (Аспартатаминотрансфераза) – определение уровня АСТ в сыворотке крови используют преимущественно в диагностике и контроле течения болезней печени, а также в комплексных биохимических исследованиях.

8. Гамма-глутамилтранспептидаза (ГГТ) – определение уровня ГГТ в сыворотке крови используют преимущественно для выявления возможной патологии печени и желчевыводящих путей.

9. Фосфатаза щелочная – оценку уровня щелочной фосфатазы в сыворотке крови применяют в целях скрининга и контроля лечения патологии печени или костной ткани.

10. Креатинин – продукт метаболизма мышечных клеток, удаляется из крови почками. Тест используют в качестве маркера функции почек для диагностики и мониторинга острых и хронических болезней почек, а также в скрининговых обследованиях.

11. Мочевина – конечный продукт расщепления белковых молекул, выводимый из организма почками. Определение уровня мочевины в сыворотке крови используют для оценки

выделительной функции почек и контроля эффективности лечения пациентов с почечными заболеваниями.

12. Калий, натрий, хлор в сыворотке крови – определение уровня калия, натрия и хлора в сыворотке крови используется для скрининга электролитов и исследования кислотно-щелочного дисбаланса.

В данном проекте значения и диапазоны элементов берутся из сети клиник Инвитро [1], они могут отличаться от других, в зависимости от того, какой системой и какими приборами для исследований пользуется клиника.

Разработка миварной базы знаний.

Одним из важнейших этапов в создании системы поддержки принятия решений является разработка базы знаний. В медицинской практике база знаний должна включать не только информацию о нормах и отклонениях для различных биохимических показателей, но и учитывать индивидуальные особенности пациента, такие как его возраст, пол, история заболеваний и другие важные данные.

Система будет использовать миварные технологии, которые обеспечат точность и актуальность этих данных. Статья [4] "Создание миварной базы знаний по подбору рекомендаций на маркетплейсе для предприятий машиностроения" посвящена исследованию использования баз знаний миварных экспертных систем для подбора рекомендаций на маркетплейсах, ориентированных на предприятия машиностроения и частных лиц.

В статье [5] "МЭС для подбора спортивного тренажера " Абрамова В.Г. и его коллег рассматриваются методы использования миварных систем в других отраслях, таких как спорт, для подбора тренажеров, что аналогично тому, как миварные системы могут быть использованы в медицине для подбора наилучших рекомендаций на основе данных биохимического анализа.

Миварные системы, основанные на логических алгоритмах, могут создавать сложные цепочки решений, что значительно повышает эффективность диагностики. Статья [6] "МЭС для определения профильного специалиста по собранному анамнезу" предлагает инновационный подход к решению проблемы задержек в оказании медицинской помощи пациентам с сердечно-сосудистыми заболеваниями. Использование экспертной системы на основе миварных технологий позволяет эффективно распределять пациентов между специалистами, сокращая время ожидания и улучшая качество диагностики. Такой подход не только ускоряет процесс лечения, но и помогает избежать ненужных визитов к кардиологу, что особенно важно в условиях высокой нагрузки на медицинские учреждения.

Статья [7] "МЭС для подбора оправы для очков". посвящена разработке миварной экспертной системы (МЭС) для подбора оправы для очков на основе внешних признаков пользователя. Система использует набор параметров оправы, которые подбираются в зависимости от характеристик лица человека, таких как черты лица, тон кожи, цвет волос, форма бровей, наличие или отсутствие бороды и других факторов. Для создания и тестирования системы был использован программный продукт КЭСМИ Wi!Mi Разуматор, который позволяет учитывать индивидуальные особенности пользователя и предлагать наиболее подходящие варианты оправ.

Исследование демонстрирует применение миварной экспертной системы для решения задачи индивидуального подбора оправы для очков. Использование Разуматора позволяет

учитывать уникальные внешние признаки каждого человека, что делает систему эффективным инструментом для рекомендаций. Такой подход не только упрощает процесс выбора оправы, но и повышает удовлетворенность пользователей, предлагая им персонализированные решения, соответствующие их внешности и стилю.

Статья [8] "МЭС для подбора гаммы цветов веб-сайта" демонстрирует применение миварной экспертной системы для автоматизации выбора цветовой гаммы веб-сайтов. Использование КЭСМИ позволяет создать интеллектуальную систему, которая учитывает предпочтения пользователя и специфику проекта, что делает ее полезным инструментом для веб-дизайнеров и разработчиков. Такой подход не только упрощает процесс подбора цветов, но и повышает качество визуального оформления веб-сайтов, делая их более привлекательными для целевой аудитории.

В статье [9] "О проекте создания миварной экспертной системы 'Метаболический синдром. Анализ и предварительный диагноз'" рассматривается процесс создания миварной базы знаний, которая будет использоваться для диагностики метаболического синдрома. Это пример того, как база знаний в миварных системах может быть эффективно использована для диагностики сложных заболеваний на основе биохимического анализа.

Для самой разработки базы знаний потребуется программное обеспечение КЭСМИ (Конструктор Экспертных Систем Миварный) – это конструктор, позволяющий создавать содержащие большое количество правил и параметров экспертные системы в разных предметных областях. Благодаря миварному подходу можно находить алгоритмы и решения задач за доли секунд, пользуясь компьютером или ноутбуком. Простые правила в программе можно настраивать через логику ЕСЛИ-ТО, а для более сложных правил пишутся скрипты на языке программирования JavaScript.

Модель КЭСМИ сохраняется в формате XML, что нужно для хранения и передачи базы знаний. В модели введена ограниченная группа возраста от 18 до 50 лет, так как иначе требуется детальнее учитывать возрастные особенности. В систему вводятся параметры, они проходят через правила и отношения, показывая, где выше, ниже или в норме, далее показывается рекомендация к кому следует обратиться и пройти дальнейшее обследование.

Отношение на языке программирования JavaScript для анализа уровня АЛТ (аланинаминотрансферазы) позволяет продемонстрировать работу миварной системы (рис. 1). Миварная экспертная система анализирует, что если уровень фермента превышает норму, то требуется порекомендовать направление к специалисту. Этот принцип можно адаптировать для множества других показателей, например, для анализа уровня глюкозы, холестерина и других важных биохимических маркеров.

```
// Отношение Норма_АланинАТ
var gender, age, alanine_aminotransferase, alanine_aminotransferase_n
if (gender == "М") {
    if (age >= 18 && age <= 50) {
        if (alanine_aminotransferase > 41) {
            alanine_aminotransferase_n = "выше нормы"
        }
        else {
            alanine_aminotransferase_n = "в норме"
        }
    }
    else {
        alanine_aminotransferase_n = "ошибка (возраст)"
    }
}
else if (gender == "Ж") {
    if (age >= 18 && age <= 50) {
        if (alanine_aminotransferase > 31) {
            alanine_aminotransferase_n = "выше нормы"
        }
        else {
            alanine_aminotransferase_n = "в норме"
        }
    }
    else {
        alanine_aminotransferase_n = "ошибка (возраст)"
    }
}
else {
    alanine_aminotransferase_n = "ошибка (пол)"
}
```

Рисунок 1 – Пример отношения Норма_АланинА

Особенность предлагаемой системы заключается в том, что она не только помогает интерпретировать биохимические показатели, но и рекомендует направление пациента к профильному специалисту. Например, если у пациента повышены уровни глюкозы и калия, система может рекомендовать консультацию эндокринолога. Это значительно улучшит точность диагностики и ускорит процесс назначения лечения.

Использование таких решений уже доказало свою эффективность в других областях. В статье [5] "МЭС для подбора спортивного тренажера" Абрамова В.Г. рассматриваются примеры, когда системы помогают пользователю выбрать подходящий тренажер на основе данных о состоянии его здоровья. Аналогичный подход может быть использован в медицине для выбора подходящих специалистов и назначения дальнейших исследований.

На Рисунке 2 изображены параметры минимального профиля биохимического анализа крови и специалисты, которые отвечают за определенную связку анализов.

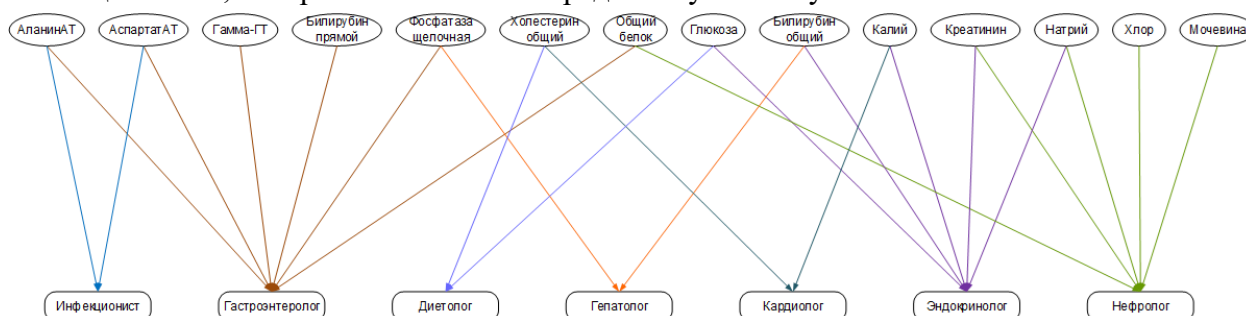


Рисунок 2 – Соответствие биохимических показателей и специалистов

Экспериментальная проверка системы.

После того как база знаний разработана, необходимо провести серию экспериментальных проверок системы. Это поможет убедиться, что система правильно интерпретирует результаты анализов и дает точные рекомендации. Экспериментальная проверка является неотъемлемой частью процесса разработки, так как она помогает выявить возможные ошибки или недочеты в алгоритмах и базе знаний, а также улучшить систему в целом.

Экспериментальная проверка в реальных условиях позволит также протестировать функциональность системы, интеграцию с медицинскими базами данных и взаимодействие с врачами. Система будет проходить несколько этапов тестирования, чтобы гарантировать корректную работу всех алгоритмов и их совместимость с различными медицинскими информационными системами.

В первом эксперименте (Рисунок 3) параметры АлАТ и АсАТ оказались выше нормы. Система рекомендует дальше обследоваться у Гастроэнтеролога и Инфекциониста. Во втором эксперименте (Рисунок 4) параметры АсАТ и Гамма-ГТ оказались выше нормы. Система также рекомендует пройти обследование у Гастроэнтеролога и Инфекциониста. Также проведена обработка неправильного ввода в КЭСМИ для проверки вывода ошибки в значении и причины. На Рисунке 5 неправильно указан возраст, так как в систему вводятся только значения от 18 до 50 лет. На Рисунке 6 неправильно указан пол, так как учитываются только сокращения «м» и «ж».

Объект	Значение	Найти
Биохимия крови		
0. Параметры пациента		
Возраст (18-50)	18	<input type="checkbox"/>
Пол (м/ж)	М	<input type="checkbox"/>
1. Результаты анализа		
2. Соответствие норме		
Норма_АланинАТ	выше нормы	<input checked="" type="checkbox"/>
Норма_АспартатАТ	выше нормы	<input checked="" type="checkbox"/>
Норма_Билирубин_общий	в норме	<input checked="" type="checkbox"/>
Норма_Билирубин_прямой	в норме	<input checked="" type="checkbox"/>
Норма_Гамма-ГТ	в норме	<input checked="" type="checkbox"/>
Норма_Глюкоза	в норме	<input checked="" type="checkbox"/>
Норма_Калий	в норме	<input checked="" type="checkbox"/>
Норма_Креатинин	в норме	<input checked="" type="checkbox"/>
Норма_Мочевина	в норме	<input checked="" type="checkbox"/>
Норма_Натрий	в норме	<input checked="" type="checkbox"/>
Норма_Общий белок	в норме	<input checked="" type="checkbox"/>
Норма_Фосфатаза-Щ	в норме	<input checked="" type="checkbox"/>
Норма_Хлор	в норме	<input checked="" type="checkbox"/>
Норма_Холестерин_общий	в норме	<input checked="" type="checkbox"/>
3. Дальнейшие обследования		
Гастроэнтеролог	требуется обследование	<input checked="" type="checkbox"/>
Гепатолог	все в порядке	<input checked="" type="checkbox"/>
Диетолог	все в порядке	<input checked="" type="checkbox"/>
Инфекционист	требуется обследование	<input checked="" type="checkbox"/>
Кардиолог	все в порядке	<input checked="" type="checkbox"/>
Нефролог	все в порядке	<input checked="" type="checkbox"/>
Эндокринолог	все в порядке	<input checked="" type="checkbox"/>

Рисунок 3 – Первый эксперимент

Тест: Биохимия крови

Объект	Значение	Найти
Биохимия крови		
0. Параметры пациента		
Возраст (18-50)	45	<input type="checkbox"/>
Пол (м/ж)	Ж	<input type="checkbox"/>
1. Результаты анализа		
2. Соответствие норме		
Норма_АланинАТ	в норме	<input checked="" type="checkbox"/>
Норма_АспартатАТ	выше нормы	<input checked="" type="checkbox"/>
Норма_Билирубин_общий	в норме	<input checked="" type="checkbox"/>
Норма_Билирубин_прямой	в норме	<input checked="" type="checkbox"/>
Норма_Гамма-ГТ	выше нормы	<input checked="" type="checkbox"/>
Норма_Глюкоза	в норме	<input checked="" type="checkbox"/>
Норма_Калий	в норме	<input checked="" type="checkbox"/>
Норма_Креатинин	в норме	<input checked="" type="checkbox"/>
Норма_Мочевина	в норме	<input checked="" type="checkbox"/>
Норма_Натрий	в норме	<input checked="" type="checkbox"/>
Норма_Общий белок	в норме	<input checked="" type="checkbox"/>
Норма_Фосфатаза-Щ	в норме	<input checked="" type="checkbox"/>
Норма_Хлор	в норме	<input checked="" type="checkbox"/>
Норма_Холестерин_общий	в норме	<input checked="" type="checkbox"/>
3. Дальнейшие обследования		
Гастроэнтеролог	требуется обследование	<input checked="" type="checkbox"/>
Гепатолог	все в порядке	<input checked="" type="checkbox"/>
Диетолог	все в порядке	<input checked="" type="checkbox"/>
Инфекционист	требуется обследование	<input checked="" type="checkbox"/>
Кардиолог	все в порядке	<input checked="" type="checkbox"/>
Нефролог	все в порядке	<input checked="" type="checkbox"/>
Эндокринолог	все в порядке	<input checked="" type="checkbox"/>

Рисунок 4 – Второй эксперимент

Проект

Наименование	Тип
Биохимия крови	
0. Параметры пациента	
Возраст (18-50)	123
Пол (м/ж)	ABC
1. Результаты анализа	
АланинАТ (31+)	123
АспартатАТ (37-)	123
Билирубин_общий (3.4-20.5)	123
Билирубин_прямой (8.6+)	123
Гамма-ГТ (32-49)	123
Глюкоза (3.8-5.9)	123
Калий (3.5-5.1)	123
Креатинин (43-104)	123
Мочевина (2.1-7.1)	123
Натрий (136-145)	123
Общий_белок (64-83)	123
Фосфатаза-Щ (40-150)	123
Хлор (101-110)	123
Холестерин_общий (2.93-7.15)	123
2. Соответствие норме	
Норма_АланинАТ	ABC
Норма_АспартатАТ	ABC
Норма_Билирубин_общий	ABC
Норма_Билирубин_прямой	ABC
Норма_Гамма-ГТ	ABC
Норма_Глюкоза	ABC
Норма_Калий	ABC
Норма_Креатинин	ABC
Норма_Мочевина	ABC
Норма_Натрий	ABC
Норма_Общий белок	ABC
Норма_Фосфатаза-Щ	ABC
Норма_Хлор	ABC
Норма_Холестерин_общий	ABC
3. Дальнейшие обследования	

Тест: Биохимия крови

Объект	Значение	Найти
Биохимия крови		
0. Параметры пациента		
Возраст (18-50)	17	<input type="checkbox"/>
Пол (м/ж)	Ж	<input type="checkbox"/>
1. Результаты анализа		
2. Соответствие норме		
Норма_АланинАТ	ошибка (возраст)	<input type="checkbox"/>
Норма_АспартатАТ	ошибка (возраст)	<input type="checkbox"/>
Норма_Билирубин_общий	ошибка (возраст)	<input type="checkbox"/>
Норма_Билирубин_прямой	ошибка (возраст)	<input type="checkbox"/>
Норма_Гамма-ГТ	ошибка (возраст)	<input type="checkbox"/>
Норма_Глюкоза	ошибка (возраст)	<input type="checkbox"/>
Норма_Калий	ошибка (возраст)	<input type="checkbox"/>
Норма_Креатинин	ошибка (возраст)	<input type="checkbox"/>
Норма_Мочевина	ошибка (возраст)	<input type="checkbox"/>
Норма_Натрий	ошибка (возраст)	<input type="checkbox"/>
Норма_Общий белок	ошибка (возраст)	<input type="checkbox"/>
Норма_Фосфатаза-Щ	ошибка (возраст)	<input type="checkbox"/>
Норма_Хлор	ошибка (возраст)	<input type="checkbox"/>
Норма_Холестерин_общий	ошибка (возраст)	<input type="checkbox"/>
3. Дальнейшие обследования		
Гастроэнтеролог	ошибка	<input checked="" type="checkbox"/>
Гепатолог	ошибка	<input checked="" type="checkbox"/>
Диетолог	ошибка	<input checked="" type="checkbox"/>
Инфекционист	ошибка	<input checked="" type="checkbox"/>
Кардиолог	ошибка	<input checked="" type="checkbox"/>
Нефролог	ошибка	<input checked="" type="checkbox"/>
Эндокринолог	ошибка	<input checked="" type="checkbox"/>

Рисунок 5 – Демонстрация ошибки возраста

Наименование	Тип
Биохимия крови	
0. Параметры пациента	
Возраст (18-50)	123
Пол (м/ж)	авс
1. Результаты анализа	
АланинАТ (31+)	123
АспартатАТ (37-)	123
Билирубин_общий (3.4-20.5)	123
Билирубин_прямой (8.6+)	123
Гамма-ГТ (32-49)	123
Глюкоза (3.8-5.9)	123
Калий (3.5-5.1)	123
Креатинин (43-104)	123
Мочевина (2.1-7.1)	123
Натрий (136-145)	123
Общий_белок (64-83)	123
Фосфатаза-Щ (40-150)	123
Хлор (101-110)	123
Холестерин_общий (2.93-7.15)	123
2. Соответствие норме	
Норма_АланинАТ	авс
Норма_АспартатАТ	авс
Норма_Билирубин_общий	авс
Норма_Билирубин_прямой	авс
Норма_Гамма-ГТ	авс
Норма_Глюкоза	авс
Норма_Калий	авс
Норма_Креатинин	авс
Норма_Мочевина	авс
Норма_Натрий	авс
Норма_Общий_белок	авс
Норма_Фосфатаза-Щ	авс
Норма_Хлор	авс
Норма_Холестерин_общий	авс
3. Дальнейшие обследования	

Объект	Значение	Найти
Биохимия крови		
0. Параметры пациента		
Возраст (18-50)	25	<input type="checkbox"/>
Пол (м/ж)	муж	<input type="checkbox"/>
1. Результаты анализа		
2. Соответствие норме		
Норма_АланинАТ	ошибка (пол)	<input type="checkbox"/>
Норма_АспартатАТ	ошибка (пол)	<input type="checkbox"/>
Норма_Билирубин_общий	ошибка (пол)	<input type="checkbox"/>
Норма_Билирубин_прямой	ошибка (пол)	<input type="checkbox"/>
Норма_Гамма-ГТ	ошибка (пол)	<input type="checkbox"/>
Норма_Глюкоза	ошибка (пол)	<input type="checkbox"/>
Норма_Калий	ошибка (пол)	<input type="checkbox"/>
Норма_Креатинин	ошибка (пол)	<input type="checkbox"/>
Норма_Мочевина	ошибка (пол)	<input type="checkbox"/>
Норма_Натрий	ошибка (пол)	<input type="checkbox"/>
Норма_Общий_белок	ошибка (пол)	<input type="checkbox"/>
Норма_Фосфатаза-Щ	ошибка (пол)	<input type="checkbox"/>
Норма_Хлор	ошибка (пол)	<input type="checkbox"/>
Норма_Холестерин_общий	ошибка (пол)	<input type="checkbox"/>
3. Дальнейшие обследования		
Гастроэнтеролог	ошибка	<input checked="" type="checkbox"/>
Гепатолог	ошибка	<input checked="" type="checkbox"/>
Диетолог	ошибка	<input checked="" type="checkbox"/>
Инфекционист	ошибка	<input checked="" type="checkbox"/>
Кардиолог	ошибка	<input checked="" type="checkbox"/>
Нефролог	ошибка	<input checked="" type="checkbox"/>
Эндокринолог	ошибка	<input checked="" type="checkbox"/>

Рисунок 6 – Демонстрация ошибки пола

Заключение.

В ходе работы проведен анализ биохимических показателей крови, выбран минимальный профиль, состоящий из 15 параметров, каждый из которых отвечает за конкретного специалиста. Разработана система поддержки принятия решений для биохимического анализа крови, которая позволяет сократить время, затрачиваемое на рутинные задачи, и повысить качество оказываемой медицинской помощи.

Создана база знаний, включающая код для каждого параметра анализа, проверку на соответствие норме, повышение или понижение показателей, а также рекомендации по дальнейшему обследованию. Проведена экспериментальная проверка системы, включая тестирование на некорректные данные, что подтвердило ее устойчивость к ошибкам ввода. Система корректно определяет, находятся ли показатели биохимического анализа крови в норме, повышены или понижены, и рекомендует дальнейшие обследования у профильных специалистов.

В будущем проект может быть расширен за счет учета индивидуальных особенностей пациентов, таких как возраст, пол, история заболеваний и другие факторы. Также планируется адаптация системы к различным медицинским учреждениям, что позволит предоставлять персонализированные рекомендации в зависимости от региона и специфики клиники. Разработанная система представляет собой важный шаг в направлении автоматизации медицинской диагностики и имеет потенциал для дальнейшего развития, что может значительно улучшить качество и скорость оказания медицинской помощи.

Список литературы

1. Биохимия крови: минимальный профиль // Инвитро URL: <https://www.invitro.ru/analizes/profi/908/6761/> (дата обращения: 26.02.2025).
2. Ким Х., Варламов О.О., Чувилов Д.А. и др. О создании прототипа миварной сети знаний для системы диагностики сахарного диабета // Информация и образование: границы коммуникаций. 2020. № 12(20). С. 173-178. EDN JNUJVB.
3. Старых Ф.А., Лупанчук В.Ю., Семкин А.П. МЭС оценки содержимого пакетных данных в локальной сети // МИВАР'24: Сборник научных статей, Москва, 18–20 апреля 2024 года. Москва: ИНФРА-М, 2024. С. 102-106. EDN FKVQMO.
4. Глазетская Л.И., Цепов И.А., Медведенко М.В. и др. Создание миварной базы знаний по подбору рекомендаций на маркетплейсе для предприятий машиностроения // Современные тенденции развития ИСиМК: Сборник трудов Всероссийской научно-технической конференции, Ростов-на-Дону, 25 января 2024 года. Ростов-на-Дону: ДГТУ, 2024. С. 171-177. EDN BQTUDK.
5. Абрамов В.Г., Еремехин В.С., Некрасов С.А. и др. МЭС подбора спортивного тренажера // МИВАР'24: Сборник научных статей, Москва, 18–20 апреля 2024 года. Москва: ИНФРА-М, 2024. С. 16-22. EDN EOYVGV.
6. Перфильева К.А., Алферов В.В., Воропаев Н.М. и др. МЭС для определения профильного специалиста по собранному анамнезу // Мивар'23: Сборник студенческих статей. Москва: ООО «Научно-издательский центр ИНФРА-М», 2023. С. 155-162. EDN QREGWK.
7. Ишков Д.О., Фадеев А.А., Курганова А.Г. и др. МЭС для подбора оправы для очков // Мивар'22: Сборник научных статей. Москва: Издательский Дом "Инфра-М", 2022. С. 38-44. EDN CXWYVK.
8. Ким А.М., Бибилов П.А., Поддубный М.Н. и др. МЭС для подбора гаммы цветов веб-сайта // МИВАР'24: Сборник научных статей, Москва, 18–20 апреля 2024 года. Москва: ИНФРА-М, 2024. С. 62-66. EDN FMWNDG.
9. Адамова Л.Е., Варламов О.О., Чувилов Д.А. О проекте создания миварной экспертной системы "Метаболический синдром. Анализ и предварительный диагноз" для эндокринолога // ИТиПММ: материалы II Всероссийской научной конференции, Дивноморское, 30 сентября – 03 октября 2019 года / Министерство науки и высшего образования РФ, ДГТУ. Дивноморское: ДГТУ, 2019. С. 46-47. EDN DHLEIR.

References

1. Blood Biochemistry: a minimal profile // Invitro URL: <https://www.invitro.ru/analizes/profi/908/6761/> (date of reference: 02/26/2025).
2. Kim H., Varlamov O.O., Chuvikov D.A. and others. On creating a prototype of a mivar knowledge network for a diabetes diagnosis system // Information and education: boundaries of communication. 2020. No. 12(20). pp. 173-178. EDN JNUJVB.
3. Starykh F.A., Lupanchuk V.Yu., Semkin A.P. MES assessment of packet data content in a local network // MIVAR'24: Collection of scientific articles, Moscow, April 18-20, 2024. Moscow: INFRA-M, 2024. pp. 102-106. EDN FKVQMO.
4. Glazetskaya L.I., Tsepov I.A., Medvedenko M.V. and others. Creation of a comprehensive knowledge base for the selection of recommendations on the marketplace for engineering

- enterprises //Current trends in the development of ISiMK: Proceedings of the All-Russian Scientific and Technical Conference, Rostov-on-Don, January 25, 2024. Rostov-on-Don: DSTU, 2024. pp. 171-177. EDN BQTUDK.
5. Abramov V.G., Eremikhin V.S., Nekrasov S.A. and others. MES selection of a sports simulator // MIVAR'24: Collection of scientific articles, Moscow, April 18-20, 2024. Moscow: INFRA-M, 2024. pp. 16-22. EDN EOYVGU.
 6. Perfilieva K.A., Alferov V.V., Voropaev N.M. and others. MES for determining the profile specialist based on the collected medical history // Mivar'23: Collection of student articles. Moscow: INFRA-M Scientific Publishing Center, LLC, 2023. pp. 155-162. EDN QREGWK.
 7. Ishkov D.O., Fadeev A.A., Kurganova A.G. and others. MES for the selection of eyeglass frames // Mivar'22: Collection of scientific articles. Moscow: Infra-M Publishing House, 2022. pp. 38-44. EDN CXWYVK.
 8. Kim A.M., Bibikov P.A., Poddubny M.N. and others. MES for selecting a range of website colors // MIVAR'24: Collection of scientific articles, Moscow, April 18-20, 2024. Moscow: INFRA-M, 2024. pp. 62-66. EDN FMWNDG.
 9. Adamova L.E., Varlamov O.O., Chuvikov D.A. On the project of creating the mivar expert system "Metabolic syndrome. Analysis and preliminary diagnosis" for an endocrinologist // ITiPMM: proceedings of the II All–Russian Scientific Conference, Divnomorskoye, September 30 - October 03, 2019 / Ministry of Science and Higher Education of the Russian Federation, DSTU. Divnomorskoye: DSTU, 2019. pp. 46-47. EDN DHLEIR.
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.942

МОДЕЛЬ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ «ТОЧНО-В-СРОК» С МНОГОЭТАПНЫМ ОБСЛУЖИВАНИЕМ

Подгорнов М.Д.

*ФГБОУ ВО "УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Ульяновск, Россия,
(432017, Ульяновская область, город Ульяновск, ул. Льва Толстого, д. 42), e-mail:
maksimka_7373@mail.ru*

В работе развивается семимартингалный (траекторный) подход к математическому описанию и моделированию систем массового обслуживания (СМО) «точно-в-срок». Рассмотрена модель СМО «точно-в-срок» с многоэтапным обслуживанием заявок. Построена математическая модель. Показан переход от математической модели к итерационным формулам, по которым проводится имитационное моделирование.

Ключевые слова: Система массового обслуживания, семимартингалное описание, точно-в-срок, многоэтапное обслуживание, точечный процесс, компенсатор, имитационное моделирование.

THE JUST-IN-TIME QUEUING SYSTEM MODEL WITH PHASED SERVICE

Podgornov M.D.

*ULYANOVSK STATE UNIVERSITY, Ulyanovsk, Russia, (432017, Ulyanovsk region, Ulyanovsk city,
Lva Tolstoy str., 42), e-mail: maksimka_7373@mail.ru*

The paper develops a semi-martingale (trajectory) approach to the mathematical description and modeling of just-in-time queuing systems. The queuing system models with phased service is considered. A mathematical model is constructed. The transition from a mathematical model to iterative formulas, which are used for simulation, is shown.

Keywords: Queuing System, system, semi-martingale description, just-in-time, phased service, point process, compensator, simulation modeling.

Введение

Современные условия ведения бизнеса требуют от компаний высокой эффективности и гибкости в организации процессов обслуживания клиентов. Одной из наиболее актуальных концепций в этой области является модель системы массового обслуживания (СМО) «точно-в-срок», также известная как ЛТ (just-in-time), которая акцентирует внимание на своевременном предоставлении услуг и минимизации временных затрат в процессе обслуживания (см., к примеру, работы [1-2]).

Многоэтапное обслуживание представляет собой стратегию, при которой процессы делятся на несколько последовательных этапов, что позволяет более эффективно управлять потоками клиентов и ресурсами предприятия.

На сегодняшний день математические и, в частности, стохастические модели систем массового обслуживания точно-в-срок развиты крайне слабо. Этот факт придает описанию и моделированию подобных систем особую значимость, поскольку область их применения

крайне широка. Целью работы является разработка стохастического описания СМО «точно-в-срок» с многоэтапным обслуживанием, подходящего как для аналитических методов, так и для компьютерного моделирования.

Для математического описания СМО использован аппарат точечных (считающих) процессов и их компенсаторов. С данным траекторным подходом при описании СМО можно ознакомиться, например, по работам [3-5].

Постановка задачи

Рассмотрим одноканальную СМО, в которую поступают заявки одного типа. Интенсивность поступления заявок определяется параметром $\lambda > 0$. С момента начала обслуживания заявки, оператор должен завершить ее обработку за определенный отрезок времени, определяемый параметром $\tau_1 > 0$, или, говоря иначе, точно-в-срок. После завершения обслуживания у первого оператора заявка отправляется ко второму оператору, который также должен обслужить её за определённое время, определяемое параметром $\tau_2 > 0$. Для заявок, которые поступают на обслуживание в момент времени, когда операторы заняты организованы бесконечные очереди (Рисунок 1).

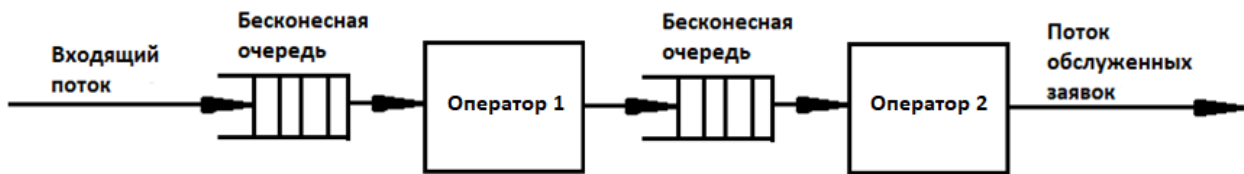


Рисунок 1 - Схема СМО

Математическая модель

Для описания работы системы введем считающие процессы A^1, A^2, D , где $A^1 = (A_t^1)_{t \geq 0}$ – число заявок, поступивших в СМО за время $t \geq 0$, $A_0^1 = 0$, $A^2 = (A_t^2)_{t \geq 0}$ – число заявок, обслуженных первым оператором и поступивших на обслуживание ко второму за время $t \geq 0$, $A_0^2 = 0$, $D = (D_t)_{t \geq 0}$ – число полностью обслуженных заявок в СМО за время $t \geq 0$, $D_0 = 0$. Точечные процессы A^1, A^2 и D определяются своими компенсаторами $\widetilde{A}^1 = (\widetilde{A}_t^1)_{t \geq 0}$, $\widetilde{A}^2 = (\widetilde{A}_t^2)_{t \geq 0}$ и $\widetilde{D} = (\widetilde{D}_t)_{t \geq 0}$ [4]:

$$A_t^1 = \widetilde{A}_t^1 + m_t^{A^1}, \quad (1)$$

$$A_t^2 = \widetilde{A}_t^2 + m_t^{A^2}, \quad (2)$$

$$D_t = \widetilde{D}_t + m_t^D, \quad (3)$$

где $\widetilde{A}^1, \widetilde{A}^2$ и \widetilde{D} – неубывающие предсказуемые процессы, $m_t^{A^1}$, $m_t^{A^2}$ и m_t^D – мартингалы.

Для системы, рассматриваемой в данной работе, компенсатор процесса $A^1 = (A_t^1)_{t \geq 0}$ будет иметь следующий вид:

$$\widetilde{A}_t^1 = \lambda t, \quad \lambda > 0, \quad (4)$$

где $\lambda > 0$ – интенсивность поступления заявок.

Компенсаторы для процессов $A^2 = (A_t^2)_{t \geq 0}$ и $D = (D_t)_{t \geq 0}$ определяются соотношениями:

$$\widetilde{A}_t^2 = \int_0^t \mu_s^1 ds, \quad (5)$$

$$\widetilde{D}_t = \int_0^t \mu_s^2 ds, \quad (6)$$

где μ_t^1 и μ_t^2 – интенсивности обслуживания первого и второго операторов соответственно. Определять их будем следующими соотношениями:

$$\mu_t^1 = \frac{1}{t_t^{o1} - t} \cdot I(t_t^{o1} > 0), \quad (7)$$

$$\mu_t^2 = \frac{1}{t_t^{o2} - t} \cdot I(t_t^{o2} > 0). \quad (8)$$

Здесь $I(\cdot)$ – индикаторная функция, t_t^{o1} – время, к которому первый оператор стремиться завершить обработку текущей заявки. Аналогично, t_t^{o2} – время, к которому стремиться закончить обработку текущей заявки второй оператор. Отметим, что в любой момент времени $t \geq 0$, $\mu_t^1, \mu_t^2 \geq 0$.

Опишем уравнение изменения t_t^{o1} . Оно будет иметь следующий вид:

$$dt_t^{o1} = (t + \tau_1) \cdot I(A_t^1 - A_t^2 = 0) dA_t^1 + (t + \tau_1 - t_t^{o1}) \cdot I(q_t^1 > 0) dA_t^2 - t_t^{o1} \cdot I(q_t^1 = 0) dA_t^2, \quad (9)$$

где q_t^1 – количество заявок в очереди в момент времени $t \geq 0$, $q_0^1 = 0$. Для параметра q_t^1 можно написать следующее балансовое уравнение:

$$dq_t^1 = I(A_t^1 - A_t^2 > 0) dA_t^1 - I(q_t^1 > 0) dA_t^2, \quad (10)$$

т.е. очередь будет увеличиваться на единицу, если в момент прихода новой заявки ($dA_t^1 = 1$) оператор занят, и уменьшаться на единицу, если в момент окончания обслуживания текущей заявки ($dA_t^2 = 1$) очередь не пуста ($q_t^1 > 0$).

Логика построения уравнения (9) такова. Во-первых, параметр t_t^{o1} принимает значение равное сумме текущего значения времени и параметра τ_1 , если в момент прихода новой заявки ($dA_t^1 = 1$) оператор свободен, либо если в момент окончания обслуживания текущей заявки ($dA_t^2 = 1$) в очереди находятся заявки ($q_t^1 > 0$). Во-вторых, обнуляется, если в момент окончания обслуживания текущей заявки ($dA_t^2 = 1$) очередь пуста ($q_t^1 > 0$).

Балансовые уравнения для t_t^{o2} и q_t^2 будут иметь аналогичную логику построения:

$$dt_t^{o2} = (t + \tau_2) \cdot I(A_t^2 - D_t = 0) dA_t^2 + (t + \tau_2 - t_t^{o2}) \cdot I(q_t^2 > 0) dD_t - t_t^{o2} \cdot I(q_t^2 = 0) dD_t, \quad (11)$$

$$dq_t^2 = I(A_t^2 - D_t > 0) dA_t^2 - I(q_t^2 > 0) dD_t, \quad (12)$$

Итерационные формулы

Выведем формулы, необходимые для имитационного моделирования СМО. На стохастическом базисе $B = (\Omega, \mathcal{F}, F = (\mathcal{F}_t)_{t \geq 0}, P)$ из формул (1)-(12) можно получить следующие инфинитезимальные соотношения:

$$P\{A_{t+\Delta}^1 - A_t^1 = 1 | \mathcal{F}_t\} = \lambda \cdot \Delta + o(\Delta), \quad (13)$$

$$P\{A_{t+\Delta}^2 - A_t^2 = 1 | \mathcal{F}_t\} = \mu_t^1 \cdot \Delta + o(\Delta), \quad (14)$$

$$P\{D_{t+\Delta} - D_t = 1 | \mathcal{F}_t\} = \mu_t^2 \cdot \Delta + o(\Delta). \quad (15)$$

Формулы (13)-(15) позволяют, основываясь на понятии геометрической вероятности, провести имитационное моделирование. А именно, введя дискретизацию (шаг по времени) Δ из условия $\lambda \cdot \Delta \ll 1$, $\mu_t^1 \cdot \Delta \ll 1$, $\mu_t^2 \cdot \Delta \ll 1$ получим следующие итерационные формулы (для

вычисления значений процессов в момент времени $t + \Delta$ через значения процессов в момент t):

$$A_{t+\Delta}^1 = A_t^1 + \delta(\lambda), \quad (16)$$

$$A_{t+\Delta}^2 = A_t^2 + \delta(\mu_t^1), \quad (17)$$

$$D_{t+\Delta} = D_t + \delta(\mu_t^2), \quad (18)$$

где $\delta(\gamma) = \begin{cases} 1, & \text{с вероятностью } \gamma \cdot \Delta, \\ 0, & \text{с вероятностью } 1 - \gamma \cdot \Delta. \end{cases}$

Оставшиеся параметры вычисляем следующим образом:

$$q_{t+\Delta}^1 = q_t^1 + I(A_t^1 - A_t^2 > 0)\Delta A_t^1 - I(q_t^1 > 0)\Delta A_t^2, \quad (19)$$

$$t_{t+\Delta}^{o1} = t_t^{o1} + (t + \tau_1) \cdot I(A_t^1 - A_t^2 = 0)\Delta A_t^1 + (t + \tau_1 - t_t^{o1}) \cdot I(q_t^1 > 0)\Delta A_t^2 - \\ - t_t^{o1} \cdot I(q_t^1 = 0)\Delta A_t^2, \quad (20)$$

$$q_{t+\Delta}^2 = q_t^2 + I(A_t^2 - D_t > 0)\Delta A_t^2 - I(q_t^2 > 0)\Delta D_t, \quad (21)$$

$$t_{t+\Delta}^{o2} = t_t^{o2} + (t + \tau_2) \cdot I(A_t^2 - D_t = 0)\Delta A_t^2 + (t + \tau_2 - t_t^{o2}) \cdot I(q_t^2 > 0)\Delta D_t - \\ - t_t^{o2} \cdot I(q_t^2 = 0)\Delta D_t. \quad (22)$$

Здесь $\Delta A_t^1 = A_{t+\Delta}^1 - A_t^1$, $\Delta A_t^2 = A_{t+\Delta}^2 - A_t^2$, $\Delta D_t = D_{t+\Delta} - D_t$.

Результаты компьютерного моделирования

Практическая реализация СМО осуществлена с помощью языка программирования высокого уровня C# в среде разработки Visual Studio 2022. На Рисунке 2 представлен результат моделирования систем при параметрах $\tau_1 = 2$, $\tau_2 = 1$, $\lambda = 1$ и времени моделирования $T = 10$.

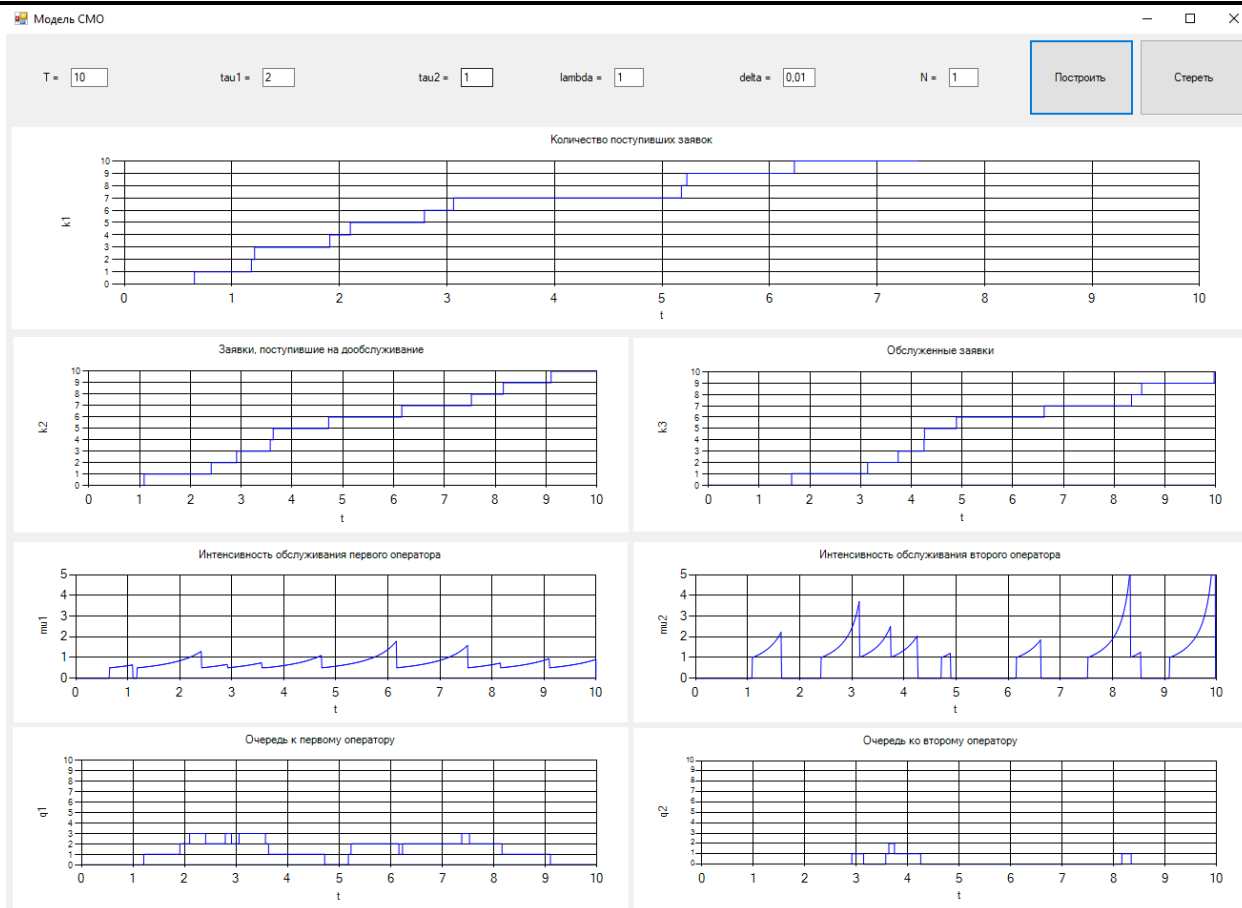


Рисунок 2 - Модель СМО

Результаты моделирования показывают, что система корректно справляется с поставленными задачами, операторы обрабатывают заявки точно в срок.

Заключение

В результате выполнения данной работы была построена математическая модель системы массового обслуживания «точно-в-срок» с многоэтапным обслуживанием в семимартингальных терминах. Показан переход от математической модели к итерационным формулам, по которым было проведено имитационное моделирование.

Список литературы

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Вестник Самарского государственного технического университета. Серия: Физикоматематические науки. 2018, т. 22, №. 3, с. 518-531.
2. Бутов А.А. Оценивание параметров распределенных продуктивных систем, работающих по принципу «точно в срок» // Автомат. и телемех. 2020, № 3, с.14–27.
3. Бородин А.Н. Случайные процессы: Учебник. Спб.: Изд-во «Лань», 2013.
4. Бутов, А.А. Теория случайных процессов и её дополнительные главы: учеб. пособие. Ч. 1. Введение в стохастическое исчисление. Ульяновск : УлГУ, 2016

5. Бутов, А.А. Теория случайных процессов и её дополнительные главы: учеб. пособие. Ч. 2. Случайное блуждание, винеровский процесс, стохастический интеграл, диффузионные процессы. Ульяновск : УлГУ, 2021

References

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Bulletin of the Samara State Technical University. Series: Physical and Mathematical Sciences. 2018, vol. 22, No. 3, pp. 518-531.
 2. Butov A.A. Estimation of parameters of distributed productive systems operating on the principle of "just in time" // Automaton. and telemech. 2020, No. 3, pp.14-27.
 3. Borodin A.N. Random processes: Textbook. St. Petersburg: Publishing house "Lan", 2013.
 4. Butov, A.A. Theory of Random Processes and Its Additional Chapters. allowance. Part 1. Introduction to Stochastic Calculus. Ulyanovsk : Ulyanovsk State University, 2016
 5. Butov, A.A. Theory of Random Processes and Its Additional Chapters. allowance. Part 2. Random walk, Wiener process, stochastic integral, diffusion processes. Ulyanovsk : Ulyanovsk State University, 2021
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.942

МОДЕЛЬ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ «ТОЧНО-В-СРОК» С ОТНОСИТЕЛЬНЫМ ПРИОРИТЕТОМ В ОБСЛУЖИВАНИИ

Подгорнов М.Д.

*ФГБОУ ВО "УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Ульяновск, Россия,
(432017, Ульяновская область, город Ульяновск, ул. Льва Толстого, д. 42), e-mail:
maksimka_7373@mail.ru*

В работе развивается семимартингалный (траекторный) подход к математическому описанию и моделированию систем массового обслуживания (СМО) «точно-в-срок» с приоритетами в обслуживании. Рассмотрена модель одноканальной СМО с относительным приоритетом. Показан переход от математической модели к итерационным формулам, по которым проводится имитационное моделирование.

Ключевые слова: Система массового обслуживания, семимартингалное описание, точно-в-срок, приоритет, точечный процесс, компенсатор, имитационное моделирование.

THE JUST-IN-TIME QUEUING SYSTEM MODEL WITH RELATIVE PRIORITY

Podgornov M.D.

*ULYANOVSK STATE UNIVERSITY, Ulyanovsk, Russia, (432017, Ulyanovsk region, Ulyanovsk city,
Lva Tolstoy str., 42), e-mail: maksimka_7373@mail.ru*

The paper develops a semi-martingale (trajectory) approach to the mathematical description and modeling of just-in-time queuing systems (QS) with service priorities. The model of singlechannel QS with relative priority is considered. The transition from a mathematical model to iterative formulas, which are used for simulation, is shown.

Keywords: Queuing System, semi-martingale description, just-in-time, priority, point process, compensator, simulation modeling.

Введение

В данной работе рассматривается достаточно новая для теории массового обслуживания система «точно-в-срок» с относительным приоритетом в обслуживании.

Алгоритм обслуживания "точно-в-срок" достаточно хорошо известен и применяется во различных областях. Эта модель фокусируется на высоком уровне сервисного обслуживания, минимизации времени ожидания и эффективном распределении ресурсов, что позволяет повышать общую производительность и удовлетворенность клиентов (см., к примеру, работы [1-2]).

Несмотря на широкое применение данной концепции в различных областях, модели систем массового обслуживания «точно-в-срок» находятся на довольно низком уровне развития. Это касается как имитационных, так и математических моделей. Однако, применение таких моделей необходимо при решении задач оптимального управления, так как они позволяют принимать оптимальные решения на основе анализа вероятностных

характеристик системы, учитывая различные факторы неопределенности. Цель исследования заключается в разработке стохастического описания СМО «точно-в-срок» с относительным приоритетом (приоритетная заявка ожидает окончания обслуживания текущей заявки и после этого встает на внеочередное обслуживание), которое было бы подходящим как для аналитических методов, так и для компьютерного моделирования.

Для математического описания СМО использован аппарат точечных (считающих) процессов и их компенсаторов. С данным траекторным подходом при описании СМО можно ознакомиться, например, по работам [3-5]. Для контроля приоритета использован подход, основанный на регулировании размеров очередей.

Постановка задачи

Рассмотрим одноканальную СМО, в которую поступают заявки двух типов: первый тип – часто поступающие, но менее важные заявки, второй тип – более важные, но поступающие реже. Заявки обоих типов поступают независимо друг от друга и образуют простейшие потоки с интенсивностями $\lambda_1 > 0$ и $\lambda_2 > 0$. С момента начала обслуживания заявки, оператор должен завершить ее обработку за определенный отрезок времени, определяемый параметром $\tau_1 > 0$ для заявок первого типа и параметром $\tau_2 > 0$ для заявок второго типа. Так как заявки второго типа являются более важными, они имеют относительный приоритет в обслуживании, то есть встают на обслуживание после обработки текущей заявки не зависимо от количества заявок первого типа в системе. Общая очередь в данном случае, очевидно, не эффективна, поэтому для заявок каждого типа организована отдельная очередь. (Рисунок 1).

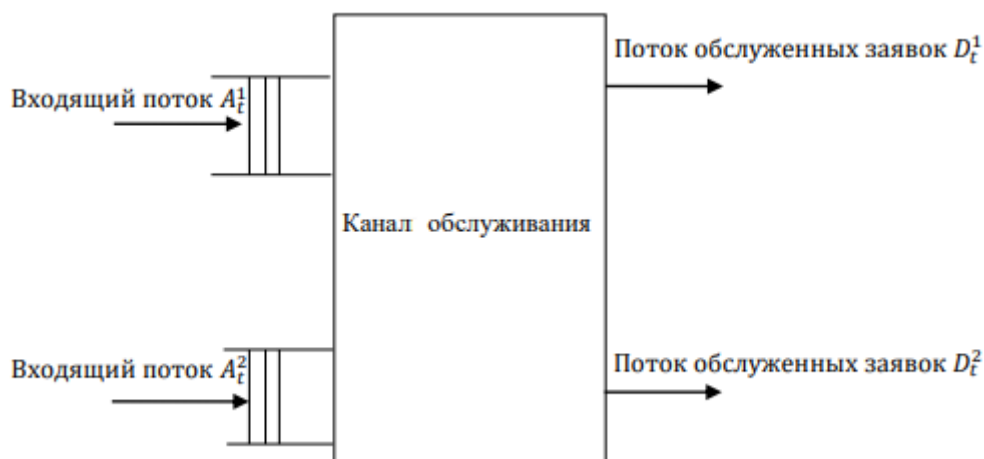


Рисунок 1 - Схема СМО

Математическая модель

Для описания работы систем введем считающие процессы A^1, A^2, D^1, D^2 где $A^1 = (A_t^1)_{t \geq 0}$ – число заявок первого типа, поступивших в СМО за время $t \geq 0$, $A_0^1 = 0$, $A^2 = (A_t^2)_{t \geq 0}$ – число заявок второго типа, поступивших в СМО за время $t \geq 0$, $A_0^2 = 0$, $D^1 = (D_t^1)_{t \geq 0}$ – число обслуженных заявок первого типа за время $t \geq 0$, $D_0^1 = 0$ и $D^2 = (D_t^2)_{t \geq 0}$ – число обслуженных заявок второго типа за время $t \geq 0$, $D_0^2 = 0$. Точечные процессы A^1, A^2, D^1 и D^2 определяются своими компенсаторами $\widetilde{A}^1 = (\widetilde{A}_t^1)_{t \geq 0}$, $\widetilde{A}^2 =$

$(\widetilde{A}_t^2)_{t \geq 0}, \widetilde{D}^1 = (\widetilde{D}_t^1)_{t \geq 0}$ и $\widetilde{D}^2 = (\widetilde{D}_t^2)_{t \geq 0}$ в соответствии с разложением Дуба-Мейера для субмартингалов [4]:

$$A_t^1 = \widetilde{A}_t^1 + m_t^{A^1}, \quad (1)$$

$$A_t^2 = \widetilde{A}_t^2 + m_t^{A^2}, \quad (2)$$

$$D_t^1 = \widetilde{D}_t^1 + m_t^{D^1}, \quad (3)$$

$$D_t^2 = \widetilde{D}_t^2 + m_t^{D^2}, \quad (4)$$

где $\widetilde{A}^1, \widetilde{A}^2, \widetilde{D}^1$ и \widetilde{D}^2 – неубывающие предсказуемые процессы, $m_t^{A^1}, m_t^{A^2}, m_t^{D^1}$ и $m_t^{D^2}$ – мартингалы.

Для рассматриваемой системы, компенсаторы процессов $A^1 = (A_t^1)_{t \geq 0}$ и $A^2 = (A_t^2)_{t \geq 0}$ определяются следующими соотношениями:

$$\widetilde{A}_t^1 = \lambda_1 t, \quad \lambda_1 > 0, \quad (5)$$

$$\widetilde{A}_t^2 = \lambda_2 t, \quad \lambda_2 > 0, \quad (6)$$

где $\lambda_1, \lambda_2 > 0$ – интенсивность поступления заявок первого и второго типов соответственно.

Компенсаторы для процессов $D^1 = (D_t^1)_{t \geq 0}$ и $D^2 = (D_t^2)_{t \geq 0}$ будут иметь вид:

$$\widetilde{D}_t^1 = \int_0^t \mu_s^1 ds, \quad (7)$$

$$\widetilde{D}_t^2 = \int_0^t \mu_s^2 ds, \quad (8)$$

где μ_t^1 и μ_t^2 – интенсивности обслуживания заявок двух типов. Определять их будем следующими соотношениями:

$$\mu_t^1 = \frac{1}{t_t^{o1} - t} \cdot I(t_t^{o1} > 0). \quad (9)$$

$$\mu_t^2 = \frac{1}{t_t^{o2} - t} \cdot I(t_t^{o2} > 0). \quad (10)$$

Здесь $I(\cdot)$ – индикаторная функция, t_t^{o1} – время, к которому оператор стремится завершить обработку заявки первого типа. Аналогично, t_t^{o2} – время, к которому оператор стремится закончить обработку заявки второго типа. Отметим, что в любой момент времени $t \geq 0, \mu_t^1 \geq 0, \mu_t^2 \geq 0$.

Опишем управление относительным приоритетом через регулирование значений параметров t_t^{o1} и t_t^{o2} и размеров очередей. Для заявок первого типа уравнения будут иметь вид:

$$dt_t^{o1} = (t + \tau_1) \cdot I(A_t^1 + A_t^2 - D_t^1 - D_t^2 = 0) dA_t^1 + (t + \tau_1 - t_t^{o1}) \cdot I(q_t^1 > 0, q_t^2 = 0) dD_t^1 + \\ + (t + \tau_1) \cdot I(q_t^1 > 0, q_t^2 = 0) dD_t^2 - t_t^{o1} \cdot I(q_t^1 = 0) dD_t^1 - t_t^{o1} \cdot I(q_t^2 > 0) dD_t^1, \quad (11)$$

где q_t^1 – количество заявок первого типа в очереди в момент времени $t \geq 0, q_0^1 = 0, q_t^2$ – количество заявок второго типа в очереди в момент времени $t \geq 0, q_0^2 = 0$. Для параметра q_t^1 можно написать следующее балансовое уравнение:

$$dq_t^1 = I(A_t^1 + A_t^2 - D_t^1 - D_t^2 > 0) dA_t^1 - I(q_t^1 > 0, q_t^2 = 0) dD_t^1 - I(q_t^1 > 0, q_t^2 = 0) dD_t^2, \quad (12)$$

т.е. очередь будет увеличиваться на единицу, если в момент прихода новой заявки первого типа ($dA_t^1 = 1$) оператор занят, и уменьшаться на единицу, если в момент окончания обслуживания текущей заявки ($dD_t^1 = 1$ или $dD_t^2 = 1$) в очереди нет заявок второго типа ($q_t^2 = 0$), а очередь заявок первого типа не пуста ($q_t^1 > 0$).

Логика построения уравнения (11) такова. Во-первых, параметр t_t^{o1} принимает значение равное сумме текущего значения времени и параметра τ_1 , если в момент прихода новой заявки

первого типа ($dA_t^1 = 1$) оператор свободен, либо если в момент окончания обслуживания текущей заявки ($dD_t^1 = 1$ или $dD_t^2 = 1$) в очереди есть заявки первого типа ($q_t^1 > 0$) и отсутствуют заявки второго типа $q_t^2 = 0$. Во-вторых, обнуляется, если в момент окончания обслуживания заявки первого типа ($dD_t^1 = 1$) либо очередь заявок первого типа пуста ($q_t^1 = 0$), либо в очереди есть заявки второго типа ($q_t^2 > 0$).

Уравнения для заявок второго типа будут таковы:

$$dt_t^{o2} = (t + \tau_2) \cdot I(A_t^1 + A_t^2 - D_t^1 - D_t^2 = 0) dA_t^2 + (t + \tau_2) \cdot I(q_t^2 > 0) dD_t^1 + (t + \tau_2 - t_t^{o2}) \cdot I(q_t^2 > 0) dD_t^2 - t_t^{o2} \cdot I(q_t^2 = 0) dD_t^2 \quad (13)$$

Балансовое уравнение для параметра q_t^2 будет следующим:

$$dq_t^2 = I(A_t^1 + A_t^2 - D_t^1 - D_t^2 > 0) dA_t^2 - I(q_t^2 > 0) dD_t^1 - I(q_t^2 > 0) dD_t^2, \quad (14)$$

т.е. очередь будет увеличиваться на единицу, если в момент прихода новой заявки второго типа ($dA_t^2 = 1$) оператор занят, и уменьшаться на единицу, если в момент окончания обслуживания текущей заявки ($dD_t^1 = 1$ или $dD_t^2 = 1$) очередь заявок второго типа не пуста ($q_t^2 > 0$).

Логика построения уравнения (13) следующая. Во-первых, параметр t_t^{o2} принимает значение равное сумме текущего значения времени и параметра τ_2 , если в момент прихода новой заявки второго типа ($dA_t^2 = 1$) оператор свободен, либо если в момент окончания обслуживания текущей заявки ($dD_t^1 = 1$ или $dD_t^2 = 1$) в очереди есть заявки второго типа ($q_t^2 > 0$). Во-вторых, обнуляется, если в момент окончания обслуживания заявки второго типа ($dD_t^2 = 1$) очередь заявок второго типа пуста ($q_t^2 = 0$).

Отметим, что уравнения построены так, что в любой момент времени $t \geq 0$ между параметрами t_t^{o1} и t_t^{o2} соблюдаются следующие соотношения. Во-первых, если $t_t^{o1} > 0$, то $t_t^{o2} = 0$. Во-вторых, если $t_t^{o2} > 0$, то $t_t^{o1} = 0$. Это связано с тем, что оператор не может одновременно обслуживать заявки двух типов.

Итерационные формулы

Выведем формулы, необходимые для имитационного моделирования СМО. На стохастическом базисе $B = (\Omega, \mathcal{F}, F = (\mathcal{F}_t)_{t \geq 0}, P)$ из формул (1)-(14) можно получить следующие инфинитезимальные соотношения:

$$P\{A_{t+\Delta}^1 - A_t^1 = 1 | \mathcal{F}_t\} = \lambda_1 \cdot \Delta + o(\Delta), \quad (15)$$

$$P\{A_{t+\Delta}^2 - A_t^2 = 1 | \mathcal{F}_t\} = \lambda_2 \cdot \Delta + o(\Delta), \quad (16)$$

$$P\{D_{t+\Delta}^1 - D_t^1 = 1 | \mathcal{F}_t\} = \mu_t^1 \cdot \Delta + o(\Delta), \quad (17)$$

$$P\{D_{t+\Delta}^2 - D_t^2 = 1 | \mathcal{F}_t\} = \mu_t^2 \cdot \Delta + o(\Delta). \quad (18)$$

Основываясь на понятие геометрической вероятности, по формулам (15)-(18) проведем имитационное моделирование. А именно, введя дискретизацию (шаг по времени) Δ из условия $\lambda_1 \cdot \Delta \ll 1$, $\lambda_2 \cdot \Delta \ll 1$, $\mu_t^1 \cdot \Delta \ll 1$, $\mu_t^2 \cdot \Delta \ll 1$ получим следующие итерационные формулы (для вычисления значений процессов в момент времени $t + \Delta$ через значения процессов в момент t):

$$A_{t+\Delta}^1 = A_t^1 + \delta(\lambda_1), \quad (19)$$

$$A_{t+\Delta}^2 = A_t^2 + \delta(\lambda_2), \quad (20)$$

$$D_{t+\Delta}^1 = D_t^1 + \delta(\mu_t^1), \quad (21)$$

$$D_{t+\Delta}^2 = D_t^2 + \delta(\mu_t^2), \quad (22)$$

где $\delta(\gamma) = \begin{cases} 1, & \text{с вероятностью } \gamma \cdot \Delta, \\ 0, & \text{с вероятностью } 1 - \gamma \cdot \Delta. \end{cases}$

Оставшиеся параметры вычисляем следующим образом:

$$q_{t+\Delta}^1 = q_t^1 + I(A_t^1 + A_t^2 - D_t^1 - D_t^2 > 0)\Delta A_t^1 - I(q_t^1 > 0, q_t^2 = 0)\Delta D_t^1 - I(q_t^1 > 0, q_t^2 = 0)\Delta D_t^2, \quad (23)$$

$$t_{t+\Delta}^{o1} = t_t^{o1} + (t + \tau_1) \cdot I(A_t^1 + A_t^2 - D_t^1 - D_t^2 = 0)\Delta A_t^1 + (t + \tau_1 - t_t^{o1}) \cdot I(q_t^1 > 0, q_t^2 = 0)\Delta D_t^1 + (t + \tau_1) \cdot I(q_t^1 > 0, q_t^2 = 0)\Delta D_t^2 - t_t^{o1}I(q_t^1 = 0)\Delta D_t^1 - t_t^{o1}I(q_t^2 > 0)\Delta D_t^1, \quad (24)$$

$$q_{t+\Delta}^2 = q_t^2 + I(A_t^1 + A_t^2 - D_t^1 - D_t^2 > 0)\Delta A_t^2 - I(q_t^2 > 0)\Delta D_t^1 - I(q_t^2 > 0)\Delta D_t^2, \quad (25)$$

$$t_{t+\Delta}^{o2} = t_t^{o2} + (t + \tau_2) \cdot I(A_t^1 + A_t^2 - D_t^1 - D_t^2 > 0)\Delta A_t^2 + (t + \tau_2) \cdot I(q_t^2 > 0)\Delta D_t^1 + (t + \tau_2) \cdot I(q_t^2 > 0)\Delta D_t^2 - t_t^{o2}I(q_t^2 = 0)\Delta D_t^2. \quad (26)$$

Здесь $\Delta A_t^1 = A_{t+\Delta}^1 - A_t^1$, $\Delta A_t^2 = A_{t+\Delta}^2 - A_t^2$, $\Delta D_t^1 = D_{t+\Delta}^1 - D_t^1$, $\Delta D_t^2 = D_{t+\Delta}^2 - D_t^2$.

Результаты компьютерного моделирования

Практическая реализация СМО осуществлена с помощью языка программирования высокого уровня C# в среде разработки Visual Studio 2022. На рисунке 2 представлен результат моделирования систем при параметрах $\tau_1 = 2$, $\tau_2 = 1$, $\lambda_1 = 2$, $\lambda_2 = 1$ и времени моделирования $T = 10$.

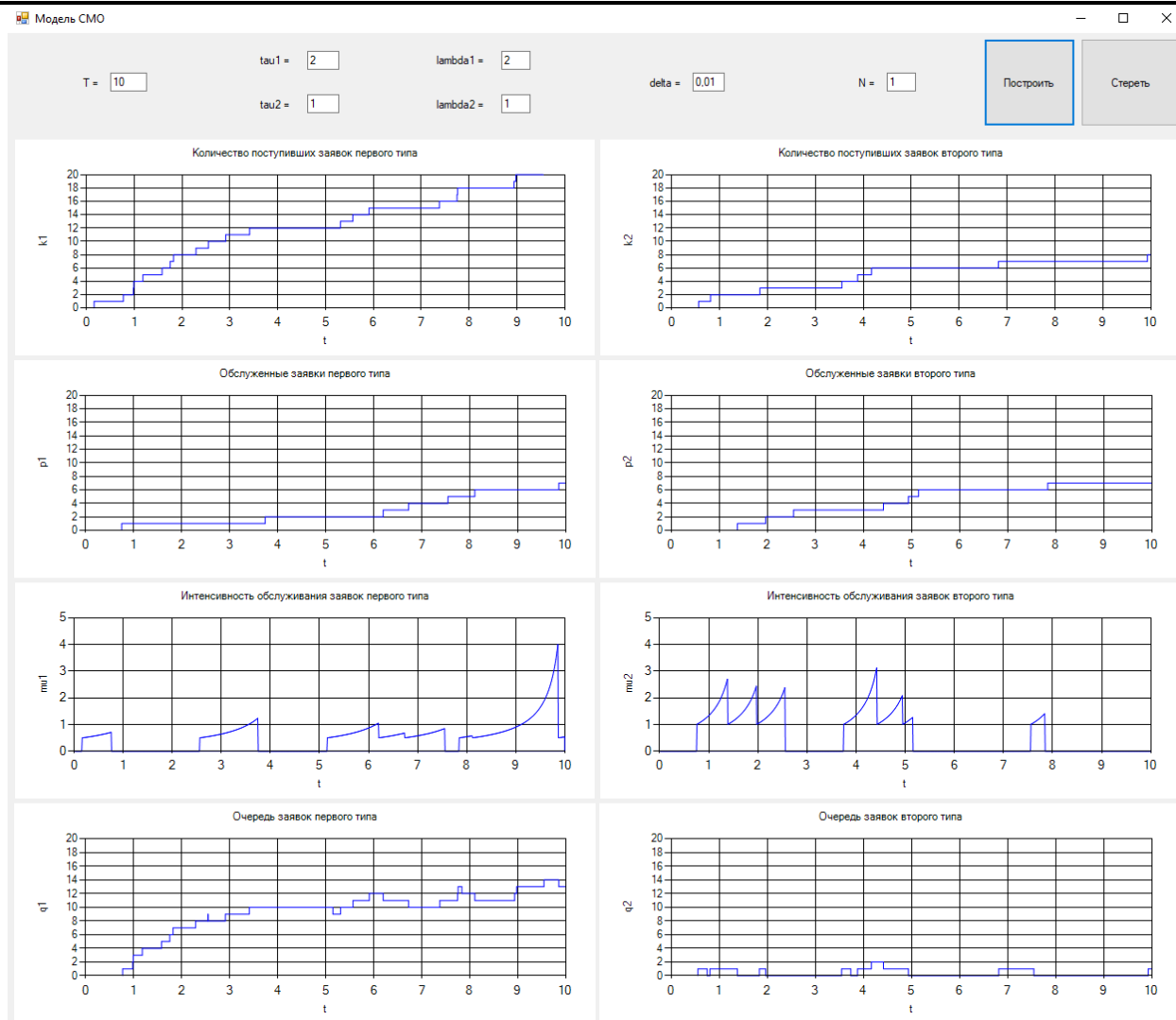


Рисунок 2 - Модель СМО

Результаты моделирования показывают, что с данными входными параметрами система перегружена, растет очередь заявок первого типа. Однако, важные заявки обслуживаются своевременно, что и являлось основной задачей модели.

Заключение

В результате выполнения данной работы была построена математическая модель системы массового обслуживания «точно-в-срок» с относительным приоритетом в семимартингальных терминах. Показан переход от математической модели к итерационным формулам, по которым было проведено имитационное моделирование.

Список литературы

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Вестник Самарского государственного технического университета. Серия: Физикоматематические науки. 2018, т. 22, №. 3, с. 518-531.
2. Бутов А.А. Оценивание параметров распределенных продуктивных систем, работающих по принципу «точно в срок» // Автомат. и телемех. 2020, № 3, с.14–27.

3. Бородин А.Н. Случайные процессы: Учебник. СПб.: Изд-во «Лань», 2013.
4. Бутов, А.А. Теория случайных процессов и её дополнительные главы: учеб. пособие. Ч. 1. Введение в стохастическое исчисление. Ульяновск : УлГУ, 2016
5. Бутов, А.А. Теория случайных процессов и её дополнительные главы: учеб. пособие. Ч. 2. Случайное блуждание, винеровский процесс, стохастический интеграл, диффузионные процессы. Ульяновск : УлГУ, 2021

References

1. Butov A.A., Kovalenko A.A. Stochastic models of simple controlled systems just-in-time // Bulletin of the Samara State Technical University. Series: Physical and Mathematical Sciences. 2018, vol. 22, No. 3, pp. 518-531.
 2. Butov A.A. Estimation of parameters of distributed productive systems operating on the principle of "just in time" // Automaton. and telemech. 2020, No. 3, pp.14-27.
 3. Borodin A.N. Random processes: Textbook. St. Petersburg: Publishing house "Lan", 2013.
 4. Butov, A.A. Theory of Random Processes and Its Additional Chapters. allowance. Part 1. Introduction to Stochastic Calculus. Ulyanovsk : Ulyanovsk State University, 2016
 5. Butov, A.A. Theory of Random Processes and Its Additional Chapters. allowance. Part 2. Random walk, Wiener process, stochastic integral, diffusion processes. Ulyanovsk : Ulyanovsk State University, 2021
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК: АНАЛИЗ ЭФФЕКТИВНЫХ СТРАТЕГИЙ И ИНСТРУМЕНТОВ

Овсянников Р.Я.

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:
rovsyannikov23@gmail.com

В современном мире количество сетевых атак стремительно растет, что требует эффективных методов защиты для предотвращения угроз и минимизации ущерба. В статье рассматриваются основные виды атак на сетевую инфраструктуру, приложения и пользователей, а также анализируются современные методы защиты, включая фильтрацию трафика, системы обнаружения вторжений, шифрование данных, сегментацию сетей и управление уязвимостями. Особое внимание уделено вопросам мониторинга безопасности и правового регулирования. Рассмотрены перспективы развития кибербезопасности, а также даны рекомендации по повышению защищенности сетевых систем.

Ключевые слова: Кибербезопасность, сетевые атаки, защита данных, шифрование, мониторинг безопасности, управление уязвимостями, правовое регулирование.

MODERN METHODS OF PROTECTION AGAINST NETWORK ATTACKS: ANALYSIS OF EFFECTIVE STRATEGIES AND TOOLS

Ovsiyannikov R.Ya.

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: rovsyannikov23@gmail.com

In the modern world, the number of network attacks is rapidly increasing, requiring effective protection methods to prevent threats and minimize damage. This article examines the main types of attacks on network infrastructure, applications, and users, as well as analyzes modern protection methods, including traffic filtering, intrusion detection systems, data encryption, network segmentation, and vulnerability management. Special attention is paid to security monitoring and legal regulations. The prospects for cybersecurity development are considered, and recommendations are provided for enhancing network security.

Keywords: Cybersecurity, network attacks, data protection, encryption, security monitoring, vulnerability management, legal regulation.

Введение

В условиях стремительного развития цифровых технологий и роста количества подключенных устройств проблема сетевой безопасности приобретает особую актуальность. Современные кибератаки становятся все более сложными и изощренными, что требует от организаций и частных пользователей применения эффективных мер защиты для предотвращения несанкционированного доступа, утечки данных и разрушительных последствий. Согласно статистике, число инцидентов, связанных с нарушением

кибербезопасности, ежегодно увеличивается, а финансовый и репутационный ущерб от атак продолжает расти.

Сетевые атаки представляют собой широкий спектр угроз, направленных на компрометацию сетевой инфраструктуры, нарушение работы сервисов, хищение конфиденциальных данных и манипуляцию информационными потоками. Вредоносные действия злоумышленников могут включать DDoS-атаки, перехват данных, использование уязвимостей программного обеспечения, фишинг, внедрение вредоносного кода и атаки на сетевые протоколы. В связи с этим разработка и внедрение современных механизмов защиты становится необходимым условием для обеспечения безопасного функционирования цифровых систем.

Цель данной статьи — проанализировать основные виды сетевых атак, рассмотреть традиционные и современные методы защиты, а также оценить перспективные направления развития кибербезопасности. В работе рассматриваются как технические, так и организационные меры, направленные на повышение устойчивости сетевой инфраструктуры к угрозам. Особое внимание уделяется мониторингу сетевого трафика, управлению уязвимостями, сегментации сетей, использованию криптографических методов защиты и внедрению стандартов безопасности.

Таким образом, защита от сетевых атак требует комплексного подхода, включающего превентивные меры, своевременное выявление угроз и эффективные механизмы реагирования. В статье представлена подробная классификация атак, анализируются наиболее распространенные методы противодействия им, а также рассматриваются правовые аспекты регулирования кибербезопасности.

Основные виды сетевых атак

Современные киберугрозы охватывают широкий спектр атак, направленных на нарушение работы сетевой инфраструктуры, компрометацию данных и манипуляцию информацией. Эти атаки можно условно разделить на несколько категорий: атаки на уровень сетевой инфраструктуры, атаки на уровень приложений и атаки, нацеленные на конечных пользователей.

Одной из наиболее распространенных угроз являются атаки на уровень сетевой инфраструктуры, в том числе DDoS-атаки, направленные на перегрузку серверов и отказ в обслуживании пользователей. Такие атаки, как UDP Flood, SYN Flood и HTTP Flood, используют массовые запросы для истощения ресурсов сети. Вредоносный трафик создается с помощью ботнетов, объединяющих тысячи зараженных устройств. Еще одной серьезной угрозой является компрометация сетевых протоколов, например, атаки на маршрутизаторы и коммутаторы, такие как BGP Hijacking и ARP Spoofing. Они позволяют злоумышленникам перенаправлять трафик, подменять данные и перехватывать конфиденциальную информацию.

На уровне приложений особую опасность представляют инъекционные атаки, такие как SQL-инъекции и межсайтовый скриптинг (XSS). SQL-инъекции используются для внедрения вредоносных команд в базы данных, что позволяет хакерам извлекать, модифицировать или удалять критически важную информацию. Атаки XSS, в свою очередь, направлены на внедрение вредоносных скриптов в веб-страницы, что может привести к краже данных пользователей или выполнению несанкционированных действий от их имени. Другим видом

атак являются атаки на веб-сессии, например, перехват cookies или угон сессий (Session Hijacking), что позволяет злоумышленникам получить доступ к аккаунтам пользователей.

Не менее опасны атаки, нацеленные на пользователей, которые чаще всего связаны с методами социальной инженерии. Фишинговые атаки представляют собой попытки обманом путем получить учетные данные пользователей через поддельные веб-сайты, электронные письма или сообщения. Вредоносные ссылки, замаскированные под легитимные ресурсы, могут приводить к загрузке вредоносного программного обеспечения или передаче персональных данных злоумышленникам. Еще одной распространенной угрозой является манипуляция с DNS (DNS Spoofing, Cache Poisoning), позволяющая перенаправлять пользователей на поддельные сайты для кражи их данных.

Таким образом, разнообразие сетевых атак требует комплексного подхода к защите, включающего мониторинг сетевого трафика, своевременное выявление угроз и использование надежных механизмов защиты данных. В следующих разделах рассматриваются эффективные методы противодействия данным атакам [1].

Классические методы защиты от сетевых атак

В современных условиях обеспечение кибербезопасности требует применения комплексных методов защиты, направленных на предотвращение атак, обнаружение угроз и быстрое реагирование на инциденты. Эффективная защита включает несколько ключевых направлений: фильтрацию трафика, аутентификацию и шифрование, мониторинг безопасности, управление уязвимостями, сегментацию сети и использование специализированных защитных систем [2].

Одним из фундаментальных методов защиты является фильтрация сетевого трафика, которая позволяет выявлять и блокировать вредоносную активность. Для этого применяются межсетевые экраны (firewalls), которые контролируют входящий и исходящий трафик на основе заранее заданных правил. Помимо традиционных файрволов, используются системы глубокого анализа пакетов (DPI), позволяющие анализировать содержимое трафика и блокировать подозрительные соединения. Специализированные решения, такие как системы предотвращения вторжений (IPS) и обнаружения вторжений (IDS), помогают выявлять аномалии и блокировать попытки компрометации сети.

Не менее важной мерой является аутентификация и шифрование данных, которые защищают информацию от несанкционированного доступа. Для этого применяются многофакторная аутентификация (MFA), криптографические протоколы (TLS, IPsec) и механизмы безопасного хранения паролей. Шифрование данных при передаче предотвращает их перехват злоумышленниками, а цифровые сертификаты гарантируют подлинность участников обмена данными [3].

Мониторинг безопасности и анализ аномалий играют ключевую роль в своевременном обнаружении атак. Современные системы безопасности используют поведенческий анализ и технологии машинного обучения для выявления подозрительной активности. Логирование событий и анализ сетевого трафика позволяют отслеживать попытки вторжений, а также обеспечивать оперативное реагирование на инциденты. Особую роль в мониторинге играют Security Information and Event Management (SIEM) системы, которые централизованно собирают и анализируют данные о безопасности из различных источников.

Еще одним важным аспектом является управление уязвимостями, включающее регулярные обновления программного обеспечения, патчинг критических уязвимостей и контроль конфигураций сетевых устройств. Использование автоматизированных сканеров уязвимостей позволяет выявлять слабые места в инфраструктуре и устранять их до того, как они будут использованы злоумышленниками.

Сегментация сети и контроль доступа помогают минимизировать риски распространения атак внутри инфраструктуры. Разделение сети на логические сегменты с ограничением доступа между ними снижает вероятность компрометации всей системы при атаке на один из узлов. Использование принципа минимально необходимого доступа (Least Privilege) и ролевой модели управления доступом (RBAC) предотвращает несанкционированное использование ресурсов.

Дополнительно, для защиты от DDoS-атак применяются специализированные анти-DDoS решения, которые анализируют трафик и автоматически фильтруют вредоносные запросы. Такие технологии используют эвристические алгоритмы и искусственный интеллект для адаптивного реагирования на угрозы.

Таким образом, защита от сетевых атак требует комплексного подхода, включающего технические, организационные и административные меры. Современные методы безопасности направлены не только на предотвращение атак, но и на их быстрое выявление и устранение последствий, что позволяет минимизировать ущерб и обеспечивать надежную работу сетевой инфраструктуры [4].

Итоги и перспективы развития кибербезопасности

Сетевые атаки продолжают эволюционировать, становясь все более сложными и изощренными, что требует постоянного совершенствования методов защиты. В результате анализа современных угроз можно сделать вывод о необходимости комплексного подхода к обеспечению кибербезопасности, включающего фильтрацию трафика, многоуровневую аутентификацию, шифрование данных, мониторинг активности и эффективное управление уязвимостями [5].

Одним из ключевых трендов в развитии защиты от сетевых атак является интеграция технологий искусственного интеллекта и машинного обучения в системы кибербезопасности. Современные алгоритмы позволяют в реальном времени анализировать большие объемы данных, выявлять аномалии и предсказывать потенциальные атаки на основе поведения пользователей и сетевого трафика. Автоматизированные системы реагирования помогают оперативно блокировать угрозы, снижая нагрузку на специалистов по безопасности.

Еще одним перспективным направлением является развитие концепции Zero Trust, которая предполагает полный контроль и верификацию всех пользователей и устройств перед предоставлением доступа к ресурсам. Этот подход минимизирует риски атак за счет строгого разграничения прав доступа и постоянного мониторинга активности в сети.

Кроме того, значительную роль играет развитие международного сотрудничества в сфере кибербезопасности. Разработка единых стандартов защиты, обмен информацией об угрозах и координация действий между государственными и частными организациями позволяют быстрее реагировать на новые угрозы и обеспечивать высокий уровень защиты критической инфраструктуры.

Необходимость постоянного обучения и повышения осведомленности пользователей также остается важным фактором в обеспечении безопасности. Большая часть атак, таких как фишинг и социальная инженерия, становится возможной из-за человеческого фактора. Развитие программ киберграмотности и внедрение строгих политик безопасности на предприятиях помогут снизить риск успешных атак.

Таким образом, перспективы развития кибербезопасности связаны с внедрением новых технологий, усилением контроля доступа, развитием международного сотрудничества и повышением уровня осведомленности пользователей. В условиях быстро меняющейся цифровой среды обеспечение надежной защиты данных и сетевой инфраструктуры остается приоритетной задачей, требующей комплексного подхода и постоянного совершенствования методов защиты.

Список литературы

1. Алехин Р. В. и др. Анализ защищенности облачной инфраструктуры openstack при эмуляции атаки вида ddos на узлах инфраструктуры //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 52-55.
2. 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.
3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
4. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 490-492.
5. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

References

1. Alekhin R. V. et al. Analysis of the security of the openstack cloud infrastructure during the emulation of a ddos attack on infrastructure nodes //Actual Problems of Infocommunications in Science and Education (APINO 2023). – 2023. – pp. 52-55.
 2. Andrianov V. I., Romanov G. G., Shterenberg S. I. Expert Systems in the Field of Information Security //Actual Problems of Infocommunications in Science and Education. – 2015. – pp. 193-197.
 3. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of Automated Control Systems //Actual Problems of Infocommunications in Science and Education (APINO 2019). – 2019. – pp. 262-266.
 4. Kovalev I. A., Kosov N. A. Adversarial Attacks in Neural Networks //Actual Problems of Infocommunications in Science and Education (APINO 2021). – 2021. – pp. 490-492.
 5. Orlov G. A., Krasov A. V., Gelfand A. M. Application of Big Data in the Analysis of Large Data in Computer Networks //Knowledge-Intensive Technologies in Earth Space Research. – 2020. – Vol. 12. – No. 4. – pp. 76-84.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.738.5

АНАЛИЗ УЯЗВИМОСТЕЙ И МЕТОДЫ ЗАЩИТЫ В ИНТЕРНЕТЕ ВЕЩЕЙ (IOT) С УЧЕТОМ РАСТУЩЕЙ СЛОЖНОСТИ СЕТЕЙ И УСТРОЙСТВ

Овсянников Р.Я.

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:
rovsyannikov23@gmail.com

В статье рассматриваются современные уязвимости, связанные с интернетом вещей (IoT), а также методы и инструменты для их обнаружения и предотвращения. Особое внимание уделяется растущей сложности сетей и устройств IoT и ее влиянию на безопасность. Анализируются основные угрозы, с которыми сталкиваются устройства IoT, и обсуждаются современные подходы к защите, включая шифрование, аутентификацию и мониторинг сетевого трафика.

Ключевые слова: Интернет вещей, уязвимости, безопасность, сети IoT, защита, шифрование.

VULNERABILITY ANALYSIS AND PROTECTION METHODS IN THE INTERNET OF THINGS (IOT) GIVEN THE INCREASING COMPLEXITY OF NETWORKS AND DEVICES

Ovsyannikov R.Ya.

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: rovsyannikov23@gmail.com

This article explores contemporary vulnerabilities associated with the Internet of Things (IoT) as well as methods and tools for their detection and prevention. Special attention is paid to the growing complexity of IoT networks and devices and its impact on security. The paper analyzes the primary threats faced by IoT devices and discusses modern approaches to protection, including encryption, authentication, and network traffic monitoring.

Keywords: Internet of Things, vulnerabilities, security, IoT networks, protection, encryption.

Введение

С развитием технологий и стремительным ростом количества устройств, подключенных к интернету вещей (IoT), вопросы безопасности приобретают особую актуальность. IoT-экосистема охватывает широкий спектр устройств – от умных бытовых приборов и носимых гаджетов до промышленных систем управления и критически важных инфраструктур. Однако, несмотря на удобство и технологические преимущества, расширение IoT-среды сопровождается увеличением числа уязвимостей, которые могут использовать злоумышленники для кибератак, компрометации данных и нарушения работы сетей.

Одной из ключевых проблем безопасности IoT является ограниченность вычислительных ресурсов устройств, что не позволяет внедрять сложные алгоритмы защиты. Многие IoT-устройства разрабатываются с акцентом на функциональность и

энергоэффективность, а вопросы безопасности часто остаются второстепенными. В результате устройства могут использовать слабые механизмы аутентификации, передавать данные в незашифрованном виде и обладать уязвимым встроенным программным обеспечением. Кроме того, высокая степень взаимосвязанности IoT-устройств в сетях приводит к тому, что компрометация одного узла может повлечь за собой массовое заражение всей системы, что делает атаки особенно опасными.

Еще одной серьезной угрозой является недостаточная сегментация сетей, когда IoT-устройства подключены к той же инфраструктуре, что и критически важные системы. Это позволяет злоумышленникам проникать в корпоративные или промышленные сети, используя IoT-устройства в качестве точки входа. Помимо этого, распространенными угрозами остаются атаки типа «человек посередине» (MITM), перехват данных, взлом слабых паролей и эксплуатация уязвимостей в прошивках.

Учитывая возрастающую сложность IoT-сетей и устройств, а также расширяющийся спектр атак, необходимо разрабатывать и внедрять надежные методы защиты. Данная статья рассматривает основные уязвимости, характерные для интернета вещей, анализирует современные методы обеспечения безопасности и перспективы дальнейшего развития технологий защиты. В работе уделяется внимание таким аспектам, как шифрование данных, аутентификация устройств, сегментация сетей, мониторинг аномальной активности и внедрение современных стандартов безопасности. Кроме того, рассматриваются перспективные решения, включая применение искусственного интеллекта и блокчейн-технологий, позволяющих повысить устойчивость IoT-систем к угрозам [1].

Уязвимости в сетях IoT

Интернет вещей (IoT) сочетает в себе огромное количество устройств, взаимодействующих друг с другом в сложных сетях, что создает множество потенциальных точек уязвимости. Из-за ограниченных вычислительных возможностей, недостаточных мер безопасности и слабой стандартизации IoT-системы часто становятся мишенями для кибератак. Одной из ключевых проблем является недостаточная аутентификация и авторизация. Многие устройства используют слабые, предустановленные или статические пароли, что делает их уязвимыми для атак методом перебора или захвата учетных данных. Отсутствие многофакторной аутентификации и надежных механизмов контроля доступа увеличивает вероятность компрометации.

Еще одной серьезной уязвимостью является отсутствие шифрования данных. Передача информации между устройствами и серверами часто осуществляется по устаревшим или незащищенным протоколам, таким как HTTP вместо HTTPS, что делает возможным перехват и анализ сетевого трафика злоумышленниками в рамках атак «человек посередине» (MITM). В результате хакеры могут не только получить доступ к передаваемой информации, но и изменять ее или подделывать команды управления устройствами. Уязвимости встроенного программного обеспечения (ПО) также представляют серьезную угрозу. Многие IoT-устройства работают на прошивках, которые редко обновляются производителями, а иногда и вовсе остаются без поддержки. В случае обнаружения уязвимостей злоумышленники могут использовать их для выполнения атак, таких как удаленное исполнение кода или повышение привилегий, что дает им полный контроль над устройством [2-3].

Отдельной проблемой является недостаточная сегментация сетей. IoT-устройства часто подключаются к тем же сетям, что и критически важные сервисы, такие как корпоративные базы данных, промышленные системы управления и облачные инфраструктуры. Это позволяет злоумышленникам, взломав одно устройство, проникнуть глубже в сеть и атаковать другие узлы, включая серверы и рабочие станции. Отсутствие изоляции IoT-устройств способствует быстрому распространению атак внутри инфраструктуры. Кроме того, уязвимые IoT-устройства часто используются в составе ботнетов, как показали атаки, подобные Mirai. Массовая инфицированность устройств и их слабая защищенность делают их удобной мишенью для создания зомби-сетей, применяемых для DDoS-атак, распространения вредоносного ПО и других преступных действий.

Физическая безопасность IoT-устройств также остается актуальной проблемой. Они часто располагаются в открытых или слабо защищенных местах, например, камеры видеонаблюдения, датчики в «умных» городах и промышленные контроллеры, что делает их уязвимыми для физического взлома. Злоумышленники могут получить прямой доступ к аппаратной части, модифицировать прошивку, извлечь учетные данные или внедрить вредоносный код. Еще одна важная угроза связана с атаками на радиointерфейсы и беспроводные сети. Многие IoT-устройства взаимодействуют через беспроводные технологии, такие как Wi-Fi, Bluetooth, Zigbee и LoRaWAN, которые подвержены атакам, включая перехват трафика, подделку команд управления и создание помех. Отсутствие надежной аутентификации в беспроводных сетях может привести к утечке конфиденциальных данных и перехвату управления устройствами [4-5].

Таким образом, IoT-среда остается крайне уязвимой из-за множества слабых мест, включая недостаточную защиту аутентификации, слабое шифрование данных, устаревшие прошивки, отсутствие сетевой сегментации и возможность использования устройств в ботнетах. Это делает вопросы безопасности критически важными для дальнейшего развития IoT-инфраструктуры. В следующих разделах статьи будут рассмотрены методы защиты и современные подходы к обеспечению безопасности IoT-устройств и сетей.

Методы защиты и обнаружения

Для обеспечения безопасности интернет вещей (IoT) необходимо применять комплексный подход, включающий защиту на уровне устройств, сетей и облачной инфраструктуры. Одним из ключевых аспектов является безопасная аутентификация и авторизация, которые позволяют ограничить несанкционированный доступ к устройствам. Для этого следует применять многофакторную аутентификацию (MFA), цифровые сертификаты и уникальные токены доступа, что снижает вероятность атак методом подбора паролей или компрометации учетных данных. Важно также отказаться от использования статических и предустановленных паролей, внедрив механизмы их регулярного обновления.

Шифрование данных играет центральную роль в защите IoT-сетей. Все передаваемые данные должны шифроваться с использованием современных протоколов, таких как TLS и DTLS. Для устройств с ограниченными вычислительными ресурсами можно применять легковесные алгоритмы, такие как AES-CCM или ECC, которые обеспечивают баланс между безопасностью и производительностью. Кроме того, необходимо защищать не только передаваемый, но и хранимый на устройствах контент, используя встроенные механизмы шифрования.

Обновление встроенного программного обеспечения (ПО) также является важной частью стратегии безопасности. Производители должны предоставлять регулярные патчи безопасности и реализовывать механизмы автоматического обновления прошивок. Кроме того, следует внедрять технологии защищенной загрузки (Secure Boot) и контроля целостности кода, которые позволяют проверять подлинность программного обеспечения перед его запуском. Это значительно усложняет внедрение вредоносного кода в систему.

Сегментация сетей — еще один эффективный метод защиты IoT-инфраструктуры. Разделение сети на изолированные сегменты с использованием VLAN и программно-определяемых сетей (SDN) помогает ограничить распространение атак. IoT-устройства должны подключаться к отдельным подсетям с минимальными привилегиями и ограниченным доступом к критически важным сервисам. Также рекомендуется применять брандмауэры и системы обнаружения вторжений (IDS/IPS), которые анализируют трафик и выявляют подозрительную активность.

Выявление аномалий и угроз с помощью машинного обучения и поведенческого анализа позволяет оперативно обнаруживать и блокировать потенциальные атаки. Такие системы анализируют поведение устройств и пользователей, выявляют нетипичные отклонения в активности и автоматически принимают меры для предотвращения угроз. Например, если устройство внезапно начинает отправлять большой объем данных на неизвестные серверы, система безопасности может заблокировать его соединение и уведомить администратора.

Дополнительно важным элементом защиты является контроль физического доступа к устройствам. IoT-устройства, расположенные в общественных местах, таких как «умные» камеры видеонаблюдения или датчики в городской инфраструктуре, должны быть защищены от несанкционированного физического вмешательства. Для этого применяются антивандальные корпуса, системы контроля доступа и механизмы обнаружения попыток несанкционированного вскрытия или модификации оборудования.

Таким образом, эффективная защита IoT-сетей требует многослойного подхода, включающего надежную аутентификацию, шифрование данных, регулярное обновление ПО, сегментацию сетей и мониторинг активности. Внедрение этих методов позволяет существенно снизить риски атак и обеспечить безопасность устройств, пользователей и инфраструктуры.

Современные тенденции и вызовы

Правовое регулирование и стандарты безопасности играют важную роль в обеспечении защиты экосистемы интернет вещей (IoT), создавая нормативную базу для производителей, разработчиков и пользователей. Различные страны разрабатывают и внедряют законы, направленные на повышение уровня безопасности IoT-устройств и минимизацию рисков, связанных с их эксплуатацией. В Европейском Союзе действует Закон о кибербезопасности, который устанавливает требования к сертификации IoT-продуктов и обязывает производителей соблюдать стандарты безопасности на всех этапах жизненного цикла устройства. В США Национальный институт стандартов и технологий (NIST) разработал рекомендации по безопасности IoT, включая требования к управлению уязвимостями, аутентификации, шифрованию и обновлению прошивок.

Международные организации также активно разрабатывают стандарты безопасности для IoT. Международный союз электросвязи (ITU) выпускает рекомендации по обеспечению защищенных IoT-экосистем, включая требования к конфиденциальности данных,

устойчивости к атакам и надежности связи. ISO/IEC 27001 и ISO/IEC 29147 содержат ключевые принципы управления рисками и раскрытия уязвимостей, что позволяет компаниям минимизировать угрозы. Кроме того, стандарт ETSI EN 303 645, разработанный Европейским институтом телекоммуникационных стандартов (ETSI), определяет базовые требования к безопасности IoT-устройств, включая запрет на использование предустановленных паролей, обязательное шифрование данных и механизмы безопасного обновления прошивок.

Важным аспектом регулирования является защита персональных данных пользователей. Законодательные акты, такие как Общий регламент по защите данных (GDPR) в Европе и Закон о конфиденциальности потребителей Калифорнии (CCPA) в США, устанавливают строгие правила обработки, хранения и передачи пользовательской информации. IoT-устройства, которые собирают и передают персональные данные, должны соответствовать этим требованиям, обеспечивая анонимизацию, шифрование и возможность контроля со стороны пользователя.

Несмотря на наличие стандартов и законодательных норм, их соблюдение остается серьезным вызовом. Многие производители игнорируют требования безопасности из-за высокой стоимости их внедрения или нехватки компетенций в области киберзащиты. В результате на рынке продолжают появляться устройства с низким уровнем защиты, что делает их уязвимыми для атак. Для эффективного соблюдения стандартов необходимо внедрение механизмов обязательной сертификации IoT-устройств, а также разработка единых международных норм, которые позволят создать универсальные правила для всех производителей.

В перспективе развитие нормативной базы IoT будет направлено на усиление требований к безопасности, внедрение автоматизированных механизмов мониторинга и контроля устройств, а также разработку новых технологий защиты, соответствующих растущей сложности сетей и угроз. Совместная работа государств, международных организаций и частного сектора позволит создать более безопасную и устойчивую экосистему интернет вещей, способную противостоять киберугрозам и обеспечивать защиту данных пользователей.

Итоги и перспективы

Безопасность интернет вещей (IoT) остается одной из ключевых проблем цифровой эпохи, поскольку увеличение количества подключенных устройств приводит к росту потенциальных угроз и уязвимостей. В ходе анализа были рассмотрены основные риски, присущие IoT-инфраструктуре, включая недостаточную аутентификацию, слабую защиту передаваемых данных, уязвимости встроенного программного обеспечения, отсутствие сетевой сегментации и угрозы, связанные с ботнетами и DDoS-атаками. Эти факторы делают IoT привлекательной целью для киберпреступников, способных использовать скомпрометированные устройства для атак на критически важные системы.

В качестве мер защиты предлагается комплексный подход, включающий надежные механизмы аутентификации, шифрование данных, регулярное обновление прошивок, сегментацию сетей и использование средств мониторинга активности. Внедрение многофакторной аутентификации (MFA), использование цифровых сертификатов и уникальных токенов позволит предотвратить несанкционированный доступ. Шифрование трафика с применением современных алгоритмов обеспечит защиту передаваемых данных от

перехвата. Регулярные обновления прошивок и использование механизмов защищенной загрузки (Secure Boot) снизят вероятность эксплуатации уязвимостей в программном обеспечении устройств. Дополнительно сегментация сетей с помощью VLAN и SDN, а также применение систем обнаружения вторжений (IDS/IPS) помогут минимизировать риск распространения атак внутри инфраструктуры.

Особое внимание следует уделить нормативно-правовому регулированию безопасности IoT. Введение обязательных стандартов и сертификации IoT-устройств повысит общий уровень защиты экосистемы. Международные инициативы, такие как стандарты ETSI EN 303 645, рекомендации NIST и требования GDPR, уже закладывают основу для более безопасного развертывания IoT, но их соблюдение остается проблемой из-за отсутствия единых глобальных норм и механизмов контроля.

В перспективе развитие технологий искусственного интеллекта (ИИ) и машинного обучения (ML) позволит более эффективно выявлять угрозы и аномалии в поведении IoT-устройств, что обеспечит автоматизированную защиту от кибератак. Кроме того, использование технологии блокчейна может улучшить управление идентификацией устройств и повысить уровень доверия в распределенных IoT-сетях. Концепция Zero Trust, которая предполагает проверку каждого устройства и запрет на свободный доступ к сети без строгой верификации, также будет играть важную роль в будущем развитии безопасности IoT.

Таким образом, несмотря на значительные вызовы, связанные с безопасностью интернета вещей, применение современных технологий, совершенствование нормативной базы и повышение осведомленности пользователей позволят создать более защищенную и устойчивую экосистему. Важно продолжать исследования в этой области, разрабатывать новые методы противодействия угрозам и внедрять эффективные механизмы защиты, чтобы минимизировать риски и обеспечить безопасное развитие IoT-инфраструктуры.

Список литературы

1. Волкогинов 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.
2. Гельфанд А. М. и др. ОЦЕНКА РИСКОВ И УГРОЗ БЕЗОПАСНОСТИ В СРЕДЕ «УМНЫЙ ДОМ» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.
3. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEMML.

References

1. Volkogonov V. N. et al. Application of Physically Unclonable Functions for Authentication in the Internet of Things Environment // Actual Problems of Infocommunications in Science and Education. – 2021. – pp. 409-414.
 2. Gelfand A. M. et al. Risk Assessment and Security Threats in the Smart Home Environment // Actual Problems of Infocommunications in Science and Education (APINO 2020). – 2020. – pp. 316-321.
 3. Katasonov A. I., Tsvetkov A. Y. Analysis of Access Control Mechanisms in Special-Purpose Systems // Actual Problems of Infocommunications in Science and Education (APINO 2020). – 2020. – pp. 563-568.
 4. Petrova T. V. et al. Approaches to Detecting Rogue Wireless Access Points in a Local Area Network // Regional Informatics (RI-2022). – 2022. – pp. 572-573.
 5. Shterenberg, S. I. Computer Viruses / S. I. Shterenberg, A. V. Krasov, A. Yu. Tsvetkov. Volume Part 1. – Saint Petersburg : Saint Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruевич, 2015. – p. 63 – EDN CMMEML.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.942:658.51

ОПТИМИЗАЦИЯ ПЛАНИРОВАНИЯ ПАРТИИ ИЗДЕЛИЙ В УСЛОВИЯХ ОГРАНИЧЕННЫХ ПРОИЗВОДСТВЕННЫХ РЕСУРСОВ

Ветров С.Ю.

*ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993,
Москва, Волоколамское ш., д. 4), e-mail: vetrov241201@yandex.ru*

В статье рассматривается задача оптимизации планирования производства партии изделий в условиях ограниченных производственных ресурсов. Предложена математическая модель, учитывающая технологические зависимости между деталями, ограничения на использование цехов и необходимость минимизации общего времени производства. Модель основана на комбинаторной оптимизации и включает в себя такие параметры, как время изготовления деталей, их распределение по цехам и соблюдение приоритетов сборки. Особое внимание уделено учету параллельного производства и предотвращению конфликтов при назначении ресурсов. Решение задачи направлено на повышение эффективности производственного процесса за счет рационального распределения работ по времени и цехам. Результаты работы имеют широкое практическое применение в машиностроении, приборостроении и других отраслях с многоуровневыми производственными процессами.

Ключевые слова: Оптимизация производства, планирование партии изделий, ограниченные ресурсы, математическая модель, комбинаторная оптимизация, технологические зависимости, распределение ресурсов, минимизация времени производства.

OPTIMIZATION OF PRODUCT BATCH PLANNING IN CONDITIONS OF LIMITED PRODUCTION RESOURCES

Vetrov S.Y.

*MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia,
(125993, Moscow, Volokolamskoye shosse, 4), e-mail: vetrov241201@yandex.ru*

The article considers the problem of optimization of planning of production of a batch of products under conditions of limited production resources. A mathematical model that takes into account technological dependencies between parts, limitations on the use of shops and the need to minimize the total production time is proposed. The model is based on combinatorial optimization and includes such parameters as manufacturing time of parts, their distribution over shops and observance of assembly priorities. Special attention is paid to accounting for parallel production and avoiding conflicts in resource assignment. The solution of the problem is aimed at improving the efficiency of the production process through rational distribution of work by time and shops. The results of the work have a wide practical application in mechanical engineering, instrument making and other industries with multilevel production processes.

Keywords: Production optimization, batch planning, limited resources, mathematical model, combinatorial optimization, technological dependencies, resource allocation, minimization of production time.

Введение

Задача планирования производства конечного изделия и партии изделий представляет собой сложную задачу комбинаторной оптимизации. Она включает в себя учет технологических зависимостей между деталями, ограничений на использование ресурсов

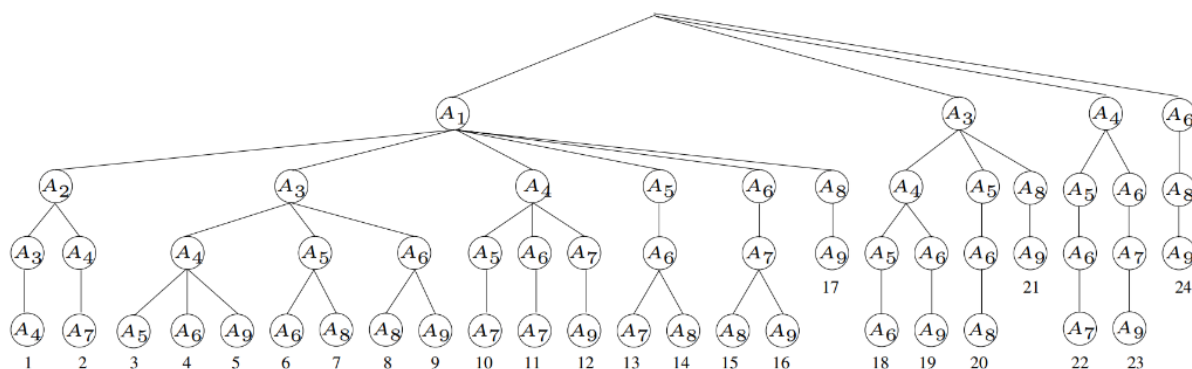
(цехов) и минимизацию общего времени производства. Рассмотрим подробно математическую модель этой задачи, её основные компоненты и целевую функцию.

Постановка задачи

Имеется древовидная структура деталей, где каждая деталь может состоять из других деталей. Верхний уровень дерева содержит одну конечную деталь (изделие), которая является результатом сборки всех нижележащих деталей. Каждая деталь имеет время изготовления и производится в определенном цехе. Учитываются следующие условия:

1. Технологические зависимости: Производство верхней детали возможно только после завершения всех её дочерних деталей.
2. Ограничения по цехам: Детали, производимые в одном цехе, не могут изготавливаться одновременно.
3. Ограниченные ресурсы: Количество цехов и их возможности ограничены.
4. Параллельное производство: Детали из разных изделий одной партии не могут производиться одновременно в одном цехе.

Цель состоит в том, чтобы найти оптимальный порядок выполнения работ, распределить детали по цехам и минимизировать общее время производства всей партии.



Математическая модель

Обозначения

- N : множество всех деталей, включая конечное изделие.
- $N_r \subset N$: множество деталей, производимых в цехе r .
- R : множество всех цехов.
- K : количество изделий в партии.
- p_{ik} : время изготовления детали i в изделии k .
- S_{ik} : время начала изготовления детали i в изделии k .
- $C_{ik} = S_{ik} + p_{ik}$: время завершения изготовления детали i в изделии k .
- $P(i)$: родительская деталь для детали i .
- x_{ikr} : бинарная переменная, равная 1, если деталь i из изделия k производится в цехе r , и 0 иначе.
- δ_{ijk} : бинарная переменная, равная 1, если деталь i из изделия k производится раньше детали j из изделия k в одном цехе, и 0 иначе.
- T : общее время производства всей партии.

Ограничения

1. Соблюдение иерархии деталей (технологические зависимости)

Производство детали возможно только после завершения всех её дочерних компонентов:

$$S_{ik} \geq C_{jk}, \quad \forall i \in N, j \in P(i), k \in K.$$

Это ограничение отражает логику процесса производства: невозможно начать сборку верхней детали, пока не будут готовы все её составляющие [1]. Например, если деталь А состоит из деталей В и С, то производство А может начаться только после завершения В и С.

2. Ограничение работы цехов (одновременное производство)

Детали, изготавливаемые в одном цехе, не могут изготавливаться одновременно:

$$S_{ik} \geq C_{jk} \cdot \delta_{ijk} + (1 - \delta_{ijk})M, \quad \forall i, j \in N_r, i \neq j, k \in K, r \in R,$$

$$S_{jk} \geq C_{ik} \cdot (1 - \delta_{ijk}) + \delta_{ijk}M, \quad \forall i, j \in N_r, i \neq j, k \in K, r \in R,$$

где М — большое число, используемое для устранения наложений работ.

Это ограничение гарантирует, что в рамках одного цеха не будет происходить одновременное выполнение двух операций. Например, если цех r производит детали X и Y, то одна из них должна быть завершена до начала другой [2].

3. Ограничение цехов (выбор цеха для каждой детали)

Каждая деталь должна быть назначена ровно в один цех:

$$\sum_{r \in R} x_{ikr} = 1, \quad \forall i \in N, k \in K.$$

Если деталь i производится в цехе r, то её время должно соответствовать ограничениям цеха:

$$S_{ik} \geq 0, \quad \forall i \in N, k \in K.$$

Это ограничение обеспечивает корректное распределение деталей по цехам, исключая возможность назначения одной детали сразу в несколько цехов.

4. Ограничение параллельного производства изделий

В одном цехе детали из разных изделий не могут производиться одновременно [3]:

$$S_{ik} \geq C_{jl} \quad \text{или} \quad S_{jl} \geq C_{ik}, \quad \forall i, j \in N_r, k \neq l, r \in R.$$

Это ограничение важно для партийного производства, когда несколько изделий собираются одновременно. Например, если цех r производит детали для изделий А и В, то он не может одновременно обрабатывать две детали из разных изделий.

5. Определение общего времени производства партии

Общее время производства — это максимальное время среди всех изделий:

$$T \geq C_{\text{root},k}, \quad \forall k \in K,$$

Здесь $C_{\text{root},k}$ — время завершения производства конечного изделия k. Общее время T определяется как момент, когда последнее изделие в партии будет полностью собрано.

Целевая функция

Минимизация общего времени производства:

$$\min T.$$

Целевая функция направлена на поиск такого распределения работ по времени и цехам, при котором общее время производства партии будет минимальным. Это особенно важно для повышения эффективности производства и снижения затрат [4].

Особенности модели

1. Учет ограниченных ресурсов

Ресурсы (цеха) являются ключевым ограничивающим фактором в задаче. Каждый цех имеет ограниченную пропускную способность, что накладывает дополнительные ограничения на планирование. Например, если цех может выполнять только одну операцию за раз, это существенно влияет на порядок выполнения работ.

2. Технологические зависимости

Технологические зависимости между деталями усложняют задачу планирования. Например, если деталь А зависит от деталей В и С, то любое изменение в сроках производства В или С автоматически влияет на сроки производства А. Это требует тщательного анализа и учета всех зависимостей.

3. Параллельное производство

Параллельное производство позволяет ускорить процесс изготовления партии изделий. Однако оно ограничено количеством доступных цехов и их возможностями. Например, если в партии 10 изделий, а доступно только 3 цеха, то необходимо грамотно распределить нагрузку между цехами, чтобы минимизировать общее время.

4. Комбинаторная сложность

Задача относится к классу NP-трудных задач, так как количество возможных вариантов распределения работ экспоненциально растет с увеличением числа деталей, изделий и цехов. Это делает её сложной для решения вручную, особенно для больших размерностей [5].

Пример практического применения

Рассмотрим пример с производством партии из 5 изделий, каждое из которых состоит из 3 деталей (А, В, С). Детали А и В производятся в цехе 1, а деталь С — в цехе 2. Время изготовления каждой детали составляет 2 часа. Задача заключается в том, чтобы определить оптимальный порядок выполнения работ и минимизировать общее время производства.

1. Шаг 1: Составляем математическую модель с учетом всех ограничений.

2. Шаг 2: Используем методы оптимизации (например, линейное программирование или эвристические алгоритмы) для нахождения решения.

3. Шаг 3: Анализируем результаты и корректируем план производства при необходимости.

Результатом будет оптимальный график производства, который позволит изготовить все 5 изделий за минимальное время [6].

Методы решения

Для решения задачи планирования производства можно использовать следующие подходы:

1. Линейное программирование: Подходит для небольших размерностей задачи, когда количество переменных и ограничений невелико.

2. Эвристические алгоритмы: Например, генетические алгоритмы или муравьиные колонии, которые позволяют находить приближенные решения для больших задач.

3. Метаэвристики: Такие методы, как имитация отжига или поиск с запретами, помогают улучшить качество решения за счет глобального поиска.

4. Специализированное программное обеспечение: Современные системы планирования производства (например, ERP-системы) часто включают встроенные инструменты для решения подобных задач.

Заключение

Представленная математическая модель позволяет решать задачу планирования производства конечного изделия и партии изделий с учетом технологических зависимостей, ограниченных ресурсов и минимизации общего времени производства. Эта задача относится к классу задач комбинаторной оптимизации и требует применения современных методов решения, таких как линейное программирование, эвристические алгоритмы или метаэвристики.

Правильное планирование производства играет ключевую роль в повышении эффективности производства, снижении затрат и сокращении времени выполнения заказов.

Список литературы

1. Построение математических моделей целочисленного линейного программирования. — Текст: электронный//nsc.ru: [сайт].—URL: http://old.math.nsc.ru/~alekseeva/Textbooks/textbook_model_building.pdf.
2. Планирование производственных операций. — Текст : электронный // Habr : [сайт]. — URL: <https://habr.com/ru/articles/672466/>.
3. Задача планирования производства. — Текст : электронный // studfile : [сайт]. — URL: <https://studfile.net/preview/6265539/page:3/>.
4. Модификация генетического алгоритма для решения задачи календарного планирования с ограниченными ресурсами. — Текст : электронный // donntu : [сайт]. — URL: <https://masters.donntu.ru/2018/fknt/strelnikov/library/article6.htm?ysclid=m8emgwgktm375778124>.
5. Выбор решения с учетом ограничений на ресурсы. — Текст : электронный // studfile : [сайт]. — URL: <https://studfile.net/preview/1097702/page:48/>.
6. Распределение производственных ресурсов в задачах объемного планирования в условиях неполноты данных. — Текст : электронный // cyberleninka : [сайт]. — URL: <https://cyberleninka.ru/article/n/raspredelenie-proizvodstvennyh-resursov-v-zadachah-obemnogo-planirovaniya-v-usloviyah-nepolnoty-dannyh>.

References

1. Construction of mathematical models of integer linear programming. — Text : electronic // nsc.ru: [website]. — URL: http://old.math.nsc.ru/~alekseeva/Textbooks/textbook_model_building.pdf.
2. Planning of production operations. — Text : electronic // Habr : [website]. — URL: <https://habr.com/ru/articles/672466/>.
3. The task of production planning. — Text : electronic // studfile : [website]. — URL: <https://studfile.net/preview/6265539/page:3/>.
4. Modification of the genetic algorithm to solve the problem of scheduling with limited resources. — Text : electronic // donntu : [website]. — URL:

<https://masters.donntu.ru/2018/fknt/strelnikov/library/article6.htm?ysclid=m8emgwgktm375778124>.

5. Choosing a solution based on resource constraints. — Text : electronic // studfile : [website]. — URL: <https://studfile.net/preview/1097702/page:48/>.
 6. Allocation of production resources in volume planning tasks in conditions of incomplete data. — Text : electronic // cyberleninka : [website]. — URL: <https://cyberleninka.ru/article/n/raspredelenie-proizvodstvennyh-resursov-v-zadachah-obemnogo-planirovaniya-v-usloviyah-nepolnoty-dannyh>.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8: 656.714

ИНТЕЛЛЕКТУАЛИЗАЦИЯ ПРОЦЕССОВ ЭКСПЛУАТАЦИИ СПЕЦТРАНСПОРТА

¹ Коникова Е.В. (научный руководитель), ² Федорин М.А.

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА", Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail: ¹elenavictorovnak@yandex.ru, ²makcfree@gmail.com

Современный мир требует от происходящих в нём процессов больше предсказуемости, надёжности и безопасности. Человеческий фактор продолжает оставаться самым гибким способом для решения проблем, однако последние создаются им самим. Для недопущения таких ситуаций, когда цена ошибки довольно высока, например, при обслуживании воздушных судов или при подготовке перрона к эксплуатации, необходимо отдавать приоритет новым технологиям, которые минимально зависят от человека.

Ключевые слова: Авиация, наземное обслуживание, эксплуатация аэродрома, организация движения на перроне, новые технологии, спецтранспорт, интеллектуализация, интеллектуальная транспортная система, искусственный интеллект.

INTELLECTUALIZATION OF SPECIAL TRANSPORT OPERATION PROCESSES

¹ Konikova E. V. (supervisor), ² Fedorin M. A.

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-mail: ¹elenavictorovnak@yandex.ru, ²makcfree@gmail.com

The modern world requires more predictability, reliability and security from the processes taking place in it. The human factor continues to be the most flexible way to solve problems, but the latter are created by itself. In order to avoid such situations where the cost of error is quite high, for example, when servicing aircraft or when preparing an apron for operation, it is necessary to give priority to new technologies that minimally depend on a person.

Keywords: Aviation, ground handling, airfield operation, apron traffic management, new technologies, special transport, intellectualization, intelligent transport system, artificial intelligence.

Современные технологии с каждым десятилетием стремительно развиваются, тем самым делая мир надёжным, прогностическим и безопасным. Без цифровизации, новых систем и высокотехнологичных механизмов невозможно представить экономику современного и успешно развивающегося государства.

В настоящее время новые технологии можно встретить практически в любой сфере деятельности, отрасли, в том числе и на транспорте, от которого зависит скорость и качество развития всего государства в целом, а также социальное благополучие граждан. В данной области новые технологии по большей части направлены на повышение комфортности и безопасности при выполнении транспортных процессов. Самым ярким примером применения

современных подходов к организации дорожного движения можно назвать интеллектуальные транспортные системы (ИТС).

Интеллектуальная транспортная система – это интегрированная автоматизированная система, при помощи инновационных методов организации и управления предоставляющая субъектам транспортной отрасли сервисы по планированию, координированию, информированию, а также более безопасному и эффективному использованию транспортных сетей [1].

Для уменьшения аварийности, заторов и загруженности дорог, для повышения эффективности дорожного движения (ДД) в целом в городских условиях обычно используется интеграция и создание единой системы, в которую входит различное оборудование, например, умные камеры видеонаблюдения, информационные табло, «умные» светофоры, спутниковые данные и т.д.

Современные аэропорты по своей сути являются своеобразными мини-городами, в которых происходят похожие процессы, что в своих более крупных аналогах. Если речь идёт про ДД, то в данном случае целесообразно сравнивать дороги общего пользования с аэродромом, где также присутствует разнообразный автомобильный транспорт и средства механизации. Здесь действуют такие же Правила дорожного движения, как и по всей стране, однако с некоторыми особенностями, которые приводятся в локальных документах главного оператора аэропорта [4]. От правильной организации движения воздушных судов, специального транспорта и средств механизмами на перроне зависит регулярность и безопасность полётов. Специфика аэродрома такова, что цена любой ошибки или халатности водителей, в результате чего происходит нарушение установленных правил или случаются столкновения, может достигнуть колоссальных масштабов и привести к серьезным финансовым и репутационным потерям.

На основании этого мы считаем целесообразным использование современных технологий организации ДД на перроне. Такой опыт можно найти при работе ИТС в городских условиях с учётом авиационной специфики. Приведём некоторые примеры технологий и разработок, которые могут применяться в современных условиях на перронах [3].

1. Технологии блокчейна. Создаёт более безопасное и эффективное управление транспортными средствами, используя технологию распределенного реестра для учета и управления данными о движении на дорогах. Также разрабатываются системы управления трафиком на основе данных о движении, создаются системы управления транспортным потоком, что позволяет в целом увеличить уровень безопасности на дорогах. Технология также может быть использована для решения задач хранения и обмена информацией о транспортных средствах, их состоянии, пробеге, данных о техническом обслуживании и ремонте и т.п.

2. Технологии обработки больших данных являются неотъемлемой частью ИТС, поскольку они помогают обрабатывать и анализировать значительные массивы информации, собираемой датчиками, камерами, мобильными устройствами и другими инструментами мониторинга. С их помощью можно прогнозировать интенсивность потоков, собирать и анализировать информацию о транспортных средствах, выявлять факторы опасности, более точно определять необходимость ремонта покрытий и т.д.

3. Автономные транспортные средства. Не требуют соблюдения режима труда и отдыха, снижают влияние человеческого фактора, повышают безопасность и экономичность движения. Могут также использоваться в патрулировании и при оценке общего состояния ДД.

4. Технологии дополненной реальности. В контексте интеллектуализации транспортных систем являются инструментом отображения навигационной и иной актуальной информации на лобовом стекле автомобиля. Такой подход позволяет упростить процесс управления транспортным средством, снизить вероятность ошибок, повысить внимательность водителя к дорожной обстановке, предупреждающим знакам и сигналам.

5. Интернет вещей. Может быть использован для сбора и анализа информации. IoT-датчики могут собирать данные о транспорте, дорогах, погодных условиях, заторах и других факторах, которые могут влиять на движение транспорта, позволяя в дальнейшем использовать полученную информацию для автоматической регулировки транспортного потока и улучшения безопасности дорожного движения.

6. A-SMGCS (Advanced Surface Movement Guidance & Control System) – это система, обеспечивающая прокладку маршрута, наведение и наблюдение для управления воздушными судами (ВС) и транспортными средствами с целью поддержания заявленной скорости движения по поверхности при любых погодных условиях в пределах эксплуатационного уровня видимости аэродрома при сохранении требуемого уровня безопасности [2].

Также в аэродромной ИТС могут применяться и другие технологии. Все они в перспективе могут быть объединены в единую сеть с единым и главным органом управления в виде искусственного интеллекта, который будет в случае необходимости контролироваться человеком для оперативного и срочного вмешательства в случае сборной ситуации, но в остальное время работать самостоятельно.

Кратко опишем потенциальную технологию работы такой ИТС при обслуживании воздушного судна по принципу «прилёт-обслуживание-вылет».

Как только ВС коснулось взлётно-посадочной полосы, на ней срабатывают датчики, которые сообщают в головной центр о прибытии судна. Ему с помощью системы «Follow the greens» прокладывается маршрут до указанной в суточном плане полётов месте стоянки. Одновременно с этим сигнал поступает на автономную перронную станцию средств механизации с информацией о судне, его типе, требованиях авиакомпании, времени обслуживания и т.д. Затем запускается процесс движения необходимых машин и оборудования к данной стоянке. При этом все автомобили имеют автономный ход за счёт современных технологий беспилотного автомобиля. С помощью датчиков места положения, определения скорости и полезной нагрузки интеллектуальная система должна быть способна определить успеет то или иное транспортное средство прибыть к указанному месту или нет. Во втором случае должна передаваться команда на активацию других средств и перронной механизации, находящихся на более близком расстоянии, а тех, кто не успеет отправить на более близкие к ним стоянки. При прибытии воздушного судна на стоянку и расставлении всего необходимого оборудования и машин начинается процесс наземного обслуживания, производимого уже человеком. Обеспечение вылета самолёта осуществляется по такой же технологии, как и прилёт только в обратном направлении, со включением в работу беспилотных тягачей и систем, обеспечивающих безопасное расстояние при таком манёвре..

Это лишь одна модель самого популярного принципа обслуживания ВС, не описывающая сбойные и нестандартные ситуации.

Таким образом, выводя человека из большинства операций, проводимых на аэродроме и связанных с эксплуатацией спецтранспорта, можно повысить предсказуемость, безопасность и надёжность всех транспортных процессов на аэродроме. Однако полностью вывести человека из обслуживания воздушного судна нельзя, поскольку именно он является самым гибким звеном, способного реагировать на выходящие из-под контроля ситуации.

Список литературы

1. Егоров С.В., Шационик П.В., Ерпылева А.И., Жарков Д.И. Мировой и российский опыт применения интеллектуальных транспортных систем // Транспортное дело России. 2022. №2. С. 130 – 136.
2. Руководство по усовершенствованным системам управления наземным движением и контроля за ним (A-SMGCS) «Doc 9830». [Электронный ресурс] // aerohelp. – URL: https://aerohelp.ru/sysfiles/374_276.pdf
3. Сысоенко М. В., Лебедева А. С. Анализ применения технологий Индустрии 4.0 в интеллектуальных транспортных системах // Экономика. Право. Инновации. 2024. № 4. С. 30–39.
4. Тецлав И.А., Ярошенко Д.С. «Организация движения спецтранспорта и средств перронной механизации на аэродромах гражданской авиации Российской Федерации». Автомобильные перевозки и транспортная логистика: теория и практика. Сборник научных трудов кафедры «организация перевозок и управление на транспорте». ФГБОУ ВО «СибАДИ», Омск. – 2021

References

1. Egorov S.V., Shatsionok P.V., Erpyleva A.I., Zharkov D.I. World and Russian experience in the application of intelligent transport systems // Transport business of Russia. 2022. No. 2. pp. 130-136.
 2. Manual on Advanced Ground Traffic Control and Control Systems (A-SMGCS) "Doc 9830". [Electronic resource] // aerohelp. – URL: https://aerohelp.ru/sysfiles/374_276.pdf
 3. Sysoenko M. V., Lebedeva A. S. Analysis of the application of Industry 4.0 technologies in intelligent transport systems // Economy. Right. Innovation. 2024. No. 4. pp. 30-39.
 4. Tetslav I.A., Yaroshenko D.S. "Organization of movement of special vehicles and apron mechanization facilities at airfields of civil aviation of the Russian Federation". Road transport and transport logistics: theory and practice. Collection of scientific papers of the department "organization of transportation and management of transport". SibADI Federal State Budgetary Educational Institution, Omsk, 2021.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.8: 656.714

ВЕРОЯТНОСТНЫЙ И СТАТИСТИЧЕСКИЙ АНАЛИЗ АВИАЦИОННЫХ ПРОИСШЕСТВИЙ

¹ Некрасов Т.Д., ² Проскурин Л.Ю., Лозница С.Ю. (научный руководитель)

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА", Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail:

¹Kvakolka885@gmail.com, ²l3on.v.2.0@gmail.com

Цель этой статьи - изучить роль, которую инструменты вероятностного и статистического анализа, такие как модели ARIMA, могут сыграть в повышении безопасности полетов. Это должно быть достигнуто путем использования имеющихся данных об авариях, их вероятностной организации на основе различных задействованных переменных, позволяющей лучше понять их, а также путем анализа временных рядов для прогнозирования будущих значений и тенденций. Полученные результаты предоставляют ценную информацию, который может быть использован различными авиационными организациями для предотвращения авиационных происшествий.

Ключевые слова: Временной ряд, математическая модель, полетный цикл, авиационное происшествие, прогнозирование, вероятность, статистика.

PROBABILISTIC AND STATISTICAL ANALYSIS OF AVIATION ACCIDENTS

¹ Nekrasov T.D., ² Proskurin L.Yu., Loznitsa S.Yu. (supervisor)

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-mail: ¹Kvakolka885@gmail.com, ²l3on.v.2.0@gmail.com

The purpose of this article is to explore the role that probabilistic and statistical analysis tools such as ARIMA models can play in improving flight safety. This should be achieved by using the available accident data, their probabilistic organization based on the various variables involved, allowing for a better understanding of them, as well as by analyzing time series to predict future values and trends. The results provide valuable information that can be used by various aviation organizations to prevent accidents.

Keywords: Time series, mathematical model, flight cycle, aviation accident, forecasting, probability, statistics.

Введение:

Авиация представляет собой крупнейшую транспортную отрасль в мире, и, несмотря на огромные масштабы ее деятельности, с 4,5 миллиардами пассажиров, перевезенных по всему миру только в 2019 году за один из 884 тысяч выполненных рейсов [1], она из года в год сохраняет звание самого безопасного способа транспортировки в мире [2,3]. Такие показатели возможны только благодаря постоянным инвестициям и исследованиям в области улучшения безопасности. Одним из ее многочисленных аспектов является предотвращение аварий, в основном направленное на минимизацию потерь человеческих жизней путем предотвращения повторения событий, угрожающих безопасности [4]. Примером непрерывной работы по улучшению безопасности стало введение в 2013 году Международной организацией гражданской авиации (ИКАО) Приложения 19, в котором говорится, что каждая организация,

участвующая в авиационной отрасли, от утвержденных учебных организаций (АТО) до авиакомпаний, должна иметь Систему управления безопасностью (СУБ). Различные СУБ с соответствующими инструментами должны быть способны предпринимать проактивное поведение вместо реактивного, определяя стандарты безопасности организации, а также позволяя, при необходимости, своевременно вмешиваться в существующие правила или процедуры для повышения безопасности [5]. Авторы в [6] утверждают, что должны использоваться соответствующие инструменты, многие из которых включают анализ и обработку больших объемов данных, собранных во время операции, либо из отчетов, системы мониторинга или аудитов. Эта информация будет работать как основа для всего процесса безопасности, поскольку ее изучение и понимание позволят получить расширенные знания о возможных моделях, корреляциях, тенденциях и даже выполнять прогнозы. Это очень ценно, поскольку позволяет различным участникам отрасли использовать такие более глубокие знания для прогнозирования возможных сценариев и вмешиваться при необходимости, избегая ненужных аварий. Многие из этих инструментов используют математическую область вероятности и статистики для выполнения этих расчетов, являясь одним из тех расчетов для создания прогнозов, как краткосрочных, так и среднесрочных или долгосрочных. Прогнозы, когда они сделаны правильно, могут иметь первостепенное значение, обеспечивая поддержку во многих организациях стратегическим процессам принятия решений и планированию [7]. Некоторые из этих математических инструментов являются моделями, связанными с анализом данных временных рядов. Как подробно описано в [8], временной ряд представляет собой набор данных, записанных в течение определенного периода времени, и его анализ важен для того, чтобы иметь большое понимание любых корреляций, закономерностей или сезонности, обнаруженных в наборе изучаемых данных. Он также, в основном посредством применения вероятностной модели, сможет создавать прогнозы возможных значений и тенденций. В настоящее время существуют различные модели, связанные с временными рядами, исследованием, такими как линейная регрессия, экспоненциальное сглаживание, авторегрессионные или скользящие средние модели или сочетание обоих, включая модели ARIMA (интегрированная модель авторегрессии — скользящего среднего). В [9] описано, что использование моделей ARIMA довольно распространено в авиации, поскольку оно объединяет модели авторегрессии (AR) и скользящего среднего (MA), предоставляя обе их преимущества и снимая ограничение на использование только стационарных временных рядов. Используя интеграцию, модели ARIMA могут преобразовывать нестационарный временной ряд в стационарный. Как описано в [7], стационарный временной ряд — это ряд со свойствами, которые не меняются со временем, и поэтому существуют постоянное среднее и стандартное отклонение, не показывающее никаких тенденций или сезонности. Модели AR опираются на значения наблюдений, сделанных в течение периода (p), чтобы прогнозировать будущие значения; интегрированные (I) модели используют интеграцию временных рядов, чтобы преобразовать их в стационарные при необходимости, порядок интеграции равен (d); модели MA опираются на разницу (ошибку) между фактически наблюдаемыми значениями и прогнозируемыми значениями в течение прошлого периода (q). Модель ARIMA представлена как порядок (p,d,q), поэтому модель ARIMA (1,1,1) будет означать, что выход у связан с входом и выражением вида

$$(y_k + a_1 y_{k-1})(1 - z^{-1}) = u_k - b_1 u_{k-1}$$

где z^{-1} — оператор задержки, член $(1 - z^{-1})$ — интегрирование, a_1 и b_1 — параметры модели, y_k и u_k — вход и выход в заданный момент времени, а y_{k-1} и u_{k-1} — вход и выход в предыдущий момент времени.

В авиации модели, связанные с анализом временных рядов, такие как ARIMA, используются с двумя основными целями: есть коммерческая, управленческая сторона и другая сторона, связанная с безопасностью полетов. Модели могут использовать данные из авиации и все связанные переменные (фаза полета, тип самолета) для изучения и анализа событий, связанных с безопасностью полетов, таких как аварии или инциденты. С одной стороны, это позволяет лучше и глубже понять основные причины, которые привели к этим событиям, а с другой стороны, использовать те же самые данные для попытки создания прогнозов, что позволяет в обоих случаях пользователю иметь проактивный подход к безопасности, а не реактивный [10]. Тот факт, что модели ARIMA позволяют использовать нестационарные временные ряды, чрезвычайно полезен при анализе данных, связанных с авиационными происшествиями, во-первых, из-за случайности значений во времени, а также, как указано в [9], из-за конфиденциальности данных об авариях и отчетов, что может затруднить сбор огромных объемов информации, которые обычно требуются для анализа временных рядов. Именно здесь модели ARIMA имеют преимущество, поскольку они могут использовать комбинацию двух описанных моделей (AR, MA), таким образом, в некоторых случаях требуя меньше данных, чем если бы модели использовались по отдельности для генерации того же количества ценных прогнозов. В этой статье основное внимание уделяется использованию моделей ARIMA, связанных с анализом временных рядов, для составления будущих прогнозов в области предотвращения несчастных случаев и безопасности. Статья структурирована следующим образом. Раздел 2 посвящен анализу данных и моделированию, раздел 3 представляет исследование случая и результаты, а раздел 4 излагает выводы.

Анализ данных и моделирование.

База данных об авиакатастрофах Aviation Safety Network (ASN) [11] является источником, использованным для сбора информации, связанной с авариями за последние 7 десятилетий (1950-2020). Все данные были распределены по пяти категориям: 1) количество аварий в год; 2) наличие причин; 3) фаза полета (земля, взлет, набор высоты, маршрут, заход на посадку, посадка); 4) повреждение самолета (незначительное, существенное, не подлежащее ремонту, фатальное); 5) тип самолета (винтовой, реактивный). Набор данных был смоделирован в соответствии со стандартизированным форматом на протяжении всего исследования для каждого отдельного временного ряда: 1) Построить график каждого временного ряда и его тенденции, изучив его стационарность или необходимость дифференцировать ряд для получения стационарного результата; 2) Изучить функции автокорреляции (AC) и частичной автокорреляции (PAC), чтобы установить количество параметров модели ARIMA (p, q, d), необходимых для моделирования ряда; 3) Создать модели разных порядков и выбрать наиболее статистически значимые из них, используя набор критериев пригодности, которые оценивают производительность каждой модели по сравнению с другими, в частности статистическую значимость, чтобы решить, следует ли отбрасывать модель; 4) Построить график подгонки созданной модели к данным и соответствующий прогноз на следующие 5 лет (2021-2025 гг.); 5) Поскольку данные о несчастных случаях за 2021 год уже были доступны в базе данных, используемой в этом

исследовании, эти данные использовались для проверки прогноза по сравнению с зарегистрированными реальными значениями, вычисляя его погрешность (%); 6) Для того чтобы иметь возможность включить данные, полученные в этом исследовании, в авиационная промышленность и извлечение фактов и выводов, исторический ряд циклов полетов за предыдущие 50 лет (1970-2020) был собран из [12]. Затем эти данные использовались как собственный временной ряд и с использованием моделей ARIMA был спрогнозирован его возможный рост до 2025 года. Объединение как прогнозов циклов полетов, так и аварий за тот же период позволило создать соотношение аварий/миллион циклов полетов, которое позволяет получить представление об уровнях безопасности отрасли, независимо от ее поведения, такого как экспоненциальный рост или замедления, наблюдавшиеся в прошлом.

Исследование случая и результаты.

Исследование случая сосредоточено на европейском воздушном пространстве с намерением изучить и понять траекторию его уровней безопасности за последние десятилетия и, используя эту информацию вместе с областью вероятности и статистики, создать прогнозы возможных будущих значений и тенденций. Было понятно, что, сосредоточившись только на европейском воздушном пространстве, поскольку оно является наиболее регулируемым и одним из самых загруженных в мире, оно послужит хорошей моделью для остальных областей земного шара. Чтобы сосредоточиться только на европейском воздушном пространстве, рассматривались происшествия, произошедшие в государствах-членах европейских авиационных регулирующих агентств, таких как Объединенные авиационные власти (JAA) и Европейское агентство по безопасности полетов (EASA), или операторах других стран, сертифицированных для этого; таким образом, полеты выполняются в соответствии с европейскими авиационными правилами. Все собранные данные были обработаны и организованы в соответствии с различными переменными, рассматриваемыми для исследования, которые влияют на происшествие. Чтобы обеспечить прошлое понимание отрасли, была дополнительно собрана и использована историческая информация, связанная с завершенными полетными циклами. Область вероятностного и статистического анализа предложила инструменты, необходимые для подготовки, организации и подачи этих огромных объемов данных в различные модели ARIMA для создания прогнозов до 2025 года (таблица 1). Эти прогнозы помогли обогатить уже сделанное прошлое исследование будущим компонентом в отношении уровней безопасности, и, сравнивая прогнозы с реальными значениями, проверить полученные результаты. Чтобы объединить все результаты в метрику, которая позволила бы оценить показатели безопасности в графическом и удобном формате, было найдено соотношение данных об авариях/прогнозах с циклами полетов. Это позволило продемонстрировать прошлую траекторию к сегодняшним значениям и спроецировать их в будущее с учетом поведения отрасли (рост и замедление) на рассматриваемом временном горизонте.

Таблица 1 - Прогнозы временных рядов (2021-2025)

	2021	2022	2023	2024	2025
Всего происшествий	12	15	20	19	13
Авиакатастрофы	2	2	2	2	1
Посадка	8	7	7	7	7
Не подлежит ремонту	2	1	2	0	0
Реактивный самолёт	13	13	13	14	14
Полетные циклы	9 201 741	9 347 256	9 492 772	9 638 288	9 783 803

Общее количество происшествий:

С анализом временного ряда, показанного на рисунке 1, количество происшествий/год, хотя и с колебаниями между его минимальным значением 6 и максимальным значением 28 в течение последних десятилетий, оставалось относительно постоянным около своего среднего значения 19. Это показывает признаки стационарности в ряде. Более низкое значение в 6 происшествий было зарегистрировано в 2020 году, нетипичном году, отмеченном пандемией Covid-19, которая привела к снижению объема воздушного движения с его значения 2019 года 8,13 миллиона до приблизительно 2,99 миллиона в 2020 году, и это снижение также оправдывает более низкое количество зарегистрированных происшествий. Модель ARIMA (0,0,5) прогнозировала 12 происшествий в 2021 году, 15 в 2022 году, 20 в 2023 году, 19 в 2024 году и 13 в 2025 году (Таблица1).

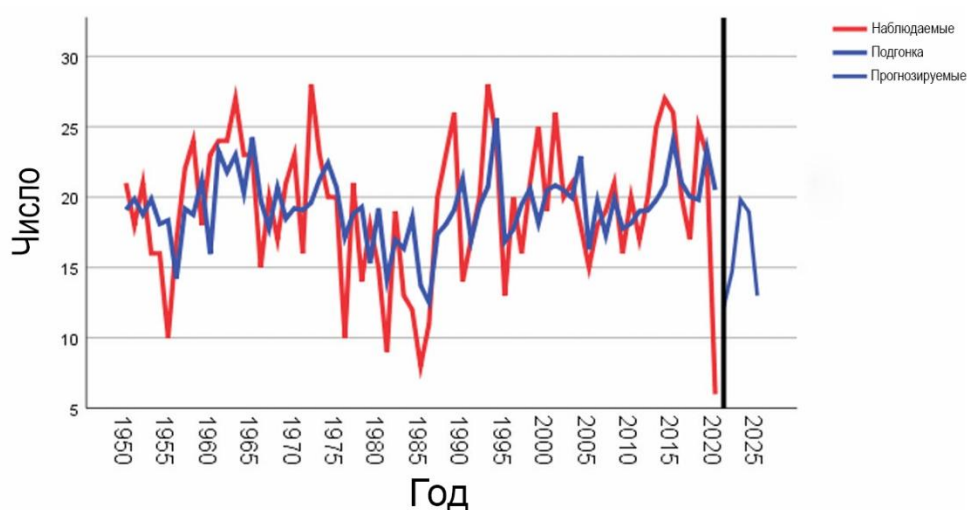


Рисунок 1 - Временной ряд общего количества наблюдаемых происшествий

Несчастные случаи со смертельным исходом:

Очевидно наличие тенденции к снижению в течение многих лет, оправданной развитием авиационной промышленности и, вместе с тем, уровнями безопасности за счет производства более безопасных и более совершенных и надежных самолетов, которые в то же время представляют меньший риск несчастных случаев, и в то же время несчастные случаи, которые происходят, приводят к меньшему количеству смертельных случаев, чем в прошлом [13]. Из-

за тенденции к снижению была применена дифференциация к ряду, чтобы превратить его в стационарный. Модель ARIMA (0,1,1) оказалась наиболее подходящей по своим критериям для временного ряда, и ее соответствие показано на рисунке 2. Временной ряд прогнозировал 2 несчастных случая со смертельным исходом в 2021, 2022, 2023, 2024 годах и одно несчастный случай в 2025 году (Таблица 1). Модель имеет ошибку 50% в прогнозе на 2021 год по сравнению с фактическим единственным происшествием со смертельным исходом.

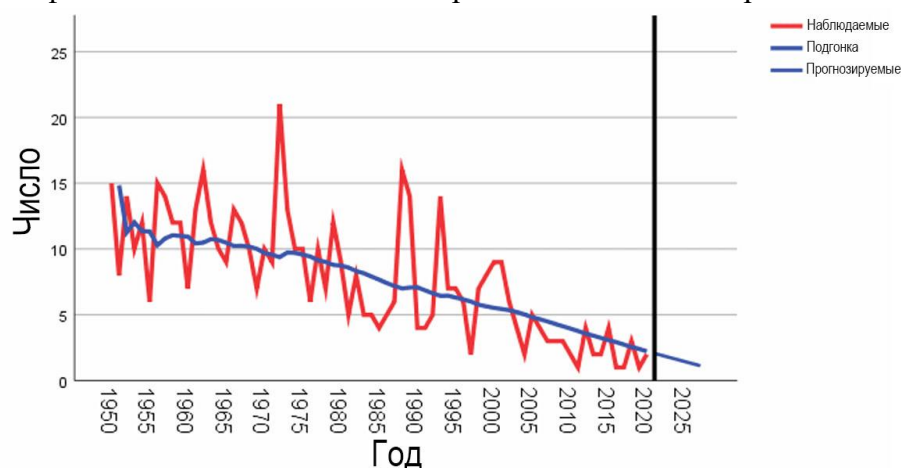


Рисунок 2 - Временной ряд происшествий с жертвами

Фаза полета:

Анализ летных происшествий является классическим методом, поскольку он позволяет разбить происшествия на разные фазы, каждая из которых имеет разный вес [14]. Этот факт был проверен в этом исследовании, поскольку большинство зарегистрированных происшествий произошло всего в три фазы, которые считаются наиболее критическими, хотя в то же время они составляют всего 6% продолжительности полета: взлет (включая начальный набор высоты), заход на посадку и посадка. Только на фазу посадки пришлось 33% всех происшествий в этом исследовании, поэтому она была выбрана для обсуждения. Анализ этого временного ряда показан на рисунке 3, выявляя положительную тенденцию, которая также предполагает необходимость ее трансформации. ARIMA (1,1,1) была выбрана на основе критериев пригодности. Ошибка модели в 60% в 2021 году между прогнозом в 8 аварий и реальным значением в 5. В 2022, 2023, 2024 и 2025 годах прогнозируемое количество аварий при посадке составляло 7 в год (Таблица 1).

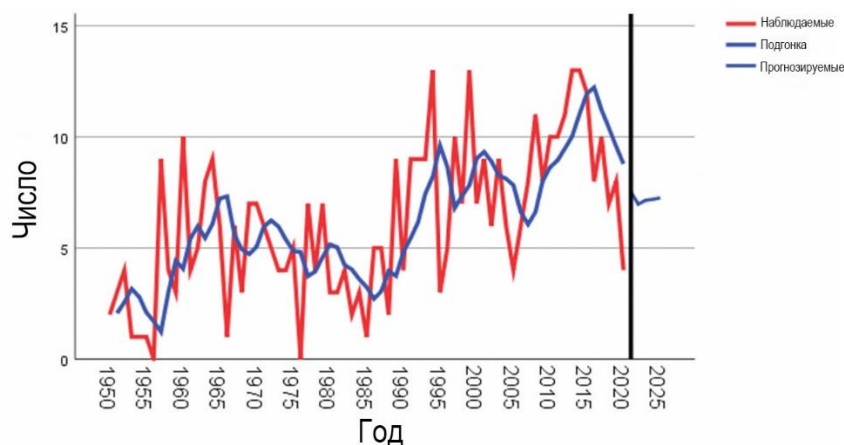


Рисунок 3 - Временной ряд посадок

Тип повреждения:

Что касается различных типов повреждений, полученных воздушными судами, особого внимания заслуживает временной ряд, не подлежащий ремонту. Этот факт обусловлен его противоположной тенденцией временного ряда, связанного со значительным ущербом, показанным на рисунке 4. Из-за наличия тенденции ряд был дифференцирован, и лучшей подгонкой оказалась модель $ARIMA(4,1,0)$. Прогнозируемые значения, проанализированные в таблице 1, следовали нисходящей тенденции данных и показывают точность 100% для 2021 года, соответствуя реальному факту двух зарегистрированных происшествий. В 2022 году модель прогнозировала 1 происшествие, 2 в 2023 году, и ни одного происшествия не прогнозировалось в 2024/2025 годах

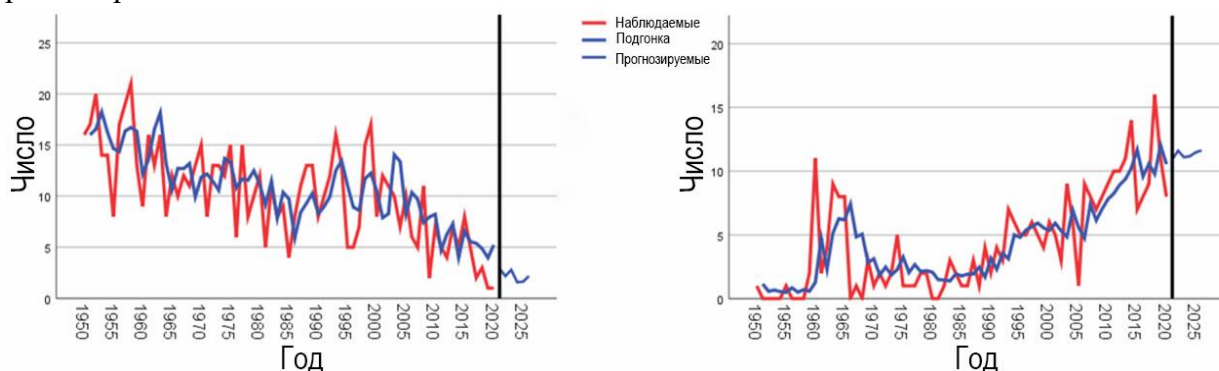


Рисунок 4 - Временной ряд повреждений, не подлежащих ремонту (Слева); Временной ряд существенный повреждений (Справа)

Тип самолета:

Анализ временных рядов реактивных и поршневых самолетов показан на Рисунке 5. Рисунок 5 показывает обратную связь, имеющую положительный (слева) и отрицательный тренд (справа), аналогично случаю типа повреждения (Рисунок 4). В случае (Рисунок 5) это может быть оправдано прогрессом в технологии в отрасли, ведущим к разработке и постепенной замене одной технологии движения поршневых двигателей на реактивные. Было обнаружено, что модель с лучшими характеристиками будет $ARIMA(1,1,1)$. Прогнозируемые значения в Таблице 1 оставались относительно постоянными на уровне 13 аварий в год с 2021 по 2023 год и 14 с 2024 по 2025 год. В 2021 году модель имеет ошибку примерно 85% по

сравнению с фактическими 7 событиями. Эту ошибку можно оправдать влиянием пандемии 2020 года на объем полетов в 2021 году, что привело к расхождению между прогнозируемыми и фактическими значениями.

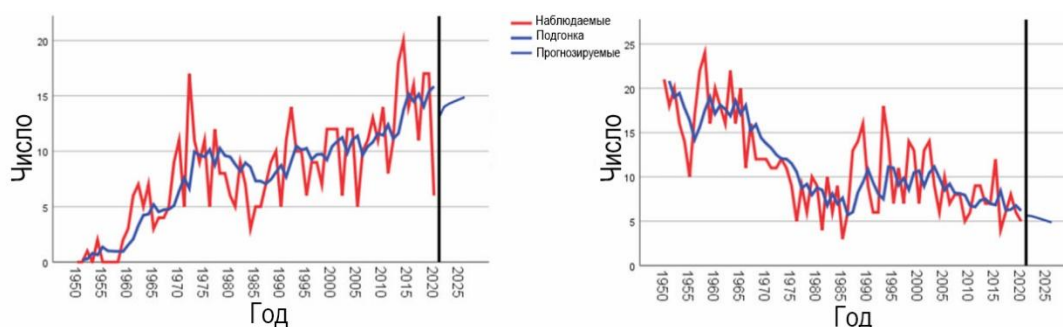


Рисунок 5 - Временной ряд реактивных самолетов (Слева); Временной ряд винтовых самолетов (Справа)

Перспективы отрасли:

Чтобы создать перспективу отрасли, обращенную в будущее, необходимо было получить данные для понимания общей траектории стандартов безопасности полетов в Европе за последние десятилетия в настоящее время. Анализ количества полетов за этот период показывает экспоненциальный рост с 1,8 млн циклов до 8,1 млн циклов с 1970 по 2018 год, что на 364% больше. Создание соотношения между авариями и циклами полета позволяет изучать уровни безопасности в течение этого периода времени с учетом различных моделей поведения в отрасли, а не только по абсолютному количеству аварий. Результатом соотношения между общим постоянным значением аварий, показанным на Рисунке 1, и растущей тенденцией в циклах полета из Рисунка 7 является отрицательная трендовая диаграмма (Рисунок 6), примерно с 13 аварий/миллион циклов полета в 1971 году по сравнению с 2 авариями в 2019 году. Эти цифры означают явное повышение уровня безопасности в Европе.



Рисунок 6 - Отношение происшествий к полетным циклам

Используя модели ARIMA, был создан новый временной ряд для прогнозирования возможного роста циклов полета на период 2021-2025 гг. Модель использовала ARIMA (1,1,1), и ее подгонка представлена на Рисунке 7, вместе с прогнозом 9 201 741 в 2021 г.; 9 347 256 в 2022 г.; 9 492 772 в 2023 г.; 9 638 288 в 2024 г. и 9 783 803 циклов полета в 2025 г. (Таблица¹).

Эти цифры отражают рост примерно на 6,33% или 582 млн циклов полетов. 2020 год был пропущен из-за искусственного влияния в прогнозе, что делает его нереалистичным по сравнению с фактическими данными о восстановлении и будущими оценками основных игроков отрасли [14].

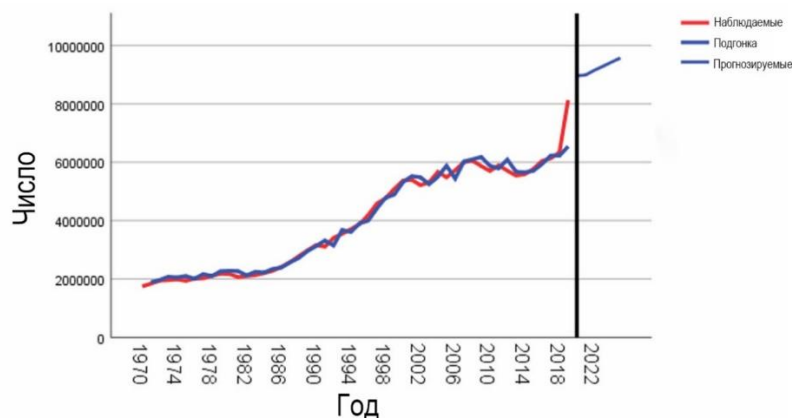


Рисунок 7 - Временной ряд наблюдаемых полетных циклов

Используя как прогноз аварий (Рисунок 2), так и прогнозируемые циклы полетов, показанные в Таблице 1, соотношение аварий на миллион циклов полетов было спрогнозировано, как показано на рисунке 8. Примечательно, что, хотя есть вариация в его значении (достигая максимального значения 2,11 аварий/миллион циклов полетов в 2023 году), оно в конечном итоге снижается, противоположно непрерывному росту циклов в год, что позволяет извлечь из рисунка 8 положительную корреляцию между ростом отрасли и уровнями безопасности. Эта положительная корреляция идентична той, что была получена при изучении прошлых и фактических уровней безопасности.

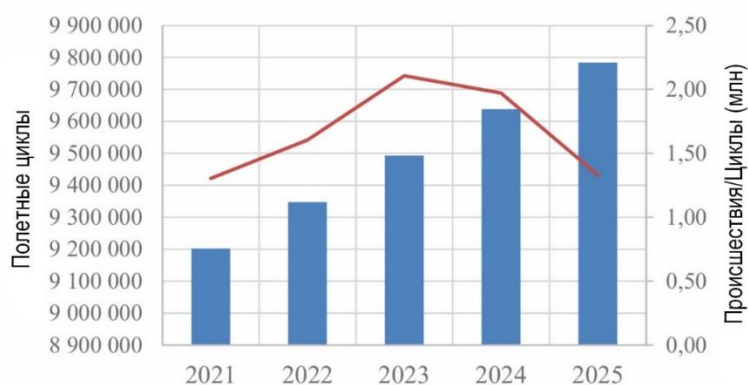


Рисунок 8 - Полетные циклы и отношение происшествий к полетным циклам

Заключение

Учитывая результаты, полученные в этом исследовании, важность используемых статистических инструментов становится ясной в авиации, особенно в области безопасности, поскольку они будут поддерживать классический подход (через расследование и анализ событий), представляя статистические данные, которые помогут прояснить и диагностировать определенные события. С другой стороны, инструменты такого рода позволяют разработать более проактивный подход к безопасности полетов, как описано в [15], посредством

всестороннего понимания различных задействованных переменных и их веса в возникновении аварий и инцидентов, помогая операторам отрасли Безопасность Система управления для выявления ключевых зон эксплуатационного риска и направления их усилий и внимания на них, что приводит к повышению уровня безопасности. Применение моделей ARIMA, связанных с анализом временных рядов, показало, что это может быть одним из инструментов, который может способствовать наряду со многими другими повышению безопасности полетов, хотя в то же время он может содержать некоторые ошибки в расчетах в своих значениях и прогнозах. Случайность данных, связанных с авиационными происшествиями, обусловлена их природой, поскольку объем воздушного движения и последующие происшествия, которые могут произойти, зависят от множества внешних факторов, которые невозможно учесть, таких как погода, геополитический кризис или последствия глобального кризиса здравоохранения, поставившего авиационную отрасль на колени.

Список литературы

1. ИКАО 2019 Мир воздушного транспорта в 2019 году (<https://www.icao.int/annual-report-2019/Pages/default.aspx>).
2. Сантос LFFM и Мелисио Р. 2019 Международный обзор аэрокосмической техники 12(1) С.35-45.
3. Мадейра Т., Мелисио Р., Валерио Д. и Сантос LFFM 2021 Аэрокосмическая техника 8(2) 47 С.1-18.
4. ИКАО 2015 Руководство по расследованию авиационных происшествий и инцидентов (<https://www.skybrary.aero/sites/default/files/bookshelf/3282.pdf>).
5. Европейское агентство по безопасности полетов 2021. Приемлемый уровень показателей безопасности (AloSP) (https://www.easa.europa.eu/sites/default/files/dfu/2021-05-31_alosp_for_publication.pdf).
6. Гослинг Г., Мьюир А., Хант К., Шнееманн Г. и Шпейер Дж.-Дж. 2003 Руководство по методам и инструментам для анализа безопасности полетов авиакомпаний (<https://skybrary.aero/sites/default/files/bookshelf/237.pdf>).
7. Монтгомери Д.К., Шерил Дж. и Мурат К. 2008 Прогнозирование и анализ временных рядов. Нью-Йорк: Wiley.
8. Brockwell PJ и Davis RA 2016 Введение во временные ряды и прогнозирование Швейцария: Springer.
9. Lališ A 2017 Проблемы транспорта 12(3) С. 51-58.
10. Zieja M, Smoliński H и Gołda P 2015 Журнал Konbin 36 (1)С. 105-114.
11. Ranter Н 2022 Сеть безопасности полетов (<https://aviationsafety.net/database/databases.php>).
12. Всемирный банк 2022 Воздушный транспорт, зарегистрированные вылеты перевозчиков по всему миру (<https://data.worldbank.org/indicator/IS.AIR.DPRT>).
13. Airbus 2022 Статистический анализ коммерческих авиационных происшествий 1958-2021 (<https://accidentstats.airbus.com/sites/default/files/2022-02/Statistical-Analysis-ofCommercial-Aviation-Accidents-1958-2021.pdf>).
14. Aalmoes R, Erkamp R, Cheung YS и van Nieuwpoort R 2013 WIT Transactions on The Built Environment 134(12) С.447-458.

15. Обновление прогноза EUROCONTROL 2021 на 2021–2027 годы, европейские авиаперевозки и службы, три сценария восстановления после COVID-19 (<https://www.eurocontrol.int/sites/default/files/2021-10/eurocontrol-7-year-forecast-2021-2027.pdf>).

References

1. ICAO 2019 Air Transport World 2019 (<https://www.icao.int/annual-report-2019/Pages/default.aspx>).
 2. Santos LFFM and Melisio R. 2019 International Review of Aerospace Engineering 12(1) pp.35-45.
 3. Madeira T., Melício R., Valerio D. & Santos LFFM 2021 Aerospace Engineering 8(2) 47 pp.1-18.
 4. ICAO 2015 Accident and Incident Investigation Manual (<https://www.skybrary.aero/sites/default/files/bookshelf/3282.pdf>).
 5. European Aviation Safety Agency 2021. Acceptable Safety Performance Level (AloSP) (https://www.easa.europa.eu/sites/default/files/dfu/2021-05-31_alosp_for_publication.pdf).
 6. Gosling, G., Muir, A., Hunt, K., Schneemann, G., and Speyer, J.-J. 2003 Manual on Methods and Tools for Airline Safety Analysis (<https://skybrary.aero/sites/default/files/bookshelf/237.pdf>).
 7. Montgomery D.K., Cheryl J. and Murat K. 2008 Time Series Forecasting and Analysis. New York: Wiley.
 8. Brockwell PJ and Davis RA 2016 Introduction to Time Series and Forecasting Switzerland: Springer.
 9. Lališ A 2017 Problems of Transport 12(3) pp. 51-58.
 10. Zieja M, Smoliński H and Gołda P 2015 Magazine Konbin 36 (1)P. 105-114.
 11. Ranter H 2022 Safety Network (<https://aviationsafety.net/database/databases.php>).
 12. World Bank 2022 Air Transport, Carriers' Registered Departures Worldwide (<https://data.worldbank.org/indicator/IS.AIR.DPRT>).
 13. Airbus 2022 Statistical Analysis of Commercial Aviation Accidents 1958-2021 (<https://accidentstats.airbus.com/sites/default/files/2022-02/Statistical-Analysis-ofCommercial-Aviation-Accidents-1958-2021.pdf>).
 14. Aalmoes R, Erkamp R, Cheung YS and van Nieuwpoort R 2013 WIT Transactions on The Built Environment 134(12) pp. 447-458.
 15. EUROCONTROL 2021 Forecast 2021-2027 Update, European Air Travel and Services, Three COVID-19 Recovery Scenarios (<https://www.eurocontrol.int/sites/default/files/2021-10/eurocontrol-7-year-forecast-2021-2027.pdf>).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 62

АНАЛИЗ КОНЦЕПЦИЙ ЭНЕРГОСНАБЖЕНИЯ МОРСКИХ НЕФТЕГАЗОВЫХ ОБЪЕКТОВ НА АРКТИЧЕСКОМ ШЕЛЬФЕ

Жигалов А.А.

ФГАОУ ВО "СЕВЕРНЫЙ (АРКТИЧЕСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА", Архангельск, Россия (163002, Архангельская область, город Архангельск, наб. Северной Двины, д.17), e-mail: dioic@yandex.ru

В настоящей статье мы рассматриваем различные концепции энергоснабжения, как традиционные, так и перспективные. К первым можно отнести дизель-генераторы и газотурбогенераторы, а ко вторым – солнечные, ветряные, гидроэлектростанции, автономные ядерные реакторы, энергоснабжение с берега. Показаны положительные и отрицательные стороны различных вариантов обеспечения электроэнергией, а также возможные варианты их комбинирования.

Ключевые слова: Арктический шельф, энергоснабжение, нефтегаз, МНГС, ПДК.

ANALYZING CONCEPTS OF POWER SUPPLY FOR OFFSHORE OIL AND GAS FACILITIES ON THE ARCTIC SHELF

Zhigalov A.A.

LOMONOSOV NORTHERN (ARCTIC) FEDERAL UNIVERSITY, Arkhangelsk, Russia (163002, Arkhangelsk region, Arkhangelsk city, Severnaya Dvina embankment, 17), e-mail: dioic@yandex.ru

In this paper we review different concepts of energy supply, both traditional, and promising ones. To the former we can refer diesel generators and gas turbine generators, and the latter include solar, wind, hydroelectric, and autonomous nuclear reactors, power supply from the shore. The positive and negative aspects of different options of power supply, as well as possible variants of their combination.

Keywords: Arctic shelf, power supply, oil and gas, MOGS, SPU.

Одним из ключевых вопросов обеспечения электроэнергии на шельфе является потребная энергия для извлечения сырья. По данным [1] в зависимости от объекта нефтегазового промысла потребная мощность генерации электроэнергии должна составлять: на собственные нужды – 5...10 МВт, на извлечение скважинной продукции – 30...40 МВт, на компримирование газа – 250...300 МВт, на сжижение газа – 300...600 МВт.

Мы можем обозначить два основных подхода к решению данной проблемы. Первый – получение энергии по месту добычи, второй – ее передача с берега. Среди первых мы можем в свою очередь выделить традиционные и перспективные методы.

Наиболее традиционным источником энергии для процессов является установка силового блока на МНГС, в частности использование *дизель-генераторов (ДГ)* и *двухтопливных газовых турбин (ГТГ)*. Примером реализации такого подхода в отечественной практике является МЛСП «Приразломная» энергетический комплекс которой состоит из трех двухтопливных газотурбогенераторов номинальной мощностью 28,932 МВт. Годовой расход топливного газа (основное топливо) составляет 24 768,3 тыс. м³/год, годовой

расход дизельного топлива (вспомогательное топливо) для каждой установки – 1 140,8 т/год. Согласно информации, представленной в [2] одновременно в работе используется два ГТГ, один находится в резерве. Таким образом можно заключить, что мощности около 58 МВт достаточно для обеспечения эксплуатации МЛСП. Кроме того, энергетический комплекс платформы включает четыре аварийных дизель-генератора (ВДГ) номинальной мощностью 880 кВт, предназначенные для обеспечения нужд бурового комплекса при отсутствии энергоснабжения от ГТГ, расход ДТ составляет 19 т/год. Аварийный дизель-генератор (АДГ) номинальной мощностью 1500 кВт используется для аварийного питания, расход – 22 т/год. При сгорании топливного газа в газотурбогенераторах в атмосферу выделяются загрязняющие вещества: азота диоксид (азот (IV) оксид), азот (II) оксид (азота оксид), углерод оксид, сера диоксид, метан, бенз(а)пирен. При сгорании дизельного топлива в газотурбогенераторах в атмосферу выделяются азота диоксид (азот (IV) оксид), азот (II) оксид (азота оксид), углерод оксид, сера диоксид, углерод (сажа), бенз(а)пирен.

В зарубежной практике добычи на арктическом шельфе данный метод энергоснабжения с одной стороны до сих пор применяется, например, на месторождении Слейпнир, с другой – норвежские добычные комплексы активно переходят на береговое энергоснабжение [3]. Основными минусами использования дизель- и газотурбогенераторов являются габариты силовых установок и систем обеспечения их эксплуатации, низкая эффективность [4], а также высокое потребление топлива, что кроме непосредственных затрат на его приобретение отражается в несоответствии их современным нормам экологичности из-за высокого содержания соединений азота, серы, углекислого газа и других вредных веществ в их выхлопных газах, что в условиях зарубежных месторождений, в особенности, норвежских ведет в том числе к значительным налоговым издержкам [5]. Кроме того, к силовому оборудованию в условиях Арктики предъявляются повышение требования по стойкости к экстремально низким температурам, а также общим условиям шельфа – вода, соленость, ветер. Нельзя также не отметить, что газотурбогенераторам необходимо более частое обслуживание, чем дизель-генераторам и их стоимость выше стоимости последних [6]. Основными направлениями развития данного способа энергоснабжения МНГС является повышение эффективности использования производимой энергии, к примеру, за счет оптимизации планирования проведения буровых операций, а также совершенствование системы управления энергоснабжением [7]. Это приведет к меньшему расходу топлива и, соответственно, приведет к уменьшению выброса в атмосферу вредных веществ.

Исходя из рассмотренных положительных сторон и недостатков так называемых традиционных методов энергоснабжения МНГС, в рамках данного подхода более интересным и перспективным представляется использование альтернативных источников энергии: ветра, прилива, солнца. В последние годы главным трендом развития энергетики стало значительное повышение доли *возобновляемых источников энергии* (ВИЭ) на мировом рынке. В 2019 году электростанции, работающие на ВИЭ, впервые обогнали по объему производства энергии атомные электростанции [8]. Один только Китай, являющийся лидером в данном секторе, за последних четыре года вложил 343 млрд. евро в развитие альтернативной энергетики, США ежегодно инвестирует около 35 млрд. евро, третье место занимает Япония, тратящая от 8 до 12 млрд. евро в год. Касательно европейских стран, доля возобновляемых источников энергии в Швеции составляет 55%, в Финляндии – 41%, в Дании — 36%, в Германии – 43,7%. Наша

страна в развитие альтернативной энергетики планировала вложить 110 млрд. рублей [9] до 2024 года. Рассмотрим несколько подробнее, что из себя представляют эти источники энергии.

В условиях шельфа Арктики наиболее перспективным является применение **ветряных электростанций** (ВЭС). Среднегодовая скорость ветра по результатам имеющихся наблюдений в разных участках Баренцева моря составляет от 5,2 до 8,0 м/с [ссылка]. В работе [11] показано, что параллельная работа газотурбины и ветряной электростанции, расположенной рядом с нефтегазовой платформой приводит к значительному снижению расхода топлива и вредных выбросов и позволяет экономить порядка 5,73 евро в год. Данное исследование показало, что доля энергии ветра составила около 43 % от общего потребления при конфигурации 4 x 5 МВт. Нельзя не отметить, что в рассматриваемом кейсе средняя скорость ветра составляла 11...13 м/с, что в среднем гораздо выше, чем средние скорости ветра на арктическом шельфе России [12]

Гидроэлектростанции (ГЭС) сходны с ветряными в принципе работы, только в первом случае рабочим телом является вода, а во втором – воздух. ГЭС, тем не менее имеют больший потенциал для производства электроэнергии ввиду большей плотности воды по сравнению с воздухом, поэтому они могут производить сравнимый объем электроэнергии при скорости рабочего тела в разы меньше, чем у ветряка [13]. По данным исследований [14] скоростей приливных течений в Баренцевом море, которое принадлежит к морям приливного типа, может достигать 1,7 м/с, что может быть достаточно для выработки около 1,7 кВт электроэнергии [15].

Среди зарубежных гидроэлектростанций можно выделить осевую турбину AR-1000 мощностью 1 МВт при скорости потока 2,65 м/с, разработанную для эксплуатации в океанических условиях, турбину HS300, расположенную в зоне поселения Kvalsund в Норвегии мощностью 0,3 МВт со скоростью 7 об/мин, турбина SeaGen, мощностью 1.2 МВт расположенная в Северной Ирландии. Кроме технологий осевых турбин существуют также радиальные, комбинированные, импульсные устройства, а также так называемые турбины качения.

Среди отечественных разработок стоит отметить проект Г.Ш. Мамулашвили под названием «Гидрореактор», получивший положительное решение экспертного совета Сколково в 2018 г. [16]. Продукт представляет собой подводные проточные турбогенераторы мощностью 5...450 кВт для работы в придонных течениях с использованием эффекта Вентури. Автор утверждает [17], что стоимость вырабатываемой ГЭС энергии в 4 раза дешевле по сравнению с ГТГ и в 2 раза по сравнению с ДГ. К сожалению, актуальных данных о ходе реализации проекта найти не удалось.

К безусловным плюсам данной технологии можно отнести ее экологичность и отсутствие затрат на топливо. С другой стороны, на данном этапе развития технология разработана скорее для эксплуатации в местах с высокой скоростью течений (проливы, реки), чем для нужд шельфа, к тому же нельзя не учитывать возможное влияние обледенения в реальных Арктики на возможность эксплуатации гидроэлектростанций.

Применение фотоэлектрических панелей (ФЭП) в составе **солнечной электростанции** (СЭС) в качестве дополнительного источника энергии для МНГС на арктическом шельфе является вполне реализуемым, к тому же условия низких температур являются более благоприятными для солнечных панелей, чем более высоких, так при 0°C эффективность ФЭП увеличивается на 10% по сравнению с +20°C, к тому же недостатка в солнечных днях в летний период тоже не наблюдается, уровень инсоляции зоны Арктики колеблется от 3 до 4,5

кВтч/м²/сутки с возрастанием с запада на восток [18]. Несмотря на то, что конкретных исследований для рассматриваемого региона найти удалось, релевантные работы по другим климатическим зонам демонстрируют, что использование солнечных панелей для запитывания прачечных в течение 20 лет (средний срок службы панели) ведет к экономии 38,8 % затрат в долларовом выражении [19]. К преимуществам ФЭП относят простоту в обслуживании, расширении, усовершенствовании системы за счет простоты конструкции. Основным недостатком считается зависимость от погожих дней, что частично решается наличием аккумуляторов для запаса энергии, достаточно большая площадь, которая требуется для размещения панелей, а также необходимость размещения ФЭП на достаточной высоте над поверхностью воды, т.к. брызги могут уменьшить эффективность работы устройств.

По мнению ряда экспертов [20], в реалиях нашей страны наибольший потенциал в обеспечении энергией на арктическом шельфе имеет **атомная энергетика**. Данный тезис обуславливается прежде всего наличием продолжительных по времени ледовых режимов во многих морях акватории Северного ледовитого океана, что препятствует размещению плавучих электростанций; удаленностью месторождений от берега и отсутствие наземной инфраструктуры для энергоснабжения по подводным проводам, а опасность разлива жидкого топлива и выброс в атмосферу остатков его сжигания в условиях Арктики может привести к катастрофическим последствиям для экологии [21]. Отмечается также экономическая выгода при использовании данного источника энергии: исследования [22] показали, что потребная мощность обеспечения нужд Штокмановского месторождения составляет 600 МВт и эти нужды перекрывают две АС на базе реакторов типа ВБЭР-300 разработки ОКБМ «Африкантов» и их использование было бы дешевле газовых турбин соответствующей выходной мощности. Также можно рассмотреть энергоблок с реакторной установкой «Шельф-10» подводного исполнения с глубиной установки до 300 м, мощностью 9 МВт и временем автономной работы 5000 ч разработки АО «НИКИЭТ» [23]. К минусам технологии на наш взгляд можно отнести разве что отсутствие значительной практики использования таких устройств в рассматриваемом контексте.

В настоящее время за рубежом преобладает **передача электроэнергии с берега по подводному кабелю**. В Норвегии активно разрабатываются и реализуются проекты по замене энергоснабжения с газотурбин на береговое мощностью 250...300 МВт [24], в 2018 году был выполнен переход на береговое питание месторождения Sverdrup, которое в свою очередь поставит питание по кабелю на месторождения Ivar Aasen, Edvard Grieg и Gina Krog, от последнего же к концу 2022 года планируется так же подключить месторождение Sleipner к частичному энергоснабжению от береговой сети [25]. Несмотря на то, что береговое энергоснабжение обходится дешевле, чем получение энергии на месторождении, это верно лишь для кластера месторождений расположенных относительно недалеко от берега при условии наличия развитой инфраструктуры.

Разумеется, оптимальным вариантом энергоснабжения является сочетание различных форм энергоснабжения с применением как традиционных источников энергии, так и возобновляемых. К примеру, для эксплуатации в условиях Арктики предлагается комбинированная схема генерации электроэнергии на основе СЭС (8 МВт), ВЭС (4,5 МВт) и ДГ (15 МВт) [26]

В данной статье мы рассмотрели различные варианты электроснабжения шельфовых месторождений, условное разделив их на традиционные (дизель-генераторы и

газотурбогенераторы) и перспективные (солнечные, ветряные, гидро- электростанции, автономные ядерные реакторы, энергоснабжение с берега). В условиях Арктики особый интерес, на наш взгляд, представляет использование энергоблоков на основе ядерных установок, из несомненных их преимуществ стоит выделить экологичность, возможность размещения на донной поверхности, автономность, низкое потребление топлива, высокий уровень развития ядерных технологий в стране. Отрицательными сторонами является отсутствие в настоящий момент опробованной конструкции энергоблока подходящей для выполнения рассматриваемых задач, а также, по нашим данным, невысокий уровень инвестиций, как со стороны государства, так и нефтегазовых компаний в развитие данного направления. Кроме того, интерес представляет использование возобновляемых источников энергии в сочетании с традиционными, например, дизель-генераторы плюс солнечные батареи и/или ветряки, это снижает потребность в топливе и уменьшает выбросы и, соответственно, негативное воздействие на экологию региона.

Список литературы

1. Конкурентоспособность нефтегазовых проектов арктического шельфа в условиях низких цен на энергоресурсы [Электронный ресурс]: Статья / Мастепанов А.М. // Журнал «Neftegaz.ru». – 2017. - №1. – с. 20-32.
2. Техническое перевооружение МЛСП «Приразломная». Этап 2.2. Документация на техническое перевооружение. Пояснительная записка [Электронный ресурс]. URL: https://adm-nmar.ru/upload/iblock/c4a/PNM_LP_TP2.2_MNGP_100_20D_DTP.PZ_izm1.pdf (дата обращения: 23.05.24).
3. More than half of Norway's offshore fields heading for electrification [Электронный ресурс]. URL: <https://www.offshore-mag.com/production/article/14178665/more-than-half-of-norways-offshore-oil-and-gas-fields-heading-for-electrification> (дата обращения: 23.05.24).
4. Powering platforms Connecting oil and gas platforms to mainland power grids [Электронный ресурс]. URL: <https://www.hitachienergy.com/content/dam/web/products-services/products-systems/hvdc/media/old-images/Powering%20platforms.pdf> (дата обращения: 23.05.24).
5. Экологические налоги на примере Норвегии [Электронный ресурс]. URL: <https://findpatent.ru/magazine/024/247802.html> (дата обращения: 23.05.24).
6. Power Management Options For Offshore Oil & Gas Rigs [Электронный ресурс]. URL: <https://www.wpowerproducts.com/news/how-to-power-offshore-oil-rigs/> (дата обращения: 23.05.24).
7. Offshore Drilling Rigs [Электронный ресурс]. URL: <https://www.ipieca.org/resources/energy-efficiency-solutions/units-and-plants-practices/offshore-drilling-rigs/> (дата обращения: 23.05.24).
8. Альтернативная энергетика в Арктике [Электронный ресурс]. URL: <https://www.ipieca.org/resources/energy-efficiency-solutions/units-and-plants-practices/offshore-drilling-rigs/> (дата обращения: 23.05.24).
9. A Case-Study on Offshore Wind Power Supply to Oil and Gas Rigs [Электронный ресурс]. URL: <https://www.sciencedirect.com/science/article/pii/S1876610212011228> (дата обращения: 23.05.24).

10. Сезонное распределение значений скорости ветра в Арктике [Электронный ресурс] URL: <https://scienceforum.ru/2021/article/2018024205> (дата обращения: 23.05.23).
11. Surfing Energy's New Wave [Электронный ресурс] URL: <https://web.archive.org/web/20110120194729/http://www.time.com/time/magazine/article/0,9171,457348,00.html> (дата обращения: 23.06.24).
12. Влияние морского льда на приливные колебания уровня моря и скорости течений в Баренцевом и Белом морях [Электронный ресурс]. URL: <http://method.meteorf.ru/publ/tr/tr370/tr370htm/10.htm> (дата обращения: 23.05.24).
13. Атомная энергетика для арктического шельфа [Электронный ресурс] URL: <https://scientificrussia.ru/articles/atomnaya-energetika-dlya-arkticheskogo-shelfa> (дата обращения: 23.12.21).
14. Применение ВИЭ на морских нефтедобывающих платформах [Электронный ресурс]. URL: http://zyt.abok.ru/articles/610/Primenenie_VIE_na_morskih_neftedobivayuchshih_platformah (дата обращения: 23.05.24).
15. Мамулашвили Георгий Шотаевич [Электронный ресурс]. URL: <https://www.famous-scientists.ru/14939/> (дата обращения: 23.05.24).
16. Мамулашвили Г.Ш. Морская энергетика может решить проблемы электроснабжения нефтегазодобывающих платформ ... [Электронный ресурс] / Описание технологии. URL: <https://old.sk.ru/foundation/energy/f/383/t/11040.aspx> (дата обращения: 23.05.24).
17. Перспективы ВИЭ в Арктике [Электронный ресурс]. URL: <https://magazine.neftegaz.ru/articles/arktika/624988-perspektivy-vie-v-arktike/> (дата обращения: 23.05.24).
18. Solar Power for Sustainable Offshore Petroleum Exploration and Production in Africa. URL: https://www.researchgate.net/publication/312085159_Solar_Power_for_Sustainable_Offshore_Petroleum_Exploration_and_Production_in_Africa (дата обращения: 23.05.24).
19. А.Я. Резниченко «Ядерные технологии в освоении Арктики» // «Арктические ведомости. Информационно-аналитический журнал», №2, 2014, стр. 80.
20. Атомная энергетика для арктического шельфа [Электронный ресурс]. URL: <https://scientificrussia.ru/articles/atomnaya-energetika-dlya-arkticheskogo-shelfa> (дата обращения: 23.05.24).
21. В.П. Кузнецов, В.В. Куштан, Д.А. Мирзоев «Арктический вызов мирного атома. Обзор российских проектов нефтегазовых технологий с атомным энергообеспечением для освоения Арктического шельфа»; журнал Объединенной Судостроительной Корпорации, №3(20), 2014 г.
22. Timeline for electrification of the Utsira High [Электронный ресурс]. URL: <https://www.equinor.com/news/archive/2012/11/01/01NovUtsirahoyden> (дата обращения: 23.05.24).
23. Maximum utilization of power from shore to Utsira High helps further reduce emissions [Электронный ресурс]. URL: <https://www.equinor.com/news/archive/2019-10-28-power-utsira-high> (дата обращения: 23.05.24).
24. Альтернативная энергетика для повышения эффективности разработки нефтегазовых месторождений [Электронный ресурс]. URL: <https://magazine.neftegaz.ru/articles/arktika/639046-alternativnaya-energetika-dlya->

povysheniya-effektivnosti-razrabotki-neftegazovykh-mestorozhdeniy-/ (дата обращения: 23.05.24).

25. Ресурсы арктического шельфа – это наш стратегический запас [Электронный ресурс]. URL: <https://energypolicy.ru/resursy-arkticheskogo-shelfa-eto-nash/business/2019/22/14/> (дата обращения: 23.05.24).

References

1. Competitiveness of oil and gas projects of the Arctic shelf in conditions of low energy prices [Electronic resource]: Article / Mastepanov A.M. // Journal "Neftegaz.ru". – 2017. - №1. – pp. 20-32.
2. Technical re-equipment of MLSP "Prirazlomnaya". Stage 2.2. Documentation for technical re-equipment. Explanatory note [Electronic resource]. URL: https://adm-nmar.ru/upload/iblock/c4a/PNM_LP_TP2.2_MNGP_100_20D_DTP.PZ_izm1.pdf (date of request: 05/23/24).
3. More than half of Norway's offshore fields heading for electrification [Electronic resource]. URL: <https://www.offshore-mag.com/production/article/14178665/more-than-half-of-norways-offshore-oil-and-gas-fields-heading-for-electrification> (accessed: 05/23/24).
4. Powering platforms Connecting oil and gas platforms to mainland power grids [Electronic resource]. URL: <https://www.hitachienergy.com/content/dam/web/products-services/products-systems/hvdc/media/old-images/Powering%20platforms.pdf> (date of request: 05/23/24).
5. Environmental taxes on the example of Norway [Electronic resource]. URL: <https://findpatent.ru/magazine/024/247802.html> (date of request: 05/23/24).
6. Power Management Options For Offshore Oil & Gas Rigs [Electronic resource]. URL: <https://www.wpowerproducts.com/news/how-to-power-offshore-oil-rigs/> (date of access: 05/23/24).
7. Offshore Drilling Rigs [Electronic resource]. URL: <https://www.ipieca.org/resources/energy-efficiency-solutions/units-and-plants-practices/offshore-drilling-rigs/> (date of request: 05/23/24).
8. Alternative energy in the Arctic [Electronic resource]. URL: <https://www.ipieca.org/resources/energy-efficiency-solutions/units-and-plants-practices/offshore-drilling-rigs/> (date of access: 05/23/24).
9. A Case-Study on Offshore Wind Power Supply to Oil and Gas Rigs [Electronic resource]. URL: <https://www.sciencedirect.com/science/article/pii/S1876610212011228> (date of access: 05/23/24).
10. Seasonal distribution of wind speed values in the Arctic [Electronic resource] URL: <https://scienceforum.ru/2021/article/2018024205> (date of request: 05/23/23).
11. Surfing Energy's New Wave [Electronic resource] URL: <https://web.archive.org/web/20110120194729/http://www.time.com/time/magazine/article/0,9171,457348,00.html> (accessed: 06/23/24).
12. The influence of sea ice on tidal fluctuations in sea level and current velocity in the Barents and White Seas [Electronic resource]. URL: <http://method.meteorf.ru/publ/tr/tr370/tr370htm/10.htm> (date of access: 05/23/24).

13. Nuclear power engineering for the Arctic shelf [Electronic resource] URL: <https://scientificrussia.ru/articles/atomnaya-energetika-dlya-arkticheskogo-shelfa> (date of request: December 23, 21).
 14. The use of renewable energy sources on offshore oil production platforms [Electronic resource]. URL: http://zvt.abok.ru/articles/610/Primenenie_VIE_na_morskih-neftedobivayuchshih-platformah (date of reference: 05/23/24).
 15. Mamulashvili Georgiy Shotaevich [Electronic resource]. URL: <https://www.famous-scientists.ru/14939/> (date of access: 05/23/24).
 16. Mamulashvili G.S. Marine energy can solve the problems of power supply to oil and gas production platforms ... [Electronic resource] / Technology description. URL: <https://old.sk.ru/foundation/energy/f/383/t/11040.aspx> (accessed: 05/23/24).
 17. Prospects of renewable energy in the Arctic [Electronic resource]. URL: <https://magazine.neftegaz.ru/articles/arktika/624988-perspektivy-vie-v-arktike> / (accessed: 05/23/24).
 18. Solar Power for Sustainable Offshore Petroleum Exploration and Production in Africa. URL: https://www.researchgate.net/publication/312085159_Solar_Power_for_Sustainable_Offshore_Petroleum_Exploration_and_Production_in_Africa (date of reference: 05/23/24).
 19. A.Ya. Reznichenko "Nuclear technologies in the development of the Arctic" // "Arctic Bulletin. Information and Analytical Journal", No. 2, 2014, p. 80.
 20. Nuclear power engineering for the Arctic shelf [Electronic resource]. URL: <https://scientificrussia.ru/articles/atomnaya-energetika-dlya-arkticheskogo-shelfa> (date of reference: 05/23/24).
 21. V.P. Kuznetsov, V.V. Kushtan, D.A. Mirzoev "The Arctic challenge of the peaceful atom. Review of Russian projects of oil and gas technologies with nuclear power supply for the development of the Arctic shelf"; Journal of the United Shipbuilding Corporation, No. 3(20), 2014.
 22. Timeline for electrification of the Utsira High [Electronic resource]. URL: <https://www.equinor.com/news/archive/2012/11/01/01NovUtsirahoyden> (date of access: 05/23/24).
 23. Maximum utilization of power from shore to Utsira High helps further reduce emissions [Electronic resource]. URL: <https://www.equinor.com/news/archive/2019-10-28-power-utsira-high> (date of request: 05/23/24).
 24. Alternative energy for improving the efficiency of oil and gas field development [Electronic resource]. URL: <https://magazine.neftegaz.ru/articles/arktika/639046-alternativnaya-energetika-dlya-povysheniya-effektivnosti-razrabotki-neftegazovykh-mestorozhdeniy-> / (date of access: 05/23/24).
 25. The resources of the Arctic shelf are our strategic reserve [Electronic resource]. URL: <https://energypolicy.ru/resursy-arkticheskogo-shelfa-eto-nash/business/2019/22/14/> / (date of request: 05/23/24).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 614.841.2.001.5

СОВРЕМЕННЫЕ ПОДХОДЫ К РАССЛЕДОВАНИЮ ПОЖАРОВ НА ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТАХ: ИНТЕГРАЦИЯ НАУКИ И ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ

Мокряк А.В.

ФГБОУ 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

Пожары на энергетических объектах, включая электростанции и распределительные сети, представляют собой серьезную угрозу для экономики и экологии. В 2024 году ущерб от таких чрезвычайных происшествий в России превысил 12 миллиардов рублей (по данным МЧС России). Это обстоятельство стимулирует развитие новых подходов к расследованию причин возгораний, где наука и технологии становятся ключевыми инструментами. Работа в этой области требует интеграции различных дисциплин, таких как пожарная безопасность, материаловедение и современная электроника. В статье рассматриваются современные методы и технологии, применяемые для анализа причин пожаров, а также обсуждаются проблемы и перспективы их внедрения.

Ключевые слова: Алюминиевые проводники, экспертиза пожаров, энергетика, пожарная опасность, искусственный интеллект, тепловизионный анализ.

MODERN APPROACHES TO THE INVESTIGATION OF FIRES AT ENERGY FACILITIES: INTEGRATING SCIENCE AND TECHNOLOGY TO ENHANCE SAFETY

Mokryak A.V.

ST. 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: mokryakanna@mail.ru

Fires at energy facilities, including power plants and distribution networks, pose a significant threat to both the economy and the environment. In 2024, the damage from such emergencies in Russia exceeded 12 billion rubles (according to the Ministry of Emergency Situations). This circumstance stimulates the development of new approaches to investigating the causes of fires, where science and technology are becoming key tools. Work in this area requires the integration of various disciplines, such as fire safety, materials science, and modern electronics. The article discusses modern methods and technologies used to analyze the causes of fires, as well as the challenges and prospects for their implementation.

Keywords: Aluminium conductors, fire expertise, power engineering, fire hazard, artificial intelligence, thermal imaging analysis.

Введение

Современное состояние исследований в области расследования пожаров на объектах энергетики представляет собой актуальную задачу, направленную на обеспечение безопасности и предотвращение чрезвычайных ситуаций. Алюминий широко используется для производства электрических проводов и кабелей в сфере энергетики (Рисунок 1).

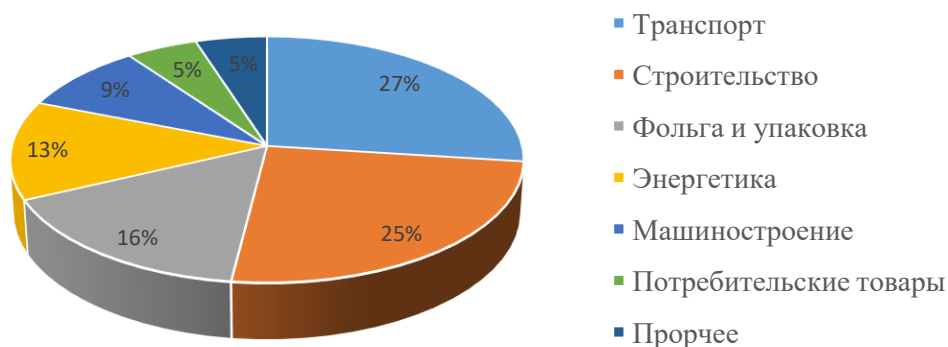


Рисунок 1 – Диаграмма потребления алюминия по отраслям

Алюминиевые провода и кабели, являясь ключевыми элементами энергетической инфраструктуры, подвергаются различным рискам, включая повреждения при пожарах. Это требует проведения тщательных исследований для оценки их состояния после инцидентов [1-3].

Причины пожаров на энергетических объектах могут быть вызваны техническими неисправностями, человеческим фактором, а также природными явлениями, такими как удары молний и перегрев оборудования из-за экстремальных погодных условий. Актуально также учитывать влияние старения оборудования и недостаточную квалификацию персонала, что может приводить к несчастным случаям (Рисунок 2).



Участок бронированного алюминиевого кабеля с изоляцией



Фрагмент алюминиевого секторного кабеля



Изолятор с присоединенным к нему алюминиевым проводником, оплавленным на конце.



Фрагмент силового алюминиевого кабеля и крупный план его участка

Рисунок 2 - Примеры пожаров, вызванные алюминиевыми проводниками

Исследования в области расследования пожаров на энергетических объектах направлены на разработку и внедрение новых технологий, которые позволяют точно определять причины возгораний и предотвращать их повторение. Среди наиболее перспективных методов можно выделить следующие [5-6]:

1. Использование систем мониторинга и анализа данных: Эти системы позволяют в режиме реального времени отслеживать состояние оборудования, выявлять аномалии и предотвращать потенциальные аварии. Это значительно повышает безопасность эксплуатации объектов.

2. Применение искусственного интеллекта и машинного обучения: Эти технологии позволяют анализировать большие объемы данных, выявлять закономерности и прогнозировать возможные сценарии развития аварийных ситуаций.

3. Использование тепловизоров: Тепловизоры позволяют обнаруживать перегрев оборудования на ранних стадиях, что помогает предотвратить возгорание и существенно снизить риски аварий.

4. Современные методы лабораторных исследований и экспертизы пожаров: Такие методы, как сканирующая электронная микроскопия, металлографический анализ и рентгенофлюоресцентный метод, помогают точно определить причину возгорания, что является важным шагом для последующих расследований и предотвращений.

Несмотря на прогресс в области изучения и расследования пожаров, существует ряд проблем, требующих решения. В частности, современные системы мониторинга генерируют огромное количество данных, что требует разработки новых методов их обработки и анализа. Внедрение таких технологий может помочь в автоматизации процесса анализа данных, но их адаптация к специфике пожарных расследований представляет собой сложную задачу. Необходимо разработать обучающие модели, учитывающие специфику работ и возможные сценарии.

Заключение

Таким образом, на сегодняшний день исследования в области изучения пожаров на объектах энергетической инфраструктуры указывают на необходимость разработки комплексного подхода к анализу состояния алюминиевых проводников после пожара. Это позволит более точно определить причины возникновения пожаров и оценить последствия воздействия высоких температур на проводники, что, в свою очередь, повысит уровень безопасности энергетических объектов. Развитие современных технологий и их интеграция в процесс расследования пожаров на энергетических объектах имеют критическое значение для повышения уровня безопасности и предотвращения серьёзных аварий.

Список литературы

1. Мокряк А.Ю., Мокряк А.В. Исследование металлических и электротехнических объектов судебной пожарно-технической экспертизы: монография / под общей редакцией Б.В. Гавкалюка – СПб: Санкт-Петербургский университет ГПС МЧС России, 2022. – 212 с.
2. Кошель Р. Я., Тырин Г. С., Малетина Н. С., Аполлонов И. А. Использование алюминиевых кабелей в электроснабжении жилых и общественных помещений // Современная наука: актуальные вопросы, достижения и инновации: сборник статей XXI Международной научно-практической конференции, Пенза, 05 сентября 2021 года. – Пенза: Наука и Просвещение, 2021. – С. 60-63.
3. Черкасов В. Н., Харламенков А. С. Почему в настоящее время медные проводники предпочтительнее алюминиевых // Пожаровзрывобезопасность. – 2017. – Т. 26. – № 7. – С. 76-77
4. ГОСТ 22483-2012 Жилы токопроводящие для кабелей, проводов и шнуров
5. Мокряк, А. В. Обзор и пожарная опасность алюминиевых проводников // Наукосфера. – 2023. – № 8-2. – С. 67-70.
6. Тихонова И. В., Кузовлева О. В., Роот Е. А., Гвоздев А. Е. Влияние короткого замыкания и термического воздействия на микроструктуру медных и алюминиевых проводников //

Взаимодействие дефектов и неупругие явления в твердых телах, Тула, 24 сентября 2007 года – 28 2009 года. – Тула: Тульский государственный университет, 2007. – С. 49.

References

1. Mokryak A.Yu., Mokryak A.V. Investigation of metal and electrotechnical objects of judicial fire-technical expertise: a monograph / edited by B.V. Gavkalyuk – St. Petersburg: Saint Petersburg University of the Ministry of Emergency Situations of Russia, 2022. – 212 p.
 2. Koshel R. Ya., Tyrin G. S., Maletina N. S., Apollonov I. A. The use of aluminum cables in the power supply of residential and public premises // Modern science: current issues, achievements and innovations: collection of articles of the XXI International Scientific and Practical Conference, Penza, September 05, 2021. Penza: Nauka i Prosveshchenie, 2021. pp. 60-63.
 3. Cherkasov V. N., Kharlamenkov A. S. Why copper conductors are currently preferable to aluminum // Fire and explosion safety. – 2017. – Vol. 26. – No. 7. – pp. 76-77
 4. GOST 22483-2012 Conductive conductors for cables, wires and cords
 5. Mokryak, A.V. Review and fire hazard of aluminum conductors // Naukosphere. – 2023. – No. 8-2. – pp. 67-70.
 6. Tikhonova I. V., Kuzovleva O. V., Root E. A., Gvozdev A. E. The effect of short circuit and thermal effects on the microstructure of copper and aluminum conductors // Interaction of defects and inelastic phenomena in solids, Tula, September 24, 2007 – 28, 2009 of the year. Tula: Tula State University, 2007, p. 49.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 656.71

ОПТИМИЗАЦИЯ ИСПОЛЬЗОВАНИЯ МЕСТ СТОЯНОК ВОЗДУШНЫХ СУДОВ АЭРОДРОМА Г. САНКТ-ПЕТЕРБУРГ «ПУЛКОВО»

Поверинов Д.А.

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА",
Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail:
overhellwr@gmail.ru

В статье рассматриваются актуальные проблемы оптимизации использования мест стоянок воздушных судов в аэродроме Пулково. Проанализированы факторы, влияющие на эффективность эксплуатации перронного пространства, и предложены современные решения по совершенствованию системы управления местами стоянок, включая внедрение автоматизированных систем и пересмотр тарифной политики.

Ключевые слова: Аэродром, аэропорт, воздушные суда, места стоянок, наземное обслуживание.

OPTIMIZATION OF THE USE OF AIRCRAFT PARKING AREAS AT ST. PETERSBURG PULKOVO AIRPORT

Poverinov D.A.

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF
MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-
mail: overhellwr@gmail.ru

The article discusses the current problems of optimizing the use of aircraft parking areas at Pulkovo airport. The factors influencing the efficiency of the apron space operation are analyzed and modern solutions are proposed to improve the parking management system, including the introduction of automated systems and the revision of tariff policy.

Keywords: Airfield, airport, aircraft, parking areas, ground handling.

В условиях постоянного роста авиационных перевозок и увеличения интенсивности полетов особую актуальность приобретает вопрос эффективной организации наземной инфраструктуры аэродромов. Особенно остро стоит проблема оптимального использования мест стоянок воздушных судов, поскольку от рационального размещения и эксплуатации этих объектов напрямую зависит пропускная способность аэродрома, безопасность полетов и качество обслуживания пассажиров.

Современные подходы к организации пространства аэродромов характеризуются комплексным решением задач оптимизации наземного обслуживания воздушных судов. Ключевым направлением развития является внедрение концепции мобильных пассажирских терминалов, реализуемой посредством использования специализированных перронных автобусов-салонов. Данное решение позволяет существенно повысить гибкость использования перронного пространства и оптимизировать маршруты руления воздушных

судов. Значительное внимание уделяется организации безопасного передвижения пассажиров в перронной зоне посредством создания изолированных маршрутов, исключая пересечение с путями движения специального транспорта и средств механизации. Современные тенденции также включают формирование специализированных зон ожидания с развитой инфраструктурой и создание визуально комфортной среды за счет продуманного зонирования и архитектурно-планировочных решений.

Аэродром Пулково характеризуется сложной многоуровневой системой организации мест стоянок воздушных судов, включающей семь перронов различного назначения. Особого внимания заслуживает первый перрон, являющийся центральным элементом наземной инфраструктуры и отличающийся наиболее интенсивным движением специальной техники. В рамках программы развития аэродромной инфраструктуры в текущем году была введена в эксплуатацию дополнительная универсальная парковочная зона, позволяющая разместить до 85 воздушных судов различных типов [1]. Важным преимуществом новой зоны является ее близость к пассажирскому терминалу, что существенно сокращает время наземного обслуживания и повышает общую эффективность использования мест стоянок. Существующая конфигурация перронного пространства аэродрома Пулково обеспечивает возможность одновременного обслуживания значительного количества воздушных судов различных типов, однако требует дальнейшей оптимизации с учетом растущего пассажиропотока и изменяющихся требований к наземной инфраструктуре.

Проведенное исследование загруженности мест стоянок воздушных судов на аэродроме Пулково демонстрирует существенную неравномерность их использования в различные временные периоды. Наибольшая интенсивность эксплуатации стояночных позиций наблюдается в утренние и вечерние часы, что обусловлено формированием традиционных пиков прилета и вылета воздушных судов. При этом в ночной период значительная часть мест стоянок остается незадействованной, что свидетельствует о недостаточно эффективном планировании их использования [3].

При анализе факторов, влияющих на эффективность использования стояночных мест, особое внимание следует уделить структуре воздушного движения. Существенное влияние оказывает соотношение внутренних и международных рейсов, поскольку различные типы воздушных судов требуют разных по размеру и конфигурации мест стоянок. Немаловажным фактором является сезонность авиаперевозок - в летний период наблюдается значительное увеличение нагрузки на места стоянок, что создает дополнительные сложности в организации наземного обслуживания воздушных судов.

В ходе исследования были выявлены существенные проблемные аспекты в текущей системе распределения мест стоянок. Прежде всего, это ограниченность имеющегося пространства при постоянно растущем спросе на авиаперевозки. Существующая инфраструктура аэродрома не всегда позволяет оптимально распределять воздушные суда различных типов по имеющимся местам стоянок, что приводит к снижению эффективности использования перронного пространства. Отдельного внимания заслуживает проблема недостаточной гибкости системы распределения мест стоянок, что особенно остро проявляется при необходимости оперативного реагирования на изменения в расписании полетов или внештатные ситуации.

Текущая ситуация усугубляется неравномерностью заполняемости различных зон аэродрома, что требует внедрения более совершенных методов планирования и управления

местами стоянок. Существующая система распределения не в полной мере учитывает специфику обслуживания различных типов воздушных судов и особенности их технического обслуживания, что создает дополнительные сложности в организации наземного движения и обслуживания воздушных судов [2].

Интерес вызывает проблема высоких тарифов на парковку воздушных судов. В 2024 году Федеральная антимонопольная служба признала их монопольно высокими [5], что создает дополнительную финансовую нагрузку на авиакомпании и может негативно влиять на их решения относительно базирования воздушных судов в аэропорту Пулково. Высокие тарифы также могут приводить к нерациональному использованию мест стоянок, когда перевозчики стремятся минимизировать время пребывания воздушных судов на земле, что усугубляет проблему неравномерности загрузки в пиковые часы.

Исходя из выявленных проблем в системе организации и эксплуатации мест стоянок воздушных судов на аэродроме Пулково, необходимо предложить комплексный подход к их оптимизации, учитывающий современные технологические возможности и экономические аспекты.

Первостепенное значение имеет внедрение автоматизированной системы управления местами стоянок, основанной на использовании искусственного интеллекта и машинного обучения. Данная система позволит в режиме реального времени анализировать загруженность перронного пространства, прогнозировать потребность в местах стоянок с учетом сезонности и суточной неравномерности, а также оптимально распределять имеющиеся ресурсы. Интеграция современных датчиков и средств видеонаблюдения обеспечит точный мониторинг положения воздушных судов и специальной техники, что существенно повысит безопасность и эффективность наземного движения.

Совершенствование методики планирования предполагает разработку гибкой системы распределения мест стоянок, учитывающей множество факторов: тип воздушного судна, время пребывания на стоянке, необходимость технического обслуживания, близость к терминалу и другие операционные требования. Особое внимание следует уделить созданию буферных зон для оперативного реагирования на внештатные ситуации и отклонения от расписания.

Одной из основных проблем остается высокая стоимость использования мест стоянок, что требует пересмотра тарифной политики. В качестве решения предлагается внедрение дифференцированной системы тарификации, учитывающей время суток, продолжительность стоянки и регулярность полетов авиакомпании. Дополнительно рекомендуется рассмотреть возможность предоставления скидок для базовых перевозчиков и применения повышающих коэффициентов в пиковые часы для оптимизации использования стояночных мест.

Аэродром Пулково демонстрирует последовательное движение в направлении оптимизации своей инфраструктуры. По рекомендации ФАС произведено снижение тарифов на стоянку воздушных судов, что способствует повышению привлекательности аэродрома для авиакомпаний. Масштабный проект реконструкции, запланированный до 2028 года, предусматривает строительство новых перронов с современным оборудованием, включая телетрапы, что существенно расширит возможности по обслуживанию воздушных судов различных типов [4]. Реализация данных мероприятий позволит значительно повысить эффективность использования мест стоянок и обеспечить дальнейшее развитие аэродромной инфраструктуры в соответствии с растущими потребностями авиационной отрасли.

Таким образом, проведенное исследование организации мест стоянок воздушных судов в аэропорту Пулково выявило ряд существенных проблем, включая неравномерность использования стояночных мест, высокие тарифы и недостаточную гибкость системы распределения. Предложенные решения, основанные на внедрении автоматизированной системы управления с использованием искусственного интеллекта, совершенствовании методики планирования и оптимизации тарифной политики, в сочетании с реализуемой программой реконструкции аэродромной инфраструктуры, позволят существенно повысить эффективность использования мест стоянок и обеспечить устойчивое развитие аэропорта в соответствии с растущими потребностями авиационной отрасли.

Список литературы

1. Новый федеральный проект по развитию аэродромной инфраструктуры на 2025-2030 годы сформируют к лету [Электронный ресурс]. URL: <https://securityexp.ru/tpost/cy2xjyxu51-novii-fedproekt-po-razvitiyu-aerodromnoi> (дата обращения: 24.02.2025 г.).
2. Организация наземного обслуживания в аэропорту «Пулково» [Электронный ресурс]. URL: <https://jetport.ru/services/obsluzhivanie-vs> (дата обращения: 27.02.2025 г.).
3. Параметры аэродрома Пулково. [Электронный ресурс]. URL: https://pulkovoairport.ru/about/about_pulkovo/airfield/ (дата обращения: 24.02.2025 г.).
4. Пулково добавят размаха. [Электронный ресурс]. URL: <https://www.fontanka.ru/2023/03/22/72155297/> (дата обращения: 27.02.2025 г.).
5. УФАС признало тарифы на парковку Пулково монополично высокими. [Электронный ресурс]. URL: <https://spb.fas.gov.ru/publications/12198> (дата обращения: 27.02.2025 г.).

References

1. A new federal project for the development of airfield infrastructure for 2025-2030 will be formed by the summer [Electronic resource]. URL: <https://securityexp.ru/tpost/cy2xjyxu51-novii-fedproekt-po-razvitiyu-aerodromnoi> (date of reference: 02/24/2025).
 2. Organization of ground handling at Pulkovo airport [Electronic resource]. URL: <https://jetport.ru/services/obsluzhivanie-vs> (date of request: 02/27/2025).
 3. Parameters of the Pulkovo airfield. [electronic resource]. URL: https://pulkovoairport.ru/about/about_pulkovo/airfield/ (date of access: 02/24/2025).
 4. Pulkovo will add scope. [electronic resource]. URL: <https://www.fontanka.ru/2023/03/22/72155297/> (date of application: 02/27/2025).
 5. OFAS recognized the tariffs for Pulkovo parking monopolistically high. [electronic resource]. URL: <https://spb.fas.gov.ru/publications/12198> (date of application: 02/27/2025).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 656.7.025

ПРИМЕНЕНИЕ МЕТОДА ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ПРОЦЕССА НАЗЕМНОГО ОБСЛУЖИВАНИЯ ВОЗДУШНЫХ СУДОВ В ЦЕЛЯХ ПОВЫШЕНИЯ КАЧЕСТВА

Чистяков Д.Ю.

ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА",
Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail:
www.chistyakov@gmail.com

В статье рассматривается вопрос повышения эффективности наземного обслуживания воздушных судов через совершенствование метода взаимодействия между авиакомпаниями и аэропортами. Отмечается, что ключевую роль в обеспечении качества обслуживания и соблюдении технологического графика выполняют оперативные коммуникации между представителями авиакомпании и аэропортовыми службами. Автором выявлены основные проблемы существующих методов взаимодействия, включая несогласованность технологических процессов, недостаточную координацию между службами и неэффективное распределение ответственности.

В качестве решения предлагается новый метод взаимодействия, основанный на усиленной роли представителя авиакомпании. Представитель авиакомпании становится ключевым связующим звеном между операционными подразделениями аэропорта, координируя их работу в режиме реального времени. Основное внимание уделяется его взаимодействию с начальниками смен, диспетчерами центра управления ресурсами и другими ответственными специалистами аэропорта. Такой подход позволяет оперативно согласовывать корректировки в технологическом графике обслуживания воздушных судов, обеспечивая бесшовное выполнение всех операций — от прибытия ВС до его отправления. Благодаря непосредственному контакту с ответственными лицами, представитель авиакомпании может своевременно реагировать на возникающие отклонения, что способствует сокращению операционных задержек, повышению точности выполнения регламентных процедур и улучшению качества обслуживания пассажиров.

Дополнительно рассмотрены показатели качества наземного обслуживания, в частности коэффициент регулярности вылетов, основанный на анализе временных контрольных точек (STD, ETD, ATD). Подчеркивается, что соблюдение технологического графика обслуживания ВС напрямую влияет на регулярность полетов и общую эффективность работы авиационного комплекса.

Внедрение предложенного метода взаимодействия позволит повысить предсказуемость и оперативность наземного обслуживания, что в долгосрочной перспективе приведет к повышению качества наземного обслуживания.

Ключевые слова: Наземное обслуживание, метод взаимодействия, авиакомпания, аэропорт, регулярность вылетов, технологический график, представитель авиакомпании, координация служб, оперативное управление, управление качеством.

APPLICATION OF THE INTERACTION METHOD OF GROUND HANDLING PROCESS PARTICIPANTS TO IMPROVE SERVICE QUALITY

Chistyakov D.Yu.

"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF
MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-
mail: www.chistyakov@gmail.com

The article examines the issue of improving the efficiency of aircraft ground handling through the enhancement of the interaction method between airlines and airports. It is noted that operational communications between airline representatives and airport services play a key role in ensuring service quality and adherence to the technological schedule. The author identifies the main problems of existing interaction methods, including inconsistencies in technological processes, insufficient coordination between services, and ineffective responsibility distribution.

As a solution, a new interaction method is proposed, based on the enhanced role of the airline representative. The airline representative becomes a key link between the airport's operational units, coordinating their work in real-time. Special attention is given to their interaction with shift supervisors, resource management center dispatchers, and other responsible airport specialists. This approach enables the prompt adjustment of the aircraft ground handling technological schedule, ensuring seamless execution of all operations—from aircraft arrival to departure. Through direct contact with key personnel, the airline representative can respond promptly to emerging deviations, helping to reduce operational delays, increase the accuracy of regulatory procedures, and improve passenger service quality.

Additionally, quality indicators for ground handling are examined, particularly the flight regularity coefficient, based on the analysis of time control points (STD, ETD, ATD). It is emphasized that adherence to the aircraft ground handling schedule directly affects flight regularity and the overall efficiency of the aviation complex.

The implementation of the proposed interaction method will enhance the predictability and efficiency of ground handling operations, ultimately leading to an overall improvement in service quality.

Keywords: Ground handling, interaction method, airline, airport, flight regularity, technological schedule, airline representative, service coordination, operational management, quality management.

Эффективное взаимодействие между авиакомпаниями и аэропортами играет ключевую роль в организации наземного обслуживания (НО) воздушных судов (ВС). От слаженности и координации всех участников этого процесса зависят не только регулярность вылета рейсов [2], но и качество обслуживания пассажиров. В условиях роста пассажиропотока, повышения требований к показателям качества и повсеместного ускорения процессов поиск оптимальных методов взаимодействия становится особенно актуальным.

Несмотря на развитие систем управления наземным обслуживанием, сохраняется ряд проблем, связанных с недостаточной координацией между службами аэропорта и авиакомпаний [2]. Одна из ключевых трудностей – несогласованность технологических процессов, вызванная различиями в регламентах и внутренних стандартах работы. Это приводит к задержкам рейсов, росту операционных затрат и перегрузке персонала.

Значимость данной темы подтверждается современной научной литературой и учебными пособиями, например, в пособии Сытых ставится упор на взаимодействие аэропортового предприятия и авиаперевозчика по вопросам качества обслуживания в аэропорту на договорной основе [1]. Договорной основой в данном случае выступает соглашение об уровне качества наземного обслуживания или Service Level Agreement (SLA), основанное на принципе партнерства при обслуживании общего потребителя услуг – пассажира. Важно понимать, что ключевыми условиями для выполнения SLA являются согласованные аэропортовыми предприятиями и перевозчиками конкретные виды обслуживания, цели в отношении уровней качества обслуживания (например, не более 15-и минут ожидания в очереди на регистрацию для пассажиров экономического класса обслуживания и не более 5-и минут – для пассажиров бизнес класса обслуживания), а также механизм определения и контролирования выполнения поставленных задач.

Соглашение об уровне качества НО выступает как основа взаимодействия аэропортового предприятия и авиакомпании, а впоследствии формируются подходы, способы, алгоритмы взаимодействия в рамках, прописанных в SLA. Вышеперечисленное можно заключить в одно понятие – «метод взаимодействия» – которое редко встречается в отраслевой литературе.

Понятие «метод взаимодействия» можно рассмотреть через призму общих определений терминов «метод» и «взаимодействие».

Метод – это один из приёмов выполнения какого-л. действия, позволяющий осуществить что-л. на практике; процедура [4]. Метод определяется как способ достижения какой-либо цели, решения конкретной задачи или способ передачи знаний [6].

Взаимодействие – воздействие различных предметов, явлений действительности друг на друга, обуславливающее изменения в них [5]. Взаимодействие — это процесс, при котором объекты или субъекты оказывают влияние друг на друга, приводя к изменениям в их состоянии или поведении.

Объединяя эти понятия, «метод взаимодействия» можно определить как определенный способ (-ы) или подход (-ы), используемый для организации и управления процессом взаимного влияния между объектами или субъектами. Это может включать стратегии, техники, инструменты, направленные на эффективное сотрудничество и достижение общих целей.

В различных областях науки и практики методы взаимодействия могут принимать специфические формы. Например, в психологии изучаются методы взаимодействия с людьми в зависимости от их типов личности, что позволяет выстраивать эффективные коммуникации и взаимовыгодные отношения.

Понятие «метод взаимодействия» в контексте наземного обслуживания воздушных судов можно рассматривать как совокупность способов, инструментов и процессов, используемых авиакомпанией и аэропортом для координации совместной деятельности, обеспечения своевременного и качественного наземного обслуживания.

Основой метода становится оперативное взаимодействие между представителем авиакомпании и ключевыми аэропортовыми службами. Важную роль играет непосредственный контакт с ответственными лицами, что позволяет ускорить процесс согласования корректировок в технологическом графике обслуживания - пооперационном графике наземного обслуживания воздушных судов.

Главной целью интеграции нового метода взаимодействия является создание бесшовного управления всеми процессами наземного обслуживания. Это означает, что каждая операция – от прибытия ВС до его отправления – выполняется в едином логическом цикле без задержек, вызванных несогласованностью действий различных служб. Представитель авиакомпании становится связующим звеном между операционными подразделениями, координируя их работу в режиме реального времени.

Качество — степень соответствия совокупности присущих характеристик объекта установленным требованиям [7]. Для оценки и повышения качества наземного обслуживания необходимо прибегнуть к показателям качества (критериям качества).

Основными показателями качества для оценки качества наземного обслуживания могут применяться следующие показатели: показатели безопасности, экологичности, информационного обслуживания и своевременности (регулярности). Показатель своевременности (регулярности) характеризуют свойства пассажирских перевозок, обуславливающие движение воздушных судов в соответствии с объявленным расписанием или другими установленными требованиями по времени их движения. К показателям своевременности относят:

- долю транспортных средств, отправляемых по расписанию;

- долю транспортных средств, прибывающих по расписанию.

В целях учета регулярности полетов используются контрольные точки:

- STD – Время начала движения по расписанию (scheduled time departure);
- ETD – Расчетное время начала движения (estimated time departure);
- ATD – Фактическое время начала движения (actual time departure).

Используя вышесказанное, можно принять за основной показатель качества наземного обслуживания показатель своевременности, выраженное в процентах отношение количества выполненных рейсов без задержки к общему количеству выполненных рейсов [3]:

$$R = \frac{Q_{\text{нрег}}}{Q_{\text{рег}}} * 100\%, \text{ где}$$

R – коэффициент регулярности;

$Q_{\text{нрег}}$ – кол-во рейсов с $ATD > STD$;

$Q_{\text{рег}}$ – кол-во рейсов с $ATD \leq STD$.

Таким образом, для повышения качества наземного обслуживания, необходимо, чтобы коэффициент R был выше, что происходит с увеличением количества рейсов, отправленных регулярно.

Регулярность вылета напрямую связана с соблюдением технологического графика обслуживания ВС.

$$T = \sum_{n=1}^n t_n, \text{ где}$$

T – общее затрачиваемое время наземного обслуживания ВС;

t_n – затрачиваемое время на n -операцию;

n – порядковый номер операции.

Однако в условиях неопределенности постоянно происходят отклонения от выполнения операций, что приводит к увеличению продолжительности операций:

$$t_n = t_{\text{план}} + \Delta t, \text{ где}$$

$t_{\text{план}}$ – запланированное время на операцию t_n ;

Δt – дополнительное время на операцию t_n .

Таким образом, показатель регулярности напрямую зависит от предотвращения возникновения Δt в технологическом графике ВС. В этих целях может быть использован метод взаимодействия. Введение данного метода взаимодействия приведет к ряду положительных изменений. Во-первых, сократится количество операционных задержек за счет гибкого управления ресурсами и минимизации простоев. Во-вторых, повысится предсказуемость работы наземных служб, что позволит более эффективно планировать загрузку инфраструктуры. В-третьих, усилится контроль качества предоставляемых услуг, поскольку представитель авиакомпании сможет оперативно реагировать на отклонения от стандартов обслуживания, вовремя предпринятые корректирующие мероприятия в целом приведут к повышению качества наземного обслуживания.

Список литературы

1. Сытых, Е. И. Управление качеством технологических процессов в аэропортах [Текст] / Е. И. Сытых. — Санкт-Петербург : Университет ГА, 2019. — 124 с.
2. Кропивенцева, С. А. Взаимодействие аэропорта и авиакомпании в ходе наземного обслуживания воздушных судов [Текст] / С. А. Кропивенцева, Самар. гос. аэрокосм. ун-

- т им. С. П. Королева. — Самара : Изд-во СГАУ, 2015. — 71 с. — Библиогр.: с. 71 (8 назв.). — 300 экз.
3. Наумова, Д. А. Методики оценки регулярности полетов авиакомпаний [Текст] / Д. А. Наумова // Научный вестник Московского государственного технического университета гражданской авиации. — 2012. — № 181. — С. 90-93. — EDN PCVTBV.
 4. Большой толковый словарь русского языка [Текст] / [гл. ред. С. А. Кузнецов]. — Санкт-Петербург : Норинт; Москва : Рипол классик, 2008. — 1534, [1] с. — (Библиотека энциклопедических словарей (БЭС)). — ISBN 978-5-7711-0015-9.
 5. Ефремова, Т. Ф. Новый словарь русского языка. Толково-словообразовательный: Св. 136000 словар. ст., ок. 250000 семант. единиц: [В 2 т.] [Текст] / Т. Ф. Ефремова. — Москва : Рус. яз., 2000. — 27 см. — Библиотека словарей русского языка: А. Т. 2: П - Я. Т. 2. — 1084 с. — ISBN 5-200-02802-7.
 6. Современный образовательный процесс: основные понятия и термины: [краткий терминологический словарь] [Текст] / М-во образования Российской Федерации, Нижнетагильская гос. социально-пед. акад., Каф. рус. яз. Каф. методики технологии и предпринимательства; [Олешков М. Ю., Уваров В. М.]. — Москва : Компания Спутник+, 2006. — 189, [1] с. — ISBN 5-364-00329-9.
 7. ГОСТ Р ИСО 9000-2015. Системы менеджмента качества. Основные положения и словарь [Электронный ресурс] // Консорциум Кодекс. — Режим доступа: <https://docs.cntd.ru/document/1200124393>.

References

1. Sytykh, E. I. Quality management of technological processes at airports [Text] / E. I. Sytykh. — Saint Petersburg : University of GA, 2019. p.124
2. Kropiventseva, S. A. The interaction of the airport and the airline during the ground handling of aircraft [Text] / S. A. Kropiventseva ; Samara State Aerospace. S. P. Korolev University. Samara : Publishing House of SSAU, 2015. p. 71 Bibliogr.: p. 71 (8 titles). 300 copies.
3. Naumova, D. A. Methods for assessing the regularity of airline flights [Text] / D. A. Naumova // Scientific Bulletin of the Moscow State Technical University of Civil Aviation. - 2012. — No. 181. — pp. 90-93. — EDN PCVTBV.
4. The Great explanatory dictionary of the Russian language [Text] / [chief editor S. A. Kuznetsov]. — St. Petersburg : Norint; Moscow : Rapol classic, 2008. — 1534, [1] p. — (Library of Encyclopedic Dictionaries (BES)). — ISBN 978-5-7711-0015-9.
5. Efremova, T. F. A new dictionary of the Russian language. Explanatory and word-formation: St. 136,000 vocabulary, approx. 250,000 semantics. units: [In 2 volumes] [Text] / T. F. Efremova. — Moscow : Rus. yaz., 2000. — 27 cm. — Library of dictionaries of the Russian language: A. T. 2: P - Ya. Vol. 2. — p. 1084— ISBN 5-200-02802-7.
6. Modern educational process: basic concepts and terms: [short terminological dictionary] [Text] / Ministry of Education of the Russian Federation, Nizhny Tagil State Socio-pedagogical University. akad., Department of Russian, Department of Methods of Technology and Entrepreneurship; [Oleshkov M. Yu., Uvarov V. M.]. — Moscow : Sputnik Company+, 2006. — pp. 189, [1] — ISBN 5-364-00329-9.

Чистяков Д.Ю. Применение метода взаимодействия участников процесса наземного обслуживания воздушных судов в целях повышения качества// Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 4(54) с. 192–197

7. GOST R ISO 9000-2015. Quality management systems. Basic provisions and dictionary [Electronic resource] // Consortium Codex. — Access mode: <https://docs.cntd.ru/document/1200124393> .
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК: 621.311.21: 658.5: 681.518.3

ОЦЕНКА МЕТОДИК ОПРЕДЕЛЕНИЯ ИНДЕКСА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ

Степанов Г.А.

ФГАОУ ВО «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ», Красноярск, Россия (660041, Красноярский край, город Красноярск, Свободный пр-кт, д.79), e-mail: GStepanov-GE20@yandex.ru

В наши дни наблюдается тенденция перехода от стратегии планово-предупредительного технического обслуживания и ремонтов (далее ТОиР) – к ТОиР по фактическому состоянию, что связано с постоянным «старением» оборудования и необходимостью применения новых и более совершенных методов контроля и определения его технического состояния. Такое состояние описывается индексом технического состояния (ИТС).

В статье рассматриваются различные подходы к определению ИТС и примеры их применения в различных отраслях энергетики. Проведен анализ существующей и других методик, не утвержденных нормативными документами и не установленными на законодательном уровне, но представляющие интерес с точки зрения альтернативного варианта расчета ИТС для гидроэнергетики.

Ключевые слова: Техническое состояние, методика, гидроэнергетика, электроэнергетика, индекс технического состояния, диагностика, мониторинг.

THE EVALUATION OF METHODS FOR ESTIMATION OF THE HEALTH INDEX OF TECHNOLOGICAL EQUIPMENT

Stepanov G.A.

SIBIRIAN FEDERAL UNIVERSITY, Krasnoyarsk, Russia (79 Svobodny Ave., Krasnoyarsk, 660041), e-mail: GStepanov-GE20@yandex.ru

Nowadays, there is a tendency to switch from a strategy of planned preventive maintenance, repairs and overhaul (hereinafter MRO) to Reliability-centered maintenance (RCM), which is associated with the constant "aging" of equipment and the need to apply new and more advanced methods of monitoring and determining its technical condition. The health index (HI) of the equipment, describes this condition.

The article discusses various approaches to determining HI and provides examples of their application in different sectors of the energy industry. An analysis of existing methodologies, as well as those not approved by regulatory documents or established at the legislative level but are of interest as alternative options for calculating HI for hydropower facilities, has been conducted.

Keywords: Technical condition, methodology, hydropower, electric power industry, health index, diagnostics, monitoring.

Существует действующая методика оценки индекса технического состояния, разработанная Минэнерго [3], применяющаяся на энергообъектах и промышленных предприятиях для определения индекса технического состояния оборудования. Такая методика является единственной и не имеет альтернатив. Сложно делать выводы о том, насколько достоверные результаты она дает, а именно соответствуют ли эти результаты фактическому состоянию оборудования. Кроме того, важно понимать, как от полученного

результата зависит степень технологического воздействия на оборудование, начиная от капитального ремонта и заканчивая плановой диагностикой.

Данный документ устанавливает правила оценки технического состояния основного оборудования, что в конечном итоге сводится к определению интегрального показателя - индекса технического состояния оборудования в целом (далее ИТС), который для функциональных и обобщенного узлов (далее ИТСУ) определяется по формуле (1):

$$\text{ИТСУ} = 100 \cdot \sum i \frac{(\text{KB}_i \cdot \text{ОГП}_i)}{4}, \quad (1)$$

где KB_i – значение весового коэффициента для группы параметров технического состояния;

ОГП_i – балльная оценка группы параметров технического состояния.

Для единицы основного технологического оборудования ИТС определяется по формуле (2):

$$\text{ИТС} = \sum (\text{KBУ}_i \cdot \text{ИТСУ}_i), \quad (2)$$

где KBУ_i – значение весового коэффициента для функционального или обобщенного узла;

ИТСУ_i – ИТС функционального или обобщенного узла.

Весовые коэффициенты определяются на основании экспертных оценок и приводятся непосредственно в приказе Минэнерго [3].

Также устанавливается диапазон, отражающий вид технического состояния оборудования [2], в зависимости от полученного значения ИТС, приведенный в Таблице 1.

Таблица 1 – вид технического воздействия в зависимости от полученного ИТС

Диапазон ИТС	Вид технического состояния	Вид технического воздействия
≤ 25	Критическое	Вывод из эксплуатации, техническое перевооружение и реконструкция
$25 < X \leq 50$	Неудовлетворительное	Дополнительное техническое обслуживание и ремонт, усиленный контроль ТС, техническое перевооружение
$50 < X \leq 70$	Удовлетворительное	Усиленный контроль ТС, капитальный ремонт, реконструкция
$70 < X \leq 85$	Хорошее	По результатам плановой диагностики
$85 < X \leq 100$	Очень хорошее	Плановая диагностика

Как и любой нормативный документ, методика может иметь свои ограничения и отклонения. Возможные факторы, влияющие на точность и надежность оценок, включают в себя: ошибки и погрешности при измерениях, а также недостаток необходимых данных; человеческий фактор, а именно субъективность экспертных оценок; особенности эксплуатации самого оборудования; устаревшие или неподходящие методы диагностики, которые могут не учитывать современные требования к оборудованию. Нельзя пренебрегать

возможностью периодических ревизий и обновлений метода в соответствии с передовыми практиками.

В области гидроэнергетики данная методика применяется для расчета ИТС начиная от отдельных узлов оборудования и заканчивая ГЭС в целом.

В ПАО «Интер РАО» [4] предложена методика по оценке ИТС питательного турбонасоса тепловых электростанций на основе экспертных оценок. Предложенный подход можно назвать частным случаем методики Минэнерго [3]. Явные сходства наблюдаются в структуре выявления связей между отдельными узлами оборудования и порядком расчета, за исключением весовых коэффициентов функциональных узлов и единиц оборудования, которые определяются автором на основе опытной эксплуатации оборудования. Также сходство имеется в распределении диапазонов, определяющих степень технологического воздействия по результатам расчетов.

В другой работе, при оценке технического состояния по модифицированной методике определения ИТС [5], поднимается проблема субъективности в оценках ТС сложных технических систем, которая возникает при использовании традиционных методов, основанных на экспертных мнениях.

Здесь ИТС определяется зависимости от их изменения параметров ТС в большую или меньшую сторону в процессе работы оборудования по формуле (3) и (4) соответственно:

$$\text{ИТС}_{i,j} = \frac{(x_{i,j}^{\Phi} - x_{i,j}^{\min})}{x_{i,j}^{\max} - x_{i,j}^{\min}} \cdot 100\%, \text{ при уменьшении параметра;} \quad (3)$$

$$\text{ИТС}_{i,j} = \frac{(x_{i,j}^{\Phi} - x_{i,j}^{\max})}{x_{i,j}^{\min} - x_{i,j}^{\max}} \cdot 100\%, \text{ при увеличении параметра,} \quad (4)$$

где $\text{ИТС}_{i,j}$ – индекс технического состояния i – го узла j – го параметра;

$x_{i,j}^{\Phi}$ – фактическое значение параметра при расчете;

$x_{i,j}^{\max}, x_{i,j}^{\min}$ – максимальное и минимальное значения параметра.

Весовые коэффициенты параметра определяются по формуле (5). При таком подходе, вес параметра будет изменяться в зависимости от ТС оборудования.

$$w_{i,j} = \frac{v_{i,j}}{\sum_{j=1}^{m_i} v_{i,j}}, \quad (5)$$

$$\text{где } v_{i,j} = \frac{S_{i,j}}{\bar{x}_{i,j}} = \frac{\sqrt{\frac{\sum_{k=1}^{N_{i,j}} (x_{i,j,k} - \bar{x}_{i,j})^2}{N_{i,j} - 1}}}{\bar{x}_{i,j}} - \text{коэффициенты вариации;}$$

$S_{i,j}$ – стандартное отклонение параметра, определяемое на основе данных в период эксплуатации;

$\bar{x}_{i,j}$ – среднее значение параметра;

$N_{i,j}$ – объем выборки параметра.

Весовые коэффициенты функционального узла определяются по матрице парных сравнений, которая составляется исходя из топологического анализа графа функционального узла методом Degree importance Line, что позволяет снизить субъективность оценки.

ИТС единицы оборудования определяются аналогично методике Минэнерго [3].

Проведено сравнение расчетов для двухконтурных турбореактивных двигателей.

Если принять во внимание, что расчет ведется для объекта, который изначально находится «очень хорошо» техническом состоянии, то в начале исследуемого интервала обе методики дают схожий результат.

Однако 68 процентов исследуемого промежутка показывают заметную разницу в расчетах. Полученные значения по такой методике на данном интервале отличаются в среднем от 8 до 13 процентов. Такая разница обуславливается более гибким и усложненным анализом технических параметров объекта в предлагаемой методике, в то время как методика Минэнерго ввиду стандартизированного и упрощенного порядка определения ИТС на начальных интервалах может не позволить определить раннее снижение показателей системы.

Ближе к концу интервала расчеты снова дают близкий результат.

Другой подход по оценке технического состояния для оборудования тепловой станции, а именно конденсатора был предложен в работе авторов из Национального исследовательского университета «Московский энергетический институт» [1]. При оценке ТС сравнивались параметры существующего конденсатора пара и его математической модели. Считается, что при определении ИТС эффективно использовать решение на основе выявления степени отклонения технологических параметров от значений предупредительных уставок.

ИТС параметра определяется по формуле (6):

$$\text{ИТС}_{ij} = \begin{cases} \frac{(x_{i,j}^{\Phi} - x_{min})}{x_{mean} - x_{min}}, & \text{если } |x_{i,j}^{\Phi} - x_{min}| < |x_{max} - x_{i,j}^{\Phi}| \\ \frac{(x_{max} - x_{i,j}^{\Phi})}{x_{max} - x_{mean}}, & \text{если } |x_{max} - x_{i,j}^{\Phi}| < |x_{i,j}^{\Phi} - x_{min}| \end{cases} \quad (6)$$

где $x_{i,j}^{\Phi}$ – то же, что и в формуле (3, 4);

x_{min}, x_{max} – минимальное и максимальное значение параметра, соответствующее уставке предупредительной сигнализации;

$x_{mean} = \frac{x_{max} - x_{min}}{2}$ – среднее значение параметра, оптимальное по отношению технологической уставки.

ИТС для функционального узла, включающего группу параметров ТС определяется как среднее гармоническое от каждого ИТС параметров узла по формуле (7):

$$\text{ИТС}_i = \frac{j}{\frac{1}{\text{ИТС}_{i,1}} + \dots + \frac{1}{\text{ИТС}_{i,j}}} \cdot 100, \quad (7)$$

где j – количество параметров i – го узла.

Итоговая оценка определяется аналогично [3, 5]. С точки зрения автоматизации расчетов и легкости восприятия данный метод может применяться для систем с достаточно развитыми системами автоматического мониторинга состояния. Однако, не на всех типах оборудования существуют такие узлы, параметры которых можно определять в режиме реального времени без остановки и простоя и у которых существуют предупредительные уставки по некоторым

технологическим параметрам, что может осложнить расчет по такому методу. В таком случае предлагается комбинировать доступные методы расчета.

Выводы

Для определения ИТС и последующей оценки целесообразно принять все вышеперечисленные методики:

- методику Минэнерго [3], которую удобно использовать из-за четко установленных и стандартизированных весовых коэффициентов, что существенно упрощает процесс расчета;
- модифицированную методику [5], которая отличается более сложным порядком определения ИТС, но в тоже время наиболее подробно отражает взаимосвязь технических параметров и узлов оборудования;
- методику, предложенную научно исследовательским университетом Московским энергетическим институтом [1], в которой ИТС параметра, в отличие от методики Минэнерго определяется на основе предупредительных уставок.

На выбор именно этих методик повлияли их доступность, достаточность и полнота представленного порядка расчета и оценки ИТС. Другие источники либо не предоставляли необходимой информации для возможности их применения, либо в большей мере повторяли уже существующую методику.

Однако, за эталонную будет считаться официально утвержденная методика ввиду того, что она подкреплена действующей нормативно-технической документацией.

Полученные результаты по приведенным методикам не дают однозначного решения о возможности применения их для Гидроэнергетики, ввиду отсутствия показательных и качественных примеров использования таких методик в этой области.

Список литературы

1. Щербатов И.А., Долгушев А.Н., Белов М.К., Агибалов В.А., Салов В.А. Оценка технического состояния оборудования тепловой станции на примере конденсатора // International Journal of Open Information Technologies vol. 11. - 2023. - №3. - С. 45-51.
2. О комплексном определении показателей технико-экономического состояния объектов электроэнергетики, в том числе показателей физического износа и энергетической эффективности объектов электросетевого хозяйства, и об осуществлении мониторинга таких показателей: Постановление Правительства РФ от 19 декабря 2016 г. № 1401. в ред. Постановления Правительства РФ от 30.05.2023 N 878. // URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=450200> (дата обращения 12.02.2025). – Режим доступа: свободный. – Текст: электронный.
3. Об утверждении методики оценки технического состояния основного технологического оборудования и линий электропередачи электрических станций и электрических сетей: приказ от 26.07.2017 г. № 676. в ред. Приказа Минэнерго России от 17.03.2020 №192 – Москва: Министерство энергетики РФ, 2017. – 274 с. URL: <https://base.garant.ru/71779722/> (дата обращения 05.02.2025). – Режим доступа: свободный. – Текст: электронный.
4. Оклей П. И., Методика оценки интегрального технического состояния оборудования тепловых электростанций // Транспортное дело России. - 2015. - №6. - С. 72-75.

5. Хиеу В.Д., Файзрахманов Р.А. Модифицированная модель индекса технического состояния системы. Алгоритм расчета и анализ применимости // Вестник Пермского Государственного технического университета. Электротехника, информационные технологии, системы управления. – 2024. – №50. – С. 195-215.

References

1. Shcherbatov I.A., Dolgushev A.N., Belov M.K., Agibalov V.A., Salov I.V. Thermal plant equipment technical condition assessment on the example of a condenser // International Journal of Open Information Technologies vol. 11. – 2023. – №3. – pp. 45-51.
 2. O kompleksnom opredelenii pokazatelej tehniko-jekonomicheskogo sostojanija ob"ektov jelektrojenergetiki, v tom chisle pokazatelej fizicheskogo iznosa i jenergeticheskoy jeffektivnosti ob"ektov jelektrosetevogo hozjajstva, i ob osushhestvlenii monitoringa takih pokazatelej: Postanovlenie Pravitel'stva RF ot 19 dekabrya 2016 g. № 1401. v red. Postanovlenija Pravitel'stva RF ot 30.05.2023 N 878. // Available at: <https://normativ.kontur.ru/document?moduleId=1&documentId=450200> (accessed 12 February 2025).
 3. Ob utverzhdenii metodiki ocenki tehničeskogo sostojanija osnovnogo tehnologicheskogo oborudovaniya i linij jelektroperedachi jelektricheskikh stancij i jelektricheskikh setej: prikaz ot 26.07.2017 g. № 676. v red. Prikaza Minjenergo Rossi ot 17.03.2020 №192 – Moskva: Ministerstvo jenergetiki RF, 2017. – 274 s. Available at: <https://base.garant.ru/71779722/> (accessed 5 February 2025).
 4. Okley P.I. Methodology to evaluate the integral technical state of equipment for thermal power stations // Transport business in Russia. – 2015. – №6. pp. 72-75.
 5. Hieu W.D., Fayzrahmanov R.A. Modified model of the system technical condition index. Algorithm for calculation and applicability analysys // Vestnik Permskogo Gosudarstvennogo tehničeskogo universiteta. Jeletrotehnika, informacionnye tehnologii, sistemy upravlenija. – 2024. – №50. – pp. 195-215.
-