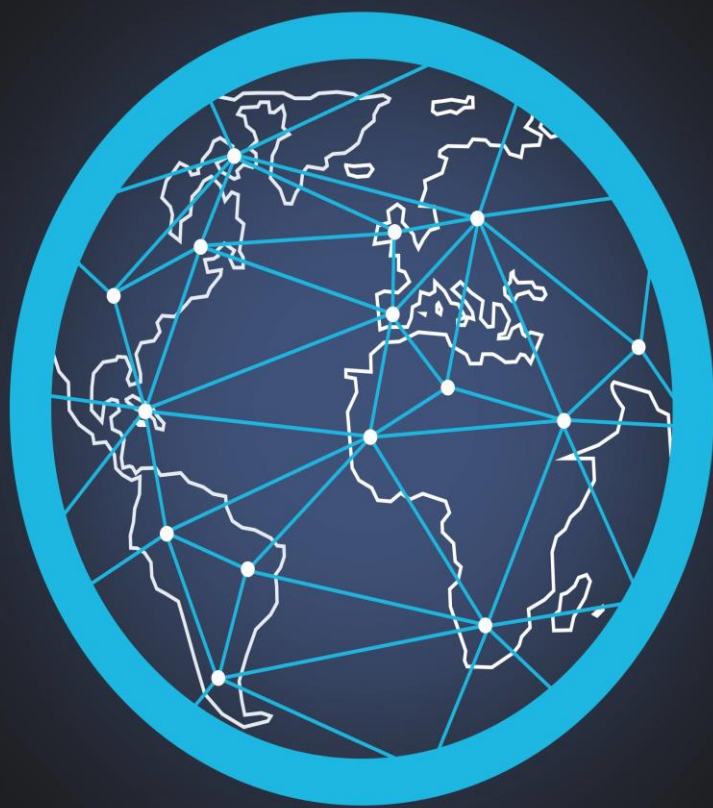


Международный журнал информационных технологий и энергоэффективности



Том 9 Номер 12 (50)



2024



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

| | | |
|----|--|-----------|
| 1. | Усванова Д.Р. Исследование методов защиты ВЕБ-приложений от атак типа SQL-инъекция | 5 |
| | Usmanova D.R. Investigation of methods for protecting WEB applications from SQL injection attacks | |
| 2. | Ван Цинь, Ма Буюнь, Чжао Шиюй, Ли Цзымин Анализ популярных в настоящее время технологий ФРОНТЕНД-ФРЕЙМВОРКОВ | 8 |
| | Wang Qin, Ma Buoni, Zhang Shiyu, Li Zimin Analysis of currently popular FRONT-END FRAMEWORK technologies | |
| 3. | Поляков А.А. Скрытые риски массовых обновлений данных: как избежать потери и утечки информации | 12 |
| | Polyakov A.A. Hidden risks of mass data updates: how to prevent data loss and leaks | |
| 4. | Сушко А.В. Разработка мобильного приложения 1С с использованием REACT NATIVE | 16 |
| | Sushko A.V. Development of a 1C mobile application using react | |
| 5. | Никитин А.А. Сравнительный анализ производительности REST и GRPC подходов обмена данными | 20 |
| | Nikitin A.A. Comparative analysis of the performance of REST and GRPC data exchange approaches | |
| 6. | Ноянов Р.С. Как защитить JSONB-поля в POSTGRESQL от утечек данных и инъекций | 25 |
| | Nayanov R.S. How to protect JSONB fields in POSTGRESQL from data leaks and injections | |
| 7. | Поляков А.А. Технологии защиты данных на мобильных устройствах как часть комплексной системы защиты объектов информатизации | 29 |
| | Polyakov A.A. Data protection technologies on mobile devices as part of a comprehensive information security system | |
| 8. | Ноянов Р.С. Использование микросегментации для повышения безопасности в крупных объектах информатизации | 33 |
| | Nayanov R.S. The use of microsegmentation to improve security in large information facilities | |
| 9. | Некрасов Т.Д., Комбаров В.Д., Лозница С.Ю. Восприятие человеческого голоса при помощи искусственного интеллекта | 37 |

| | | |
|-----|---|------------|
| | Nekrasov T.D., Kombarov V.D., Loznitsa S.Yu. Perception of the human voice with the help of artificial intelligence | |
| 10. | Варбанский К.С., Городничев М.Г. Анализ тенденций развития сетей с комплементарной разреженностью | 43 |
| | Varbansky K.S., Gorodnichev M.G. analysis of trends in the development of networks with complementary sparsity | |
| 11. | Ветров С.Ю. Сравнение реляционных СУБД с открытым исходным кодом | 52 |
| | Vetrov S.Y. Comparison of open source relational DBMS | |
| 12. | Чвала Д.А. Основные источники угроз в информационных системах персональных данных | 57 |
| | Chvala D.A. Main sources of threats in personal data information systems | |
| 13. | Тищенко В.А. Применение методов реструктуризации и дублирования для отображения результатов запросов в ООСУБД НИКА | 62 |
| | Tishchenko V.A. Application of restructuring and duplication methods for representation query results in NIKA OODBMS | |
| 14. | Пивоварова У.А. Уязвимости контейнеров: риски, примеры и методы защиты | 71 |
| | Pivovarova U.A. Container vulnerabilities: risks, examples, and protection methods | |
| 15. | Гулов Т.У., Иванченко С.А., Сысоев Н.Д. Рост автоматизации и его влияние на рынок труда | 75 |
| | Gulov T.U., Ivanchenko S.A., Sysoev N.D. The growth of automation and its impact on the labor market | |
| 16. | Бютнер С.И. HIDDENEYE: инструмент для фишинга | 84 |
| | Buetner S.I. HIDDENEYE: a phishing tool | |
| 17. | Гулов Т.У., Иванченко С.А., Сысоев Н.Д. Искусственный интеллект в здравоохранении | 88 |
| | Gulov T.U., Ivanchenko S.A., Sysoev N.D. Artificial intelligence in healthcare | |
| 18. | Шаханова М.В., Четверик М.А., Шаханова В.С. Защита информации в условиях чрезвычайных ситуаций | 96 |
| | Shakhanova M. V., Chetverik M.A., Shakhanova V.S. Information protection in emergency situations | |
| 19. | Бютнер С.И. RUSTSCAN: быстрое и эффективное сканирование портов с использованием RUST | 102 |
| | Buetner S.I. RUSTSCAN: fast and efficient port scanning using RUST | |
| 20. | Хихол Е.А. Разработка системы сбора набора данных для анализа эксплойтов | 106 |
| | Khikhol E.A. Developing a data collection system for exploit analysis | |
| 21. | Царегородцев Е.Л., Романенков А.А., Соколов А.Д. Объектно-визуальный способ моделирования замкнутой системы управления температурой с двухступенчатым контроллером | 110 |

| | | |
|---|---|------------|
| | Tsaregorodtsev E.L., Romanenkov A.A., Sokolov A.D. An object-visual method for modeling a closed temperature control system with a two-stage controller | |
| 22. | Колода Е. Кейс-стадии: первопроходцы внедрения ИИ | 114 |
| | Koloda E. Case studies: pioneers in ai implementation | |
| ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ | | |
| 23. | Родионов Д.Р., Литвин Р.А. Интеграция ветрогенераторов в транспортные средства и перспективы их использования в арктическом регионе | 120 |
| | Rodionov D. R., Litvin R. A. Integration of wind turbines into vehicles and prospects for their use in the arctic region | |
| 24. | Кудабаев Р.Б., Сулейменов У.С. Повышение энергоэффективности термообработки бетонных и железобетонных изделий | 125 |
| | Kudabaev R.B., Suleimenov U.S. Improving the energy efficiency of heat treatment of concrete and reinforced concrete products | |
| 25. | Ткачева Е.Г., Калашников В.С. Выбор датчиков для гиперспектральных систем | 130 |
| | Tkacheva E.G., Kalashnikov V.S. Sensor selection for hyperspectral systems | |
| 26. | Калашников В.С., Ткачева Е.Г. Многокритериальная оптимизация параметров мостика для прыжков в бассейн | 134 |
| | Kalashnikov V.S., Tkacheva E.G. Multicriteria optimization of parameters of a pool diving bridge | |
| 27. | Брагин Д.М., Зинина С.А., Попов А.И., Мустафин Р.М., Кечин Н.Н. Теплопроводность композиционного материала со стальной решеткой на основе TPMS типа SCHOEN'S GW и матрицей из керамического материала | 144 |
| | Bragin D.M., Zinina S.A., Popov A.I., Mustafin R.M., Kuchin N.N. Thermal conductivity of a composite material with a steel lattice based on TPMS of SCHOEN'S GW TYPE and a matrix made of ceramic material | |
| ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ | | |
| 28. | Мокряк А.В. Исследования с применением сканирующей электронной микроскопии в целях установления причин возникновения пожаров на алюминиевых проводниках | 151 |
| | Mokryak A.V. Scanning electron microscopy studies to determine the causes of fires on aluminum conductors | |
| 29. | Мокряк А.В. Причины возникновения пожаров в электромобиле | 157 |
| | Mokryak A.V. Causes of fires in electric vehicles | |



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.736

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ АТАК ТИПА SQL-ИНЪЕКЦИЯ

Усванова Д.Р.

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:
dusvanova@gmail.com

В статье рассмотрены методы защиты веб-приложений от атак типа SQL-инъекция, которые остаются одной из наиболее серьезных угроз информационной безопасности. Приведён анализ основных типов SQL-инъекций, их механизма действия и возможных последствий, включая угрозу конфиденциальности, целостности и доступности данных. В работе выделены три ключевых подхода к защите: использование подготовленных выражений (Prepared Statements), валидация входных данных и применение объектно-реляционного отображения (ORM).

Ключевые слова: SQL-инъекции, защита веб-приложений, Prepared Statements, валидация данных, ORM, информационная безопасность, методы защиты, анализ атак.

INVESTIGATION OF METHODS FOR PROTECTING WEB APPLICATIONS FROM SQL INJECTION ATTACKS

Usmanova D.R.

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: dusvanova@gmail.com

The article examines methods for protecting web applications against SQL injection attacks, which remain one of the most significant threats to information security. An analysis of the main types of SQL injections, their mechanisms of operation, and potential consequences, including risks to data confidentiality, integrity, and availability, is presented. The study highlights three key approaches to protection: the use of prepared statements (Prepared Statements), input data validation, and object-relational mapping (ORM).

Keywords: SQL injection, web application protection, Prepared Statements, data validation, ORM, information security, protection methods, attack analysis.

Атаки типа SQL-инъекция представляют собой одну из наиболее серьезных угроз для безопасности современных веб-приложений. Уязвимости SQL-инъекций неизменно занимают верхние строчки в ежегодных отчётах о киберугрозах, таких как OWASP Top 10. Например, в 2020 году атака на авиакомпанию EasyJet привела к утечке данных более 9 миллионов клиентов, включая финансовую информацию. SQL-инъекция является одним из наиболее распространенных типов атак на веб-приложения, и ее можно предотвратить путем использования параметризованных запросов и валидации пользовательского ввода [1]. Особую опасность SQL-инъекций представляет их универсальность. Они могут быть использованы не только для получения доступа к конфиденциальным данным, но и для

нарушения их целостности или доступности, что влечёт значительные финансовые и репутационные потери. По данным исследований, на долю SQL-инъекций в 2022 году пришлось около 40% всех зарегистрированных уязвимостей веб-приложений [3]. Цель данной работы — исследовать эффективные методы предотвращения атак типа SQL-инъекция.

Понимание механизмов SQL-инъекций играет ключевую роль. Одним из эффективных методов защиты от SQL-инъекций является использование механизмов обнаружения и предотвращения инъекций [4]. Эти атаки основаны на внедрении вредоносного кода в SQL-запросы, что позволяет злоумышленникам изменять их логику. Наиболее распространённые типы SQL-инъекций включают:

- **Ошибка-сообщения:** использование сообщений об ошибках базы данных для извлечения её структуры.
- **Объединение запросов (UNION):** выполнение дополнительных запросов через оператор UNION.
- **Булевы атаки:** анализ ответов сервера на условия, возвращающие истину или ложь.
- **Замедление выполнения:** использование временных задержек в запросах для определения успеха атаки.

К основным методам защиты относятся подготовленные выражения (Prepared Statements), валидация входных данных и объектно-реляционное отображение (ORM). Подготовленные выражения исключают возможность внедрения кода в запросы, так как параметры передаются отдельно от структуры SQL-запроса, гарантируя, что все входные данные обрабатываются только как параметры. Валидация входных данных добавляет дополнительный уровень защиты, ограничивая или фильтруя ввод пользователя в соответствии с заданными правилами. ORM-инструменты упрощают процесс разработки, автоматически генерируя SQL-запросы, что снижает вероятность ошибок, связанных с ручным кодированием.

При использовании Prepared Statements обеспечивается высокая надёжность благодаря защите от SQL-инъекций и других угроз безопасности, а также достигается универсальность, поскольку один и тот же подготовленный запрос может применяться для различных типов данных без необходимости переписывания кода. Однако внедрение Prepared Statements в существующий код может потребовать дополнительных усилий. Валидация данных характеризуется простотой реализации и низкими затратами, но она не способна защитить от сложных атак, таких как XSS и CSRF. Наконец, использование ORM упрощает разработку, автоматизирует защиту от SQL-инъекций, однако может привести к потенциальной потере производительности из-за добавления дополнительных уровней абстракции.

Сравнительный анализ этих подходов показал, что подготовленные выражения являются наиболее надёжным методом предотвращения атак. Валидация данных эффективна для защиты от простых атак, но не всегда достаточна в более сложных случаях. ORM-решения облегчают разработку, но могут увеличивать нагрузку на систему и требуют точной настройки, особенно в условиях высокой производительности. Для максимальной защиты рекомендуется использовать комплексный подход, комбинируя несколько методов. Регулярное обновление и патчинг веб-приложения и базы данных также является важной мерой по предотвращению SQL-инъекций [2].

Правильная конфигурация базы данных и использование безопасных протоколов аутентификации также являются важными мерами по предотвращению SQL-инъекций [5].

Список литературы

1. Котенко, И.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров / Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. // Вопросы кибербезопасности. 2018. № 3 (27). С. 29-38.
2. Красов, А.В. Обеспечение безопасности передачи multicast-трафика в ip-сетях / Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П.// Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.
3. Сахаров Д.В., Левин М.В., Фостач Е.С., Виткова Л.А. "Исследование механизмов обеспечения защищённого доступа к данным, размещённым в облачной инфраструктуре" // Научно-технические исследования в космических исследованиях Земли, 2017. Т. 9. № 2. С. 40–46.
4. Сахаров Д.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В. // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.
5. Штеренберг С.И. Синхронизированное использование систем защиты информации для контроля учёта рабочего времени / Штеренберг С.И., Щеголева Д.И., Виноградова О.М. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 3-8.

References

1. Kotenko, I.V. An integrated approach to ensuring the security of cyber-physical systems based on microcontrollers / Kotenko I.V., Levshun D.S., Chechulin A.A., Ushakov I.A., Krasov A.V. // Issues of cybersecurity. 2018. No. 3 (27). pp. 29-38.
 2. Krasov, A.V. Ensuring the security of multicast traffic transmission in IP networks / Krasov A.V., Sakharov D.V., Ushakov I.A., Losin E.P.// Information protection. Inside. 2017. No. 3 (75). pp. 34-42.
 3. Sakharov D.V., Levin M.V., Fostach E.S., Tsvetkova L.A. "Research of mechanisms for ensuring secure access to data hosted in cloud infrastructure" // High-tech technologies in Earth space research, 2017. Vol. 9. No. 2. pp. 40-46.
 4. Sakharov D.V. Modeling of a secure scalable enterprise network with dynamic routing based on IPv6 / Sakharov D.V., Krasov A.V., Ushakov I.A., Birikh E.V. // Information Protection. Insider 2020. No. 1 (91). pp. 51-57.
 5. Shterenberg S.I. Synchronized use of information security systems for monitoring working hours / Shterenberg S.I., Shchegoleva D.I., Vinogradova O.M. // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2019. No. 4. pp. 3-8.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.023

АНАЛИЗ ПОПУЛЯРНЫХ В НАСТОЯЩЕЕ ВРЕМЯ ТЕХНОЛОГИЙ ФРОНТЕНД-ФРЕЙМВОРКОВ

¹Ван Цинь, ²Ма Буюнь, ³Чжао Шиюй, ⁴Ли Цзымин

^{1,2,4}ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ (ИТМО)", Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: ¹ wang.qin_001@foxmail.com

³ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. А. И. ГЕРЦЕНА", Санкт-Петербург, Россия (191186, город Санкт-Петербург, наб. Реки Мойки, д.48)

Предметом исследования являются популярные фронтенд-фреймворки для веб-разработки: AngularJS, React и Vue.js. Объект исследования — возможности и особенности применения данных фреймворков при создании интерактивных одностраничных приложений (SPA). В исследовании применялись методы анализа и сравнения функциональных возможностей этих фреймворков. Рассматриваются такие аспекты, как двусторонняя привязка данных, компонентная структура, производительность, а также прогрессивный подход к разработке. Основными выводами являются определение подходящих областей применения для каждого фреймворка: AngularJS для двусторонней привязки данных, React для высокопроизводительных приложений, а Vue.js для гибких и простых решений. Вкладом автора является сравнительный анализ, позволяющий разработчикам выбрать наиболее подходящий инструмент для их задач.

Ключевые слова: Фронтенд-фреймворк, AngularJS, React, Vue.js, одностраничное приложение, двусторонняя привязка данных, компонентная структура, производительность.

ANALYSIS OF CURRENTLY POPULAR FRONT-END FRAMEWORK TECHNOLOGIES

¹ Wang Qin, ² Ma Buoni, ³ Zhang Shiyu, ⁴ Li Zimin

^{1,2,4} NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS (ITMO), St. Petersburg, Russia (197101, St. Petersburg, Kronverkskiy pr-kt, 49), e-mail: ¹ wang.qin_001@foxmail.com

³ "RUSSIAN STATE PEDAGOGICAL UNIVERSITY". A. I. HERZEN", St. Petersburg, Russia (191186, St. Petersburg, Moika River Embankment, 48)

The subject of the research is popular frontend frameworks for web development: AngularJS, React and Vue.js. The object of the research is the capabilities and features of using these frameworks in creating interactive single-page applications (SPA). The study used methods for analyzing and comparing the functionality of these frameworks. Such aspects as two-way data binding, component structure, performance, and a progressive approach to development are considered. The main conclusions are the definition of suitable areas of application for each framework: AngularJS for two-way data binding, React for high-performance applications, and Vue.js for flexible and simple solutions. The author's contribution is a comparative analysis that allows developers to choose the most suitable tool for their tasks.

Keywords: Frontend framework, AngularJS, React, Vue.js, single page application, two-way data binding, component structure, performance.

На заре веб-разработки отображение страниц полностью контролировалось внутренними PHP и JSP. Появление технологии Ajax принесло пользователям новый опыт. Внешняя и внутренняя части взаимодействуют через интерфейс Ajax, и разделение труда постепенно становится ясным. Благодаря инновациям технологии JavaScript на стороне браузера заменяет серверный. боковые страницы JSP, которые могут полагаться на JavaScript Он обрабатывает сложную бизнес-логику во внешнем интерфейсе, но сложность кода по-прежнему высока, Поэтому, чтобы повысить эффективность разработки, упростить код и облегчить последующее обслуживание, были разработаны следующие библиотеки front-end framework [1]. В этой статье они будут подробно проанализированы и сравнены.

Фреймворк AngularJS — это фреймворк MVVM, выпущенный Google в 2009 году. Он имеет такие функции, как двусторонняя привязка данных, модульность, внедрение зависимостей, компоненты, конвейеры и драйверы шаблонов. В AngularJS модель и модель представления взаимодействуют через объект \$scope, а модель не содержит связанной логики. Получайте данные на стороне сервера через \$http и полагайтесь на зависимости модулей для обеспечения совместного использования данных. Кроме того, AngularJS содержит множество встроенных инструкций, которые могут уменьшить объем кода и реализовать тележки для покупок, списки продуктов и т. Д.[2]. Пользовательские инструкции и службы эффективно улучшают возможность повторного использования кода. Кроме того, поскольку jQuery Lite встроен внутрь, моделью представления легко управлять с помощью JavaScript. Для событий взаимодействия с пользователем используется логика поведения \$scope для изменения модели через модель представления и «механизм грязной проверки» \$scope обновляется до View, а затем реализуется разделение представления и модели.

AngularJS предоставляет следующие удобства для разработчиков программ: связывание данных приложения с элементами HTML, клонирование и повторение элементов HTML, скрывание и отображение элементов HTML, добавление кода за элементами HTML, поддержка проверки ввода[3].

Фреймворк React был разработан внутренней командой FaceBook и был открыт в мае 2013 года. После появления React его функции, такие как одностраничные приложения, виртуальный DOM, высокая производительность, компонентизация и односторонний поток данных, подорвали всю область фронтенда. Все страницы, упомянутые в React, состоят из компонентов, а логика реализации динамически генерируется JS. Компонентная конструкция также полностью отражает низкую производительность соединения и максимально увеличивает возможность повторного использования.

В React принят принцип виртуального DOM. Элементы, нарисованные синтаксисом JSX, представляют собой просто структуру данных, похожую на DOM, а не реальный DOM. Этот принцип значительно снижает рабочую частоту узлов DOM и оптимизирует производительность. Кроме того, поток данных в React это односторонне, и данные передаются слой за слоем через свойства и состояние компонента. Если вы хотите добавить обратный поток данных, вам нужно передать функцию обратного вызова дочернему компоненту через родительский компонент. Всякий раз, когда состояние обновляется, запускается обратный вызов, и родительский компонент вызывает setState для повторного рендеринга страницы.

Выпущенный в 2014 году, Vue.js является дружелюбным, универсальным и высокопроизводительным фреймворком JavaScript, который использует паттерн MVVM. Это может помочь создать более удобный и тестируемый код, и в настоящее время это фреймворк с самой мягкой кривой обучения среди всех основных фреймворков. Vue.js является прогрессивным. Так называемый прогрессивный относится к многоуровневости фреймворка. Основной частью является рендеринг уровня представления, а внешней последовательностью является компонентный механизм, механизм маршрутизации, управление состоянием и инструменты построения. Vue.js обладает достаточной гибкостью, чтобы адаптироваться к различным потребностям. Помимо введения виртуального DOM, он также обеспечивает поддержку JSX и TypeScript, поддерживает потоковую отрисовку на стороне сервера и обеспечивает кросс-платформенные возможности. Он очень подходит для создания подобных веб-сайтов. версия Quora Этот тип веб-приложения имеет множество элементов формы, и его содержимое необходимо изменять в соответствии с действиями пользователя.

Фреймворк Vue.js имеет много общего с фреймворком Angular.js, например, двусторонняя привязка данных, инструкции, маршрутизация и т. д. позволяют разрабатывать одностраничные приложения. Однако методы реализации двусторонней привязки данных различны. Из-за грязного механизма проверки Angular. Гораздо быстрее, пока обнаруживаются изменения данных, представление будет обновляться, особенно когда данные увеличиваются, преимущества фреймворка Vue.js более очевидны.

По сравнению с платформой React, платформа Vue.js использует виртуальную модель DOM, предоставляет адаптивные и компонентные компоненты представления, фокусируется на основной библиотеке и оставляет другие функции, такие как маршрутизация и управление глобальным состоянием, связанной библиотеке. Разница между Vue и React заключается в следующем:

1. Изменения в компонентах React приведут к повторному рендерингу всего поддерева компонентов, в то время как система Vue может определить конкретные компоненты, которые необходимо визуализировать, и разработчикам не нужно учитывать оптимизацию рендеринга компонентов;
2. Все в React — это JavaScript, и функции рендеринга всех компонентов основаны на JSX, а Vue.js имеет собственную функцию рендеринга, поддерживает JSX и может использовать официально рекомендованный шаблон для рендеринга представления;
3. React реализует область видимости CSS через решение CSS-in-JS, а Vue.js реализуется путем добавления тега области действия к тегу стиля;
4. Библиотека маршрутизации React и библиотека управления состоянием поддерживаются сообществом, а Vue.js Библиотека маршрутизации js и библиотека управления состоянием официально поддерживаются и поддерживают синхронные обновления с основной библиотекой.

Ранний веб-интерфейс в основном состоял из трех частей: HTML, CSS и JavaScript, среди которых HTML в основном отвечал за структуру страницы, CSS в основном отвечал за стиль страницы, а JavaScript в основном контролировал поведение страницы и взаимодействие с пользователем. терминальная реализация. С быстрым развитием веб-приложений функциональность интерфейса становится все сильнее и сильнее, а сложность разработки

постепенно увеличивается. Появление большого количества отличных интерфейсных фреймворков способствовало развитию интерфейсных технологий, снижению затрат на разработку и повышению эффективности разработки. Оригинальный фреймворк JavaScript jQuery занимает доминирующее положение благодаря удобным DOM-операциям, поддержке выбора компонентов и внутренней инкапсуляции Ajax-операций[4]. Однако с дальнейшим развитием внешнего интерфейса использование jQuery для разработки веб-приложений не может разделить бизнес-логику, логику взаимодействия и дизайн пользовательского интерфейса, что увеличивает сложность обслуживания кода. Появление шаблона проектирования MVVM реализует автоматическую привязку данных и представлений, отделяет операцию DOM от бизнес-кода и повышает удобство сопровождения и повторное использование кода.

Благодарности: Я хотел бы выразить свою благодарность Китайскому комитету по делам образования (CSC) за предоставленную финансовую поддержку. Также благодарю моего научного руководителя Быковского Сергея Вячеславовича за его ценное руководство и поддержку.

Список литературы

1. Xu Pengtao. Design and implementation of front-end development framework based on Vue[D]. Jinan: Shandong University, 2020: 17.
2. Shiming. Research on Web mainstream front-end development framework[J]. information recording materials, 2020, 21(5): pp.215-216.
3. Novac O C, Madar D E, Novac C M, et al. Comparative study of some applications made in the Angular and Vue. js frameworks[C]//2021 16th International Conference on Engineering of Modern Electric Systems (EMES). IEEE, 2021: pp.1-4.
4. Nasution A B, Rustam M T. Practical Workshop on How to Build Attendance Applications with jQuery, JavaScript and AJAX[J]. Indonesian Journal of Advanced Social Works, 2023, 2(3): pp.165-172.

References

1. Xu Ping tao. Design and implementation of front-end development framework based on Vue[D]. Jinan: Shandong University, 2020: 17.
 2. Shiming. Research on Web mainstream front-end development framework[J]. information recording materials, 2020, 21(5): pp.215-216.
 3. Nova cOC, Madar D E, Novak C M, et al. Comparative study of some applications made in the Angular and Vue. js frameworks[C]//2021 16th International Conference on Engineering of Modern Electric Systems (EMES). IEEE, 2021: pp. 1-4.
 4. Nasution A B, Rustam T. Practical Workshop on How to Build Attendance Applications with jQuery, JavaScript and AJAX[J]. Indonesian Journal of Advanced Social Works, 2023, 2(3): pp.165-172.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

СКРЫТЫЕ РИСКИ МАССОВЫХ ОБНОВЛЕНИЙ ДАННЫХ: КАК ИЗБЕЖАТЬ ПОТЕРИ И УТЕЧКИ ИНФОРМАЦИИ

Поляков 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:
artpol2001@gmail.com

Массовые обновления данных играют важную роль в поддержании актуальности информации в крупных компаниях и организациях. Однако такие процессы могут сопровождаться рисками, связанными с потерей данных, нарушением целостности и утечками информации. В статье рассматриваются основные скрытые угрозы, возникающие при массовых обновлениях данных, а также предлагаются методы защиты, такие как управление правами доступа, резервное копирование и проверка целостности данных, чтобы минимизировать риски.

Ключевые слова: Массовое обновление данных, утечка информации, потеря данных, безопасность, резервное копирование, управление доступом, целостность данных.

HIDDEN RISKS OF MASS DATA UPDATES: HOW TO PREVENT DATA LOSS AND LEAKS

Polyakov 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: artpol2001@gmail.com

Mass data updates are crucial for keeping information current in large companies and organizations. However, these processes can carry risks, such as data loss, integrity violations, and information leaks. The article examines the main hidden threats associated with mass data updates and offers protection methods, including access management, data backup, and integrity checks, to mitigate risks.

Keywords: mass data updates, data leakage, data loss, security, backup, access management, data integrity.

Введение

В эпоху цифровой трансформации массовые обновления данных стали необходимостью для организаций, стремящихся поддерживать актуальность и точность информации. Эти процессы, затрагивающие огромные объёмы данных, часто включают модификацию, удаление или добавление записей, что помогает компаниям оставаться конкурентоспособными и соответствовать постоянно меняющимся бизнес-требованиям. Однако масштабные изменения данных нередко сопряжены с рисками, которые могут привести к нарушению конфиденциальности, потере данных или их повреждению.

Риски, возникающие при массовых обновлениях, зачастую остаются незамеченными, особенно когда процесс плохо управляется или недостаточно защищён. Эти угрозы могут быть связаны с несанкционированным доступом, ошибками персонала или техническими

сбоями. Без соответствующих мер безопасности последствия могут быть серьёзными: от утраты критически важной информации до утечек, способных нанести значительный вред репутации компании. Введение в процесс обновления надёжных методов управления, таких как контроль доступа, автоматическое резервное копирование и регулярные проверки целостности, поможет снизить риск потерь и утечек данных, что становится всё более актуальным в условиях возросших требований к безопасности.

Скрытые риски массовых обновлений данных

Массовое обновление данных — это процесс, который требует тщательной координации и надёжного управления, поскольку даже минимальная ошибка может привести к серьёзным последствиям. Например, если на этапе обновления будет нарушена целостность данных, это способно негативно отразиться на работе всех зависимых систем. В случае массовых обновлений в базе данных ошибка в одной записи может распространиться на тысячи других, вызывая проблемы с обработкой транзакций, выводом отчётности и даже влияя на аналитические данные, что, в свою очередь, может привести к принятию ошибочных бизнес-решений[1].

Одна из серьёзных угроз при массовых обновлениях — это риск потери данных. Потеря информации может произойти как из-за случайных ошибок, так и из-за недосмотра сотрудников, а также из-за технических проблем, таких как сбой в работе серверов или сетевые неполадки. В случае отсутствия актуальных резервных копий восстановление данных может стать крайне трудоёмким процессом или даже невозможным. Чтобы избежать подобных проблем, компании должны использовать продуманные стратегии резервного копирования, включая создание дублирующих копий данных перед началом массового обновления. Эти резервные копии необходимо хранить в надёжном месте и периодически проверять на соответствие актуальному состоянию данных[2].

Другой важный аспект защиты данных при массовых обновлениях — это управление доступом. Не все сотрудники должны иметь возможность изменять или удалять данные, и ограничение прав доступа в зависимости от должностных обязанностей является важным шагом для предотвращения несанкционированного вмешательства. Использование ролевой модели управления доступом помогает контролировать, кто именно может вносить изменения, снижая риск случайных ошибок и потенциальных утечек. При этом, чем больше людей имеют доступ к данным, тем выше вероятность ошибки или преднамеренного нарушения безопасности. В дополнение к этому, рекомендуется использовать двухфакторную аутентификацию и регистрацию всех действий, связанных с изменениями данных, что позволит отслеживать каждый шаг процесса и оперативно выявлять подозрительные активности[3].

Помимо угроз потери данных и нарушений доступа, массовое обновление может представлять риск для конфиденциальности информации. В случае ошибки при обновлении чувствительная информация может быть случайно отправлена в неподходящее место, что приведёт к утечке данных и возможным юридическим последствиям. Этого можно избежать, используя проверенные и надёжные методы шифрования данных, что особенно важно при обработке персональных и финансовых данных. Дополнительно, компании могут внедрить протоколы безопасности, которые будут обеспечивать автоматическое сканирование на

наличие ошибок и недопустимых изменений перед финальным обновлением данных в системе[4].

Для обеспечения целостности данных также необходимо проводить регулярные проверки и тестирование на контрольных средах. Это позволит своевременно выявить и устранить ошибки до того, как они нанесут серьёзный ущерб. Кроме того, перед каждым обновлением необходимо провести тестовые испытания на отдельном сервере, чтобы убедиться, что процесс обновления не создаст конфликтов в системе. Таким образом, компании могут минимизировать риски, связанные с массовыми изменениями, и предотвратить сбои, которые могут нарушить рабочие процессы и привести к финансовым потерям[5].

Многие компании всё ещё недооценивают важность регулярных проверок и анализа данных после массовых обновлений. Эти проверки должны проводиться автоматически, чтобы сравнивать состояния данных до и после обновления. Если выявлены какие-либо отклонения или несовпадения, процесс может быть остановлен до тех пор, пока проблема не будет решена. Эти меры контроля помогут сохранить целостность данных и предотвратить возможные утечки. Кроме того, автоматизация процессов обновления и мониторинга данных также играет ключевую роль в снижении риска человеческих ошибок и повышении эффективности системы безопасности.

Заключение

Массовое обновление данных — это сложный и многогранный процесс, сопряжённый с рядом скрытых угроз, таких как потеря данных, утечка информации и нарушение целостности. Для минимизации этих рисков компаниям необходимо внедрять надёжные системы управления данными, использовать продуманные протоколы резервного копирования и шифрования, а также контролировать доступ на основе должностных обязанностей. Введение регулярных проверок целостности данных и тестирования обновлений на контрольных серверах перед массовым применением поможет предотвратить крупные сбои и минимизировать вероятность утечек.

Эффективная защита данных требует систематического подхода, который учитывает все этапы процесса обновления, от подготовки до завершения. В условиях, когда утечки и потери данных могут нанести серьёзный ущерб компании, внедрение комплексной стратегии защиты данных становится критически важным. Массовые обновления данных могут быть выполнены безопасно только при условии, что компании обеспечат высокий уровень контроля и защиты, что позволит избежать множества потенциальных проблем и защитить конфиденциальные данные от потерь и утечек.

Список литературы

1. Свидетельство о государственной регистрации программы для ЭВМ № 2020664289 РФ. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV : № 2020663625 : заявл. 03.11.2020 : опубл. 11.11.2020 / И.Е.Пестов, А.М.Гельфанд, Н.Н.Лансере, И.И.Фадеев, заявитель ФГБОУ ВО «С-Пб-кий гос.университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN PKSCLB.

2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. 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. Пестов И. Е. МЕТОДИКА АВТОМАТИЗИРОВАННОГО ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ НА ИНСТАНСЫ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ БЕЗАГЕНТНОГО МЕТОДА СБОРА МЕТРИК.
5. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.

References

1. Certificate of state registration of the computer program No. 2020664289 Russian Federation. The program for providing a computer vision system based on the OpenCV library : No. 2020663625 : application 03.11.2020 : publ. 11.11.2020 / I. E. Pestov, A.M. Gelfand, N. N. Lancere, I.I. Fadeev ; applicant Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch- Bruevich." – EDN PKSCLB.
 2. Lesnova E. M., Pestov I. E. Development of a method of error detection and correction for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
 3. 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. – No. 4. – pp. 72-76.
 4. Pestov I. E. METHOD OF AUTOMATED COUNTERACTION TO UNAUTHORIZED IMPACTS ON CLOUD INFRASTRUCTURE INSTANCES USING AN AGENTLESS METHOD OF COLLECTING METRICS.
 5. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.43

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ 1С С ИСПОЛЬЗОВАНИЕМ REACT NATIVE

Сушко А.В.

ФГБОУ ВО «КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ И.Т. ТРУБИЛИНА», Краснодар, Россия (350044, Краснодарский край, город Краснодар, ул. им. Калинина, д.13), e-mail: mail@kubsau.ru

В данной статье рассматривается разработка мобильных приложений 1С с помощью React Native – кроссплатформенного фреймворка, который предоставляет возможности для создания современных, производительных и гибких приложений. Рассматриваются преимущества React Native, архитектурные решения для взаимодействия 1С, этапы разработки и примеры применения мобильных приложений 1С, разработанных с помощью React Native.

Ключевые слова: Мобильная разработка, 1С, React Native, кроссплатформенная разработка, мобильная платформа, разработчики, приложения.

DEVELOPMENT OF A 1C MOBILE APPLICATION USING REACT NATIVE

Sushko A.V.

"KUBAN STATE AGRARIAN UNIVERSITY NAMED AFTER I.T. TRUBILIN", Krasnodar, Russia (350044, Krasnodar region, Krasnodar city, Kalinina street, 13), e-mail: mail@kubsau.ru

This article discusses the development of 1C mobile applications using React native, a cross-platform framework that provides opportunities to create modern, productive and flexible applications. The advantages of React Native, architectural solutions for 1C interaction, development stages and examples of application of 1C mobile applications developed using Re-act Native are considered.

Keywords: Mobile development, 1C, React Native, cross-platform development, mobile platform, developers, applications.

В современном мире мобильные приложения играют главную и ключевую роль, позволяя компаниям быть более гибкими, доступными и эффективными. Учитывая данный тренд, разработчики 1С стремятся расширить свои возможности и узнать, как создавать адаптированные решения для мобильных устройств.

Для удобства интеграции с системами, которые есть в 1С используется платформа для разработки приложений в 1С. Однако, с развитием технологий и ростом популярности кроссплатформенных решений, таких как React Native, открываются новые возможности для разработчиков.

Разберем более подробно ключевые ограничения мобильной платформы 1С, которые могут существенно препятствовать разработке высококачественных и современных мобильных приложений.

1. Негибкость: стандартный дизайн и ограниченная функциональность.

Мобильная платформа 1С предлагает ограниченный набор стандартных компонентов и визуальных стилей, что может быть недостаточным для создания приложений с уникальным

пользовательским опытом. Нестандартные элементы дизайна и удобства интерфейса требует больших усилий, а компоненты платформы, которые созданы для создания более простых стилей усложняют и ограничивают работу.

2. Низкая производительность: снижение скорости и отзывчивости.

Приложения, которые разработаны на мобильной платформе 1С, могут отличаться невысокой скоростью работы и отзывчивостью, особенно это касается устройств с ограниченными ресурсами, такими как старые модели смартфонов или планшеты с небольшим объемом оперативной памяти. Это обусловлено особенностями архитектуры платформы, которые не всегда качественно работают на современных мобильных устройствах. В итоге приложения могут демонстрировать низкую производительность, что достаточно отрицательно сказывается на пользовательском опыте.

3. Ограниченная экосистема: недостаток доступных библиотек и инструментов для расширения функциональности приложения.

Мобильная платформа 1С обладает минимальным количеством готовых библиотек и инструментов. В результате чего это приводит к ограниченному использованию и невозможности расширения функций мобильных приложений. Частая необходимость разработчиков – создавать собственные решения для реализации специфических функций, что приводит к увеличению времени разработки, а также повышению затрат.

4. Высокие затраты: дополнительные расходы на разработку.

Создание приложений на мобильной платформе 1С достаточно дорогостоящая и требует дополнительных ресурсов, особенно при необходимости разработки отдельных версий для IOS и Android. Это объяснимо тем, что отдельные процессы разработки для каждой платформы, требуют еще больше вложений на тестирование и поддержку. [3]

Рассмотрим, что такое React Native? React Native – это фреймворк для создания мобильных приложений, который основан на языке программирования JavaScript и использует React как свою основную библиотеку. Он предоставляет возможность разработчикам разрабатывать приложения с уникальным интерфейсом, который визуально воспринимается и функционирует как нативное приложение для IOS и Android.

Мы можем наблюдать, что с появлением кроссплатформенных фреймворков, таких как React Native, у разработчиков появилась возможность создавать приложения 1С без использования платформы, получая ряд преимуществ.

- Повышенная производительность.

React Native предоставляет возможность использовать нативные компоненты, обеспечивая высокую скорость и отзывчивость приложения. Нативные компоненты – элементы интерфейса, которые написаны на языке программирования, специфичном для конкретной операционной системы (IOS или Android).

- Снижение стоимости.

React Native позволяет использовать единый код для IOS и Android, сокращая время разработки и затраты.

- Широкая экосистема.

React Native предлагает доступ к обширному набору готовых библиотек и инструментов, которые могут быть использованы для расширения функциональных возможностей приложения.

- Гибкость.

React Native предоставляет гораздо большую свободу в дизайне и возможностях приложения в сравнении с мобильной платформой 1С. [4]

При разработке мобильного приложения 1Сс помощью React Native существует возможность применять некоторые архитектурные подходы:

- RESTAPI: приложения взаимодействуют с сервером 1С через RESTAPI, используя HTTP и HTTPSзапросы для обмена данными. Это позволяет использовать стандартные методы авторизации и аутентификации.
- WebSockets: для более быстрого обмена данными используют WebSockets. Обеспечивает двустороннюю связь между приложениями и сервером 1С в режиме реального времени.
- GraphQL: для запросов к серверу 1С используют GraphQL. Он позволяет определить конкретный набор данных, необходимых для запроса, оптимизируя трафик и повышая скорость работы.

Рассмотрим этапы разработки мобильного приложения для мобильной платформы 1С с помощью React Native.

1. Настройка среды разработки.
 - Установка Node.js и npm: базовая среда для React Native.
 - Создание нового проекта: *create-react-native-app* используется для быстрой генерации проекта.
 - Настройка проекта: установка зависимостей, конфигурация для используемой архитектуры (REACTAPI, WebSockets, GraphQL).
2. Реализация макета интерфейса.
 - Использование компонентов: React Native предоставляет широкий набор компонентов для создания пользовательского интерфейса.
 - Стиль и анимации: CSS и JavaScript используется для придания приложению уникального вида и динамики.
 - Навигация: React Natvigation обеспечивает надежную и интуитивно понятную навигацию между экранами.
3. Настройка взаимодействия с сервером 1С.
 - РеализацияAPI на стороне сервера.
 - Функции для обмена данными: написание функций для получения, отправки и обновления данных из базы данных 1С.
4. Тестирование и развертывание.
 - Внутреннее тестирование: проверка функциональности, производительности и работы на разных устройствах.
 - Передача заказчику: демонстрация функционала, проведение приемочного тестирования.

Разберем как React Native расширяет возможности бизнеса и открывает новые горизонты. Примеры применения:

- Мобильные приложения для складского учета. Позволяют просматривать и обновлять информацию о товарах, отслеживать перемещение на складе, а также оформлять заказы.

- Мобильные приложения для управления продажами. Дают возможность принимать заказы от клиентов, отслеживать статусы заказов, работать с клиентской базой.
- Мобильные приложения для персонала. Предоставляют доступ к просмотру расписания, запись на отпуск, просмотр информации о зарплате.

В заключение важно отметить, что создание мобильных приложений для 1С с использованием React Native представляет собой не только актуальное, но еще эффективное и перспективное решение, что помогает существенно сократить время и затраты на разработку. Это позволяет создавать современные и легко адаптируемые мобильные приложения с большим количеством возможностей, которые обеспечивают высокую производительность и гибкость. React Native улучшает пользовательский опыт, а также предоставляет разработчикам 1С необходимые инструменты для расширения своих возможностей и создания оригинальных мобильных приложений.

Список литературы

1. Кондратьев В.Ю., Кондратьев С.В. Информационное обеспечение системы управления агропромышленным предприятием в растениеводстве // В сборнике: Научное обеспечение агропромышленного комплекса. Сборник статей по материалам IX Всероссийской конференции молодых ученых. Ответственный за выпуск: А.Г. Коцаев. – 2016. – С. 267-269.
2. Кондратьев В.Ю., Плотников В.В. Информационное обеспечение системы управления агропромышленным предприятием, подсистема расчетов с поставщиками и покупателями // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2005.- № 12. - С. 37-47.
3. Хрусталева Е. Ю. Знакомство с разработкой мобильных приложений на платформе «1С:Предприятие 8» [Текст] / Е. Ю. Хрусталева — Издание 3. — 2022 — 276 с.
4. [Электронный ресурс] // ReactNative: [сайт]. — URL: <https://reactnative.dev/>

References

1. Kondratiev V.Yu., Kondratiev S.V. Information support of the agro-industrial enterprise management system in plant production. Collection of articles based on the materials of the IX All-Russian Conference of Young Scientists. Responsible for the issue: A.G. Koshchayev. – 2016. – pp. 267-269.
 2. Kondratiev V.Yu., Plotnikov V.V. Information support of the agro-industrial enterprise management system, subsystem of settlements with suppliers and buyers. – 2005.- № 12. - pp. 37-47.
 3. Khrustaleva E. Y. Acquaintance with the development of mobile applications on the platform "1C: Enterprise 8" [Text] / E. Y. Khrustaleva — Edition 3. — 2022 — P. 276.
 4. [Electronic resource] // ReactNative: [site]. — URL: <https://reactnative.dev/>
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.8

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ REST И gRPC ПОДХОДОВ ОБМЕНА ДАННЫХ

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

В статье рассматривается сравнение производительности нескольких подходов по взаимодействию с микросервисами: REST и gRPC. Основными различиями между двумя подходами являются: REST – просто в понимании и популярен при взаимодействии между клиентской и серверной части интернет-сервисов среди разработчиков, при обмене данных используется гибкий JSON формат. gRPC – альтернативный подход к обмену данных, имеет ряд особенностей: передача данных происходит в бинарном формате, необходимо заранее описывать контракты для обмена данными в Protocol Buffers, чаще всего данный подход используется при взаимодействии между микросервисами, но также он может применяться при обмене данных между клиентской и серверной частями в интернет сервисах.

Ключевые слова: Передача данных, REST, gRPC, тестирование, производительность, нагрузка.

COMPARATIVE ANALYSIS OF THE PERFORMANCE OF REST AND gRPC DATA EXCHANGE APPROACHES

Nikitin A.A.

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

The article discusses a comparison of the performance of several approaches for interacting with micro-services: REST and gRPC. The main differences between the two approaches are: REST is easy to understand and is popular among developers when interacting between the client and server parts of Internet services, and a flexible JSON format is used for data exchange. gRPC is an alternative approach to data exchange, it has a number of features: data transfer takes place in binary format, it is necessary to describe contracts for data exchange in Protocol Buffers in advance, most often this approach is used when interacting between microservices, but it can also be used when exchanging data between client and server parts in Internet services.

Keywords: Data transfer, REST, gRPC, testing, performance, load.

При проектировании различных интернет-сервисов встает вопрос о выборе подхода обмена данными между клиентской и серверной частями или между узлами в микросервисной архитектуре. Среди популярных подходов необходимо выделить два популярных: REST и gRPC.

Главными различиями между данными подходами обмена данных выделяют:

- формат данных: REST – текстовые форматы JSON, XML, gRPC – бинарный формат protobuf;
- протоколы: REST работает поверх HTTP/1.1, а gRPC поверх HTTP/2;

- потоковая передача данных: gRPC поддерживает двустороннюю потоковую передачу с помощью стриминга данных, в то время как REST требует для этого дополнительных решений, например, веб-сокеты;
- типизация: gRPC строго типизирован с использованием protobuf, REST более гибкий в формате данных.

Из основных особенностей каждого из подходов вытекает разность в производительности:

- бинарный формат передачи данных в HTTP/2 производительнее, чем JSON в HTTP/1.1, связано это с оптимизацией передачи данных, а также передачей в бинарном формате, который использует меньший объем данных, чем при передаче JSON;
- В HTTP/2 оптимизирован процесс передачи заголовков, а именно используется механизм сжатия заголовков, в HTTP/1.1 каждый запрос и ответ содержит заголовки, которые повторяются при каждом новом соединении;
- HTTP/2 поддерживает мультиплексирование, то есть несколько потоков для передачи данных в рамках одного соединения. Это приводит к уменьшению задержек.

В качестве тестового сервиса для производительности была выбрана образовательная платформа для изучения различных материалов в авиации [1, 2]. На данной платформе есть два микросервиса, написанных на языке программирования (ЯП) go: первый микросервис – авторизация, аутентификация, регистрация и получение пользователей, второй - размещение и работа с курсами. Для каждого микросервиса поддерживается два подхода: REST с помощью фреймворка gin и gRPC с помощью стандартного фреймворка для Go. Также был выбран ПК с процессором Intel(R) Core(TM) i7-8565U и оперативной памятью 16 ГБ DDR4-2400 МГц, ОС – windows 11 pro.

Существует множество различных технологий для тестирования производительности системы, среди таких выделяют:

- тестирование при помощи стандартной библиотеки: для go – testing;
- тестирование при помощи нагрузочной технологии pandora [3, 4];
- тестирование при помощи нагрузочной технологии k6 [5];

Каждая технология для тестирования является уникальной: *k6* имеет простое написание тестов на javascript, простую установку и запуск, *pandora* является более устойчивой, описание тестов поддерживается на go, данные технологии имеют поддержку REST и gRPC. Тестирование при помощи стандартной библиотеки является важным аспектом при разработки любого интернет-сервиса, является простым в написании и легко поддерживаемым.

Тесты для сравнения производительности проводились по следующему сценарию: регистрация и получение пользователей из базы данных при помощи пользовательского микросервиса образовательной платформы (Таблица 1, Рисунок 1);

Таблица 1 - Результаты тестирования для стандартной библиотеки, k6, pandora:

| Технология | Обмен данных | Тип метода | Действие | Среднее время, мкс | Отношение среднего время запросов REST и GRPC |
|------------------------|--------------|------------|-----------------------------|--------------------|---|
| стандартная библиотека | REST | POST | регистрация | 138,95 | 1,66 |
| | gRPC | | | 78,82 | |
| | REST | GET | получить всех пользователей | 276,47 | |
| | gRPC | | | 171,20 | |
| k6 | REST | POST | регистрация | 158,95 | 1,54 |
| | gRPC | | | 108,82 | |
| | REST | GET | получить всех пользователей | 132,82 | |
| | gRPC | | | 85,75 | |
| pandora | REST | POST | регистрация | 167,59 | 1,89 |
| | gRPC | | | 83,94 | |
| | REST | GET | получить всех пользователей | 187,59 | |
| | gRPC | | | 103,94 | |

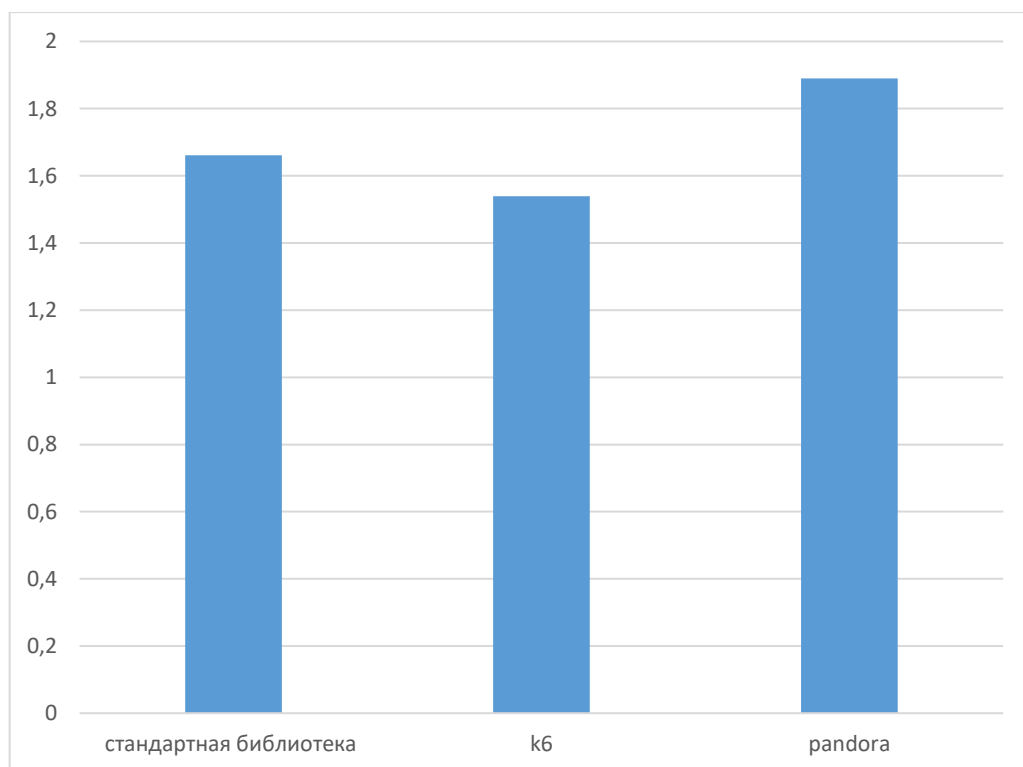


Рисунок 1.- Отношение производительности REST и GRPC.

Отношение производительности рассчитывалось как: отношение среднего значения ответа от микросервиса в микросекундах REST подхода к среднему значению ответа gRPC подходу.

В популярной работе Рувана Фернандо [6] по сравнению gRPC и REST подхода видно, что по ряду тестов gRPC опережает по производительности REST. В работе сделан вывод, gRPC примерно в семь раз быстрее REST при получении данных и в десять при отправке. В основном это связано с плотной упаковкой Protocol Buffers и использованием HTTP/2 для gRPC.

Таким образом, при проектировании интернет-сервисов стоит отдавать предпочтение gRPC для повышения производительности. gRPC значительно опережает REST по времени отклика за счет таких особенностей, как использование бинарного формата Protocol Buffers и протокола HTTP/2, который обеспечивает сжатие заголовков, мультиплексирование потоков и более эффективную передачу данных. Это делает gRPC предпочтительным решением для высоконагруженных систем и микросервисных архитектур.

Однако выбор технологии зависит от множества факторов. REST, несмотря на относительно низкую производительность, остается популярным благодаря простоте и гибкости. Он предоставляет возможность работы с текстовыми форматами JSON и XML, а также легко интегрируется с большинством современных фреймворков и библиотек. REST может быть более удобным для взаимодействия клиент-сервер и разработки прототипов, где высокая производительность не является критически важным требованием.

Вместе с тем, результаты тестирования показывают, что производительность gRPC и REST может значительно варьироваться в зависимости от специфики проекта. Например, при тестировании производительности микросервисов образовательной платформы с использованием баз данных наблюдались дополнительные накладные расходы, такие как конвертация данных и обращение к базе, что снижало общую производительность по сравнению с "чистыми" тестами. Это подтверждает, что в реальных условиях gRPC опережает REST, но разрыв может быть менее выраженным.

Для нагрузочного тестирования рекомендуется использовать такие инструменты, как стандартная библиотека Go, k6 и Pandora. Каждый из них обладает уникальными преимуществами. Стандартная библиотека проста в использовании и подходит для базового тестирования. k6 выделяется благодаря удобству написания тестов на JavaScript и легкости запуска. Pandora, в свою очередь, обеспечивает стабильность и возможность писать тесты на Go, что делает ее удобной для сложных сценариев. Эти инструменты позволяют разработчикам гибко подходить к тестированию производительности, обеспечивая более глубокое понимание особенностей работы REST и gRPC подходов для обмена данными.

В заключение, выбор подхода и инструментов для тестирования должен основываться на требованиях проекта. Если основным приоритетом является производительность, gRPC с его преимуществами станет оптимальным выбором. Если важны простота разработки и универсальность, REST может быть предпочтительным. При этом применение современных инструментов тестирования позволит добиться максимальной эффективности выбранного подхода.

Список литературы

1. Никитин А. А. Архитектура высоконагруженного интернет-сервиса: образовательная платформа для изучения авиационных материалов // 22-я Международная конференция «Авиация и космонавтика». 20-24 ноября 2023 года. Москва. Тезисы; МАИ. - Москва, 2023. - С. 161-162.

2. Никитин А.А. Анализ технологий для реализации образовательной онлайн платформы по материаловедению в авиации // Сборник тезисов работ международной молодежной научной конференции L Гагаринские чтения 2024.; МАИ. - Москва, 2024. - С. 277 -278.
3. Официальный сайт образовательно-новостного ресурса «Habr» - <https://habr.com/ru/companies/ozontech/articles/662800/> (дата обращения 19.10.2024).
4. Официальный сайт образовательно-новостного ресурса «Habr» - <https://habr.com/ru/articles/517488/> (дата обращения 19.10.2024).
5. Официальный сайт образовательно-новостного ресурса «Habr» - <https://habr.com/ru/articles/554266/> (дата обращения 19.10.2024).
6. Официальный сайт образовательно-новостного ресурса «Habr» - <https://habr.com/ru/companies/otus/articles/545688/> (дата обращения 20.09.2024).

References

1. Nikitin A. A. Architecture of a highly loaded Internet service: an educational platform for studying aviation materials // 22nd International Conference "Aviation and Cosmonautics". November 20-24, 2023. Moscow. Abstracts; MAI. - Moscow, 2023. - pp. 161-162.
 2. Nikitin A.A. Analysis of technologies for the implementation of an online educational platform for materials science in aviation // Collection of abstracts of the international youth scientific conference L Gagarin Readings 2024.; MAI. - Moscow, 2024. - pp. 277-278.
 3. The official website of the educational and news resource "Habr" - <https://habr.com/ru/companies/ozontech/articles/662800/> (accessed 19.10.2024).
 4. The official website of the educational and news resource "Habr" - <https://habr.com/ru/articles/517488/> (accessed 19.10.2024).
 5. The official website of the educational and news resource "Habr" - <https://habr.com/ru/articles/554266/> (accessed 19.10.2024).
 6. The official website of the educational and news resource "Habr" - <https://habr.com/ru/companies/otus/articles/545688/> (accessed 09/20/2024).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.736

КАК ЗАЩИТИТЬ JSONB-ПОЛЯ В POSTGRESQL ОТ УТЕЧЕК ДАННЫХ И ИНЪЕКЦИЙ

Ноянов Р.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:
romannoyanov@gmail.com

JSONB-формат в PostgreSQL активно используется для хранения сложных данных, однако его использование сопряжено с рисками утечек и SQL-инъекций. Статья обсуждает основные угрозы безопасности, связанные с использованием JSONB в PostgreSQL, описывает распространённые сценарии атак и предлагает способы защиты, такие как валидация данных, использование параметризованных запросов и конфиденциальное шифрование.

Ключевые слова: PostgreSQL, JSONB, защита, SQL-инъекции, утечки данных, шифрование, валидация.

HOW TO PROTECT JSONB FIELDS IN POSTGRESQL FROM DATA LEAKS AND INJECTIONS

Nayanov R.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: romannoyanov@gmail.com

JSONB format in PostgreSQL is widely used for storing complex data, but its use brings risks of data leaks and SQL injections. The article discusses primary security threats associated with JSONB in PostgreSQL, outlines common attack scenarios, and offers protection methods such as data validation, parameterized queries, and confidential encryption.

Keywords: PostgreSQL, JSONB, security, SQL injections, data leaks, encryption, validation.

Введение

С появлением JSONB в PostgreSQL у разработчиков появилась возможность эффективно хранить и обрабатывать неструктурированные данные в виде JSON, которые часто встречаются в современных приложениях. JSONB предоставляет возможности для хранения сложных структур данных, поиска по ключам и удобной фильтрации, что делает его полезным для работы с динамическими данными, которые сложно хранить в традиционных реляционных таблицах. Однако хранение данных в JSONB имеет и свои риски: из-за особенностей формата и его гибкости JSONB становится потенциальной точкой уязвимости для утечек данных и инъекций, особенно если данные принимаются из внешних источников.

Основные угрозы для JSONB-полей включают SQL-инъекции, утечки конфиденциальных данных и неконтролируемый доступ к данным. Например, JSONB-поля, содержащие данные пользователей, могут быть подвергнуты SQL-инъекциям или

использованы злоумышленниками для получения доступа к конфиденциальной информации. Цель этой статьи — рассмотреть типичные угрозы безопасности, связанные с использованием JSONB в PostgreSQL, и описать способы защиты, которые помогут минимизировать риски. Мы обсудим методы, которые включают параметризацию запросов, шифрование, валидацию данных и настройку прав доступа для обеспечения безопасности JSONB.

Как защитить JSONB-поля в PostgreSQL от утечек данных и инъекций

JSONB, как формат хранения данных в PostgreSQL, предоставляет не только гибкость, но и требует дополнительных мер безопасности. Одной из главных проблем является SQL-инъекция, которая может возникнуть при передаче данных в SQL-запросы напрямую. Так как JSONB позволяет хранить вложенные структуры данных, злоумышленники могут использовать уязвимости в коде для внедрения вредоносных команд в запросы, которые обращаются к JSONB-полям. Это может привести к утечке данных или выполнению непредусмотренных команд в базе данных. Чтобы предотвратить SQL-инъекции, рекомендуется использовать параметризованные запросы, которые исключают возможность передачи вредоносных данных. Параметризация защищает запросы, так как данные обрабатываются как значения, а не как части SQL-кода[1].

Ещё одним важным аспектом защиты JSONB-полей является шифрование данных. В случаях, когда JSONB-поля содержат конфиденциальную информацию, такую как пароли или номера кредитных карт, рекомендуется шифровать данные перед их сохранением. Шифрование позволяет минимизировать риск утечек даже при несанкционированном доступе к базе данных. В PostgreSQL для этой задачи можно использовать сторонние библиотеки или встроенные функции для шифрования данных на уровне приложения. Кроме того, для повышения безопасности можно рассмотреть возможность использования функций PostgreSQL, таких как pgcrypto, чтобы шифровать данные в JSONB до их записи в базу[2].

Валидация данных также играет ключевую роль в обеспечении безопасности JSONB-полей. Данные, поступающие в JSONB, часто представляют собой сложные структуры, которые могут быть подвержены уязвимостям при отсутствии должной проверки. Без строгой валидации злоумышленники могут вводить данные, содержащие недопустимые или опасные значения, что может нарушить работу системы или привести к утечке информации. Настройка валидации входящих данных помогает предотвратить такие атаки, позволяя системе принимать только корректные данные. Например, проверка входных данных может включать ограничения на допустимые типы данных и структуру JSON[3].

Также важной частью защиты JSONB является управление доступом. Ограничение прав доступа к JSONB-полям позволяет минимизировать риск, связанный с несанкционированным доступом. В PostgreSQL можно настроить права доступа к отдельным таблицам и полям, чтобы только авторизованные пользователи могли получать доступ к JSONB-данным. Настройка таких ограничений особенно важна в многопользовательских системах, где данные из JSONB могут использоваться разными группами пользователей. Например, можно настроить правила доступа, позволяющие одному пользователю просматривать только собственные данные, хранящиеся в JSONB, что повысит общую безопасность системы[4].

Сегментация данных также помогает защитить JSONB от утечек. Например, если JSONB используется для хранения различных типов данных, целесообразно рассмотреть вариант разделения данных по разным таблицам, чтобы минимизировать доступ к конфиденциальным

данным и снизить вероятность инъекций. Сегментирование данных позволяет хранить более важную информацию в защищённых таблицах, к которым есть доступ только у ограниченного круга лиц[5].

Кроме того, полезным методом защиты JSONB-полей может быть журналирование всех операций с JSONB-данными. Ведение логов всех операций вставки, обновления и удаления данных помогает отслеживать подозрительные действия и выявлять потенциальные угрозы безопасности. Настройка логирования позволяет обнаружить любые необычные действия, связанные с JSONB-полями, что является важной частью контроля безопасности.

Таким образом, защита JSONB в PostgreSQL требует комплексного подхода, включающего параметризацию запросов, шифрование, валидацию данных и настройку прав доступа. Каждая из этих мер помогает устранить уязвимости, возникающие при работе с JSONB, и обеспечивает безопасность данных от утечек и инъекций. При грамотной настройке PostgreSQL с учётом всех перечисленных мер JSONB может быть надёжным инструментом для работы с гибкими и динамическими данными без угрозы для безопасности.

Заключение

JSONB в PostgreSQL открывает широкие возможности для гибкого и эффективного хранения данных, однако требует повышенного внимания к безопасности. Без надлежащей защиты JSONB-поля могут стать точкой уязвимости, через которую злоумышленники смогут получить доступ к конфиденциальным данным или даже проникнуть в систему. SQL-инъекции, утечки данных и недостатки в проверке входных данных — это лишь часть угроз, с которыми можно столкнуться при работе с JSONB.

Для обеспечения безопасности данных рекомендуется использовать параметризованные запросы, шифрование, строгую валидацию данных и настройку доступа к JSONB-полям. Эти меры позволят минимизировать риски и сделать работу с JSONB более безопасной. JSONB остаётся мощным инструментом, но для его надёжного использования в продуктивных системах необходимо соблюдать все рекомендованные меры безопасности, включая регулярные обновления PostgreSQL и внедрение лучших практик защиты данных.

Список литературы

1. Свидетельство о государственной регистрации программы для ЭВМ № 2020664289 РФ. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV : № 2020663625 : заявл. 03.11.2020: опубл. 11.11.2020 / И.Е.Пестов, А.М.Гельфанд, Н.Н.Лансере, И.И.Фадеев, заявитель ФГБОУ ВО «С-Пб-кий гос.университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN PKSCLB.
2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. 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. Пестов И. Е. МЕТОДИКА АВТОМАТИЗИРОВАННОГО ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ НА ИНСТАНСЫ ОБЛАЧНОЙ

ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ БЕЗАГЕНТНОГО МЕТОДА СБОРА МЕТРИК.

5. 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.

References

1. Certificate of state registration of the computer program No. 2020664289 Russian Federation. The program for providing a computer vision system based on the OpenCV library : No. 2020663625 : application 03.11.2020 : publ. 11.11.2020 / I. E. Pestov, A.M. Gelfand, N. N. Lancere, I.I. Fadeev ; applicant Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch- Bruevich." – EDN PKSCLB.
 2. Lesnova E. M., Pestov I. E. Development of a method of error detection and correction for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
 3. 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. – No. 4. – pp. 72-76.
 4. Pestov I. E. METHOD OF AUTOMATED COUNTERACTION TO UNAUTHORIZED IMPACTS ON CLOUD INFRASTRUCTURE INSTANCES USING AN AGENTLESS METHOD OF COLLECTING METRICS.
 5. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ НА МОБИЛЬНЫХ УСТРОЙСТВАХ КАК ЧАСТЬ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Поляков 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:
artpol2001@gmail.com

Современные мобильные устройства, активно используемые в рабочих процессах и корпоративных сетях, становятся важными элементами объектов информатизации. Эта статья рассматривает основные технологии защиты данных, применяемые на мобильных устройствах для предотвращения утечек и несанкционированного доступа. Описаны методы шифрования, биометрическая аутентификация, управление мобильными устройствами и сетевой мониторинг. Эти технологии помогают интегрировать защиту мобильных устройств в общую систему безопасности, создавая многослойную защиту корпоративных данных и повышая общую устойчивость информационной среды к атакам.

Ключевые слова: Мобильные устройства, защита данных, шифрование, биометрическая аутентификация, управление мобильными устройствами, информационная безопасность.

DATA PROTECTION TECHNOLOGIES ON MOBILE DEVICES AS PART OF A COMPREHENSIVE INFORMATION SECURITY SYSTEM

Polyakov 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: artpol2001@gmail.com

Modern mobile devices, increasingly used in work processes and corporate networks, have become essential components of information infrastructure. This article examines key data protection technologies on mobile devices, aimed at preventing data leaks and unauthorized access. It discusses encryption, biometric authentication, mobile device management, and network monitoring. These technologies contribute to integrating mobile device security into an overall security system, creating a multi-layered defense of corporate data and increasing the overall resilience of the information environment against attacks.

Keywords: Mobile devices, data protection, encryption, biometric authentication, mobile device management, information security.

Введение

В последние годы мобильные устройства стали неотъемлемой частью информационной инфраструктуры компаний, государственных учреждений и частных лиц. Использование смартфонов и планшетов в рабочих процессах открыло множество возможностей для повышения эффективности, но одновременно привнесло и серьезные риски безопасности. Мобильные устройства могут хранить конфиденциальные данные и предоставлять доступ к корпоративным системам, и это делает их привлекательными целями для киберпреступников, заинтересованных в краже данных, вымогательстве и шпионаже.

Комплексная защита объектов информатизации требует многоуровневого подхода, в котором защита данных на мобильных устройствах занимает значимое место. Обеспечение безопасности данных на этих устройствах включает в себя не только физическую защиту, но и широкий набор технологий, таких как шифрование, аутентификация, управление мобильными устройствами и сетевой мониторинг. Эти методы помогают минимизировать риски и интегрировать мобильные устройства в общую систему защиты информации, обеспечивая безопасность корпоративных данных и непрерывность рабочих процессов.

Технологии защиты данных на мобильных устройствах как часть комплексной системы защиты объектов информатизации

Шифрование данных на мобильных устройствах — один из ключевых методов защиты информации от несанкционированного доступа. При помощи встроенного программного обеспечения создаётся зашифрованное хранилище, доступ к которому возможен только при введении уникального ключа или с использованием биометрии. Шифрование на уровне устройства особенно важно для предотвращения утечек при потере или краже устройства. На сегодняшний день современные операционные системы, такие как iOS и Android, предлагают пользователям возможность включить шифрование и для персональных, и для рабочих данных, что делает эту меру базовым элементом защиты информации[1].

Биометрическая аутентификация вносит весомый вклад в усиление безопасности мобильных устройств. Биометрические данные, такие как отпечатки пальцев и распознавание лица, предоставляют дополнительный уровень защиты и предотвращают доступ третьих лиц. Биометрия отличается от традиционных паролей своей устойчивостью к подделке и одновременно удобством: доступ к устройству можно получить быстрее и проще. Введение биометрической защиты снижает риск взлома, при этом улучшая пользовательский опыт и не снижая уровня безопасности[2].

Системы управления мобильными устройствами (MDM — Mobile Device Management) являются ещё одним неотъемлемым компонентом комплексной защиты информации. MDM позволяет администраторам внедрять корпоративные политики безопасности и управлять устройствами на расстоянии. С помощью этих решений можно контролировать установки приложений, удалённо блокировать или очищать устройства, настраивать параметры безопасности сети. Это позволяет предотвратить несанкционированный доступ к данным и обеспечить соответствие устройств корпоративным стандартам безопасности[3].

Также критически важен сетевой мониторинг и защита от угроз. Мобильные устройства часто подключаются к различным сетям, включая публичные и небезопасные, поэтому риск перехвата данных достаточно высок. Использование VPN (виртуальной частной сети) помогает шифровать сетевые подключения и снизить вероятность утечки данных, особенно при работе в публичных Wi-Fi-сетях. Дополнительные системы безопасности, такие как IDS и IPS (системы обнаружения и предотвращения вторжений), помогают отслеживать подозрительную активность в сети и блокировать потенциальные угрозы до их нанесения вреда[4].

Совокупность всех вышеперечисленных технологий позволяет создать многоуровневую защиту, где безопасность мобильных устройств интегрируется в единую систему защиты информационной инфраструктуры. Шифрование, биометрическая аутентификация, управление устройствами и сетевой мониторинг обеспечивают всестороннюю защиту данных

на мобильных устройствах и помогают снизить риски. Такой подход не только оберегает данные, но и усиливает общую безопасность корпоративной среды, снижая уязвимость перед потенциальными угрозами и обеспечивая пользователям более надёжные и безопасные условия работы[5].

Заключение

Современные мобильные устройства, активно используемые для хранения и передачи конфиденциальных данных, требуют серьёзного подхода к защите информации. Технологии защиты данных на мобильных устройствах, такие как шифрование, биометрическая аутентификация, управление мобильными устройствами и сетевой мониторинг, составляют основу комплексной системы защиты объектов информатизации. Эти методы создают многослойную систему безопасности, защищающую устройства как от физических угроз, так и от кибератак, обеспечивая целостность и конфиденциальность данных.

В условиях, когда мобильные устройства становятся важными элементами корпоративной среды, их защита должна быть приоритетом для компаний и организаций. Постоянное развитие технологий защиты данных на мобильных устройствах позволяет минимизировать риски и укрепить общую систему безопасности, что делает их значимой частью комплексной защиты объектов информатизации.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Шемякин С. Н., Ахметшина М. Э., Катаронов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
3. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of

- Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.
3. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 5. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.736

ИСПОЛЬЗОВАНИЕ МИКРОСЕГМЕНТАЦИИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ В КРУПНЫХ ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Ноянов Р.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: romannoyanov@gmail.com

Микросегментация — это передовая методика, которая позволяет улучшить безопасность информационных систем, особенно в крупных организациях с разветвлённой ИТ-инфраструктурой. Микросегментация обеспечивает защиту на уровне приложений, минимизируя возможности lateral movement (бокового проникновения) злоумышленников в случае успешного взлома одного из компонентов. В статье рассматриваются основные принципы микросегментации, её значение для защиты от кибератак, а также приводятся примеры её внедрения и рекомендации для крупных объектов информатизации.

Ключевые слова: Микросегментация, информационная безопасность, крупные организации, боковое проникновение, защита данных, сегментация сети.

THE USE OF MICROSEGMENTATION TO IMPROVE SECURITY IN LARGE INFORMATION FACILITIES

Nayanov R.S.

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: romannoyanov@gmail.com

Microsegmentation is an advanced technique that improves the security of information systems, especially in large organizations with complex IT infrastructures. It provides application-level security, reducing the risk of lateral movement by attackers if one component is compromised. The article covers the core principles of microsegmentation, its importance in cyberattack prevention, and practical examples of its deployment in large information systems.

Keywords: Microsegmentation, information security, large organizations, lateral movement, data protection, network segmentation.

Введение

С ростом объёма информации и сложностью ИТ-инфраструктур безопасность крупных объектов информатизации становится одной из первостепенных задач для организаций. Современные компании и государственные учреждения сталкиваются с целым рядом угроз, таких как взломы, утечка данных и целевые атаки, направленные на компрометацию их систем. Чтобы уменьшить риски, специалисты по безопасности используют различные техники сегментации сети, и одной из наиболее эффективных из них является микросегментация. В отличие от традиционной сегментации, микросегментация позволяет детализировать контроль и изолировать каждое приложение и сервис в пределах одного

сегмента, что обеспечивает высокую степень защиты от так называемого бокового проникновения (*lateral movement*), когда злоумышленник может перемещаться по сети, получив доступ к одной её части.

Применение микросегментации помогает изолировать рабочие процессы и сервисы друг от друга, что особенно актуально для крупных организаций, которые работают с конфиденциальной информацией. Это позволяет не только повысить безопасность данных, но и управлять политиками доступа на уровне приложений. Микросегментация даёт возможность контролировать связи между сервисами и пользователями, создавая своеобразные «цифровые барьеры» в пределах корпоративной сети и защищая критически важные ресурсы от несанкционированного доступа. В этой статье рассмотрены принципы, которые лежат в основе микросегментации, её преимущества для крупной инфраструктуры, а также примеры использования этой технологии.

Использование микросегментации для повышения безопасности в крупных объектах информатизации

Микросегментация — это методика, которая предполагает разбивку сети на мелкие логические сегменты, каждый из которых имеет свои правила и политики безопасности. Это позволяет точно контролировать доступ и взаимодействие как между отдельными устройствами, так и между приложениями, работающими в пределах одного сегмента сети. Одним из основных преимуществ микросегментации является её способность предотвращать распространение угроз в случае взлома одного из сегментов. В обычной сети, если злоумышленник получает доступ к одному устройству, он может с легкостью распространить атаку на другие устройства внутри этой же сети. Микросегментация же создаёт «защитные зоны» для каждого компонента, ограничивая доступ к ним и минимизируя последствия атаки[1].

К примеру, в случае атаки с использованием уязвимости в приложении, злоумышленник может попытаться использовать её для бокового проникновения. Если инфраструктура крупной организации сегментирована с помощью микросегментации, атакующий будет ограничен в доступе и не сможет перейти к другим важным системам, таким как базы данных или сервисы обработки платежей. Это особенно полезно для организаций, работающих с чувствительными данными, такими как финансовые учреждения, медицинские центры и государственные ведомства. В условиях сложных сетевых архитектур, где тысячи устройств и пользователей взаимодействуют между собой, возможность контролировать доступ на уровне приложения и отдельно каждой сессии позволяет значительно усилить защиту[2].

Ключевая особенность микросегментации — гибкость и масштабируемость. Современные решения по микросегментации позволяют легко адаптировать политику безопасности к новым приложениям, обновлениям или требованиям бизнеса. Это особенно важно в крупных организациях, где постоянно происходят изменения в архитектуре сети[3]. Например, если в систему добавляется новое приложение, микросегментация позволяет быстро задать необходимые правила доступа для него, без необходимости глобальных изменений всей сети. Также микросегментация может быть интегрирована с системами мониторинга, чтобы отслеживать активность внутри каждого сегмента и выявлять подозрительные действия в режиме реального времени[4].

Ещё один важный аспект микросегментации — возможность автоматизации управления. Благодаря технологиям микросегментации специалисты по безопасности могут создавать автоматические сценарии для защиты данных и управления доступом. Например, если в одном из сегментов происходит необычная активность, система может автоматически заблокировать доступ к этому сегменту, уведомить администратора и предотвратить распространение угрозы. Такой подход позволяет значительно снизить нагрузку на IT-отделы и минимизировать человеческий фактор.

Технически, микросегментация реализуется с помощью различных решений, таких как программно-определяемые сети (SDN) и системы виртуализации. Они позволяют изолировать не только физические устройства, но и виртуальные среды и облачные сервисы. С помощью этих технологий микросегментация может быть реализована в различных типах инфраструктуры, будь то традиционная корпоративная сеть, облачные решения или гибридные системы. Это делает микросегментацию одним из наиболее универсальных инструментов для повышения безопасности[5].

Несмотря на очевидные преимущества, внедрение микросегментации требует тщательного планирования и грамотной настройки. Необходимо разработать четкие правила доступа и взаимодействия для каждого сегмента, определить приоритетные ресурсы и настроить мониторинг активности внутри сегментов. Для крупных организаций этот процесс может занять значительное время, но результат оправдывает вложенные усилия: микросегментация позволяет снизить риск распространения атак, минимизировать потенциальные потери данных и обеспечить более высокий уровень безопасности для критически важных систем.

Заключение

Микросегментация представляет собой мощный инструмент для защиты крупных объектов информатизации от внутренних и внешних угроз. Её способность детально контролировать взаимодействие между компонентами сети и изолировать каждый процесс обеспечивает высокий уровень безопасности, необходимый для защиты современных корпоративных инфраструктур. Это особенно важно для крупных организаций, где большое количество пользователей и сервисов увеличивает риск несанкционированного доступа и утечек данных.

В условиях, растущих киберугроз микросегментация становится важным элементом стратегии безопасности, позволяя предотвратить распространение атак и защитить критически важные ресурсы. Внедрение микросегментации требует серьёзных ресурсов и усилий, однако преимущества, которые она предоставляет, делают её оптимальным решением для компаний, стремящихся к максимальной защите своей информации.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. 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. 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.
4. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
5. 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.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
 2. Minyaev A. A. Method for evaluating the effectiveness of an information protection system geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruevich, 1996.
 4. Gelfand A.M. Methods of choosing stegocontainers for data transmission //Regional Informatics and information security. – 2020. – pp. 260-262.
 5. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.942

ВОСПРИЯТИЕ ЧЕЛОВЕЧЕСКОГО ГОЛОСА ПРИ ПОМОЩИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

¹Некрасов Т.Д., ²Комбаров В.Д., Лозница С.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:

¹Kvakolka885@gmail.com, ²vlad54295@gmail.com

В статье рассматриваются принципы и технические возможности применения методов Фурье-анализа для обработки звуковых сигналов в ИИ. В современном мире технологии искусственного интеллекта (ИИ) играют всё более важную роль в нашей жизни. Они используются в различных областях, от медицины до развлечений, и становятся неотъемлемой частью нашего общества. Одной из ключевых задач ИИ является восприятие и анализ человеческого голоса. В этой работе мы рассмотрим основные аспекты восприятия человеческим голосом искусственным интеллектом, а также его применение в различных сферах деятельности.

Ключевые слова: ИИ, метод, анализ, звук, преобразование, дискретизация, голос.

PERCEPTION OF THE HUMAN VOICE WITH THE HELP OF ARTIFICIAL INTELLIGENCE

¹Nekrasov T.D., ²Kombarov V.D., Loznitsa S.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: ¹Kvakolka885@gmail.com, ²vlad54295@gmail.com

The article discusses the principles and technical possibilities of using Fourier analysis methods for processing audio signals in AI. In the modern world, artificial intelligence (AI) technologies are playing an increasingly important role in our lives. They are used in various fields, from medicine to entertainment, and are becoming an integral part of our society. One of the key tasks of AI is the perception and analysis of the human voice. In this paper, we will look at the main aspects of the perception of the human voice by artificial intelligence, as well as its application in various fields of activity.

Keywords: AI, method, analysis, sound, transformation, sampling, voice.

Актуальность темы обусловлена растущим интересом к использованию технологий ИИ для улучшения качества жизни людей. Понимание того, как ИИ воспринимает человеческий голос, может привести к созданию более эффективных систем распознавания речи, улучшению коммуникации между человеком и машиной, а также разработке новых методов диагностики и лечения речевых нарушений.

Цель данной работы — изучить основные принципы и методы восприятия человеческим голосом искусственным интеллектом. Для достижения этой цели будут решены следующие задачи:

- Рассмотреть физиологические и психологические аспекты восприятия звука человеком;
- Изучить основные характеристики человеческого голоса, важные для восприятия;
- Описать алгоритмы и методы машинного обучения для распознавания речи;
- Проанализировать применение методов Фурье-анализа для обработки звуковых сигналов в ИИ;
- Привести примеры использования ИИ для анализа человеческого голоса;
- Провести экспериментальное исследование восприятия человеческого голоса ИИ.

Перейдем к рассмотрению физиологических и психологических аспектов восприятия звука человеком.

Звук — это колебательное движение частиц среды, которое распространяется в пространстве и воспринимается органами слуха человека. Восприятие звука включает в себя несколько этапов: преобразование звуковой волны в электрические сигналы, передачу этих сигналов в мозг и их обработку.

Человеческий слух способен воспринимать звуки в диапазоне от 20 Гц до 20 кГц. Этот диапазон охватывает большинство звуков, которые встречаются в повседневной жизни. Звуковые волны, попадающие в ухо, вызывают колебания барабанной перепонки, которые затем передаются на слуховые косточки и улитку внутреннего уха. Улитка преобразует звуковые волны в электрические импульсы, которые передаются в мозг через слуховой нерв.

Психологические аспекты восприятия звука включают в себя такие понятия, как высота тона, громкость, тембр и длительность. Высота тона определяется частотой звуковых колебаний, громкость — амплитудой этих колебаний, тембр — наличием обертонов, а длительность — продолжительностью звука.

Основные характеристики человеческого голоса, важные для восприятия

Основными характеристиками человеческого голоса, которые важны для восприятия, являются частота, амплитуда, спектр и тембр. Частота определяет высоту тона голоса, амплитуда — его громкость, спектр — распределение частот в звуке, а тембр — его окраску.

Частота измеряется в герцах (Гц) и определяет количество колебаний звуковой волны в секунду. Чем больше частота, тем выше тон голоса. Амплитуда измеряется в децибелах (дБ) и определяет громкость звука. Спектр представляет собой график распределения частот в звуке. Тембр определяется наличием обертонов — дополнительных частот, которые придают голосу его уникальную окраску.

Для восприятия человеческого голоса важны такие характеристики, как чёткость произношения, интонация, ритм и темп речи. Чёткость произношения определяет ясность и понятность речи, интонация — эмоциональную окраску голоса, ритм — чередование ударных и безударных слогов, а темп речи — скорость произнесения слов.

Рассмотрим вопрос восприятие человеческого голоса с помощью искусственного интеллекта.

Алгоритмы машинного обучения позволяют ИИ распознавать и анализировать человеческий голос[2]. Существует несколько основных подходов к распознаванию речи:

- Распознавание по шаблонам: сравнение входного сигнала с заранее записанными шаблонами;

- Скрытые марковские модели: использование статистических моделей для описания последовательностей событий;
- Нейронные сети: обучение на больших объёмах данных для выявления закономерностей и зависимостей.

Нейронные сети являются наиболее перспективным подходом к распознаванию речи. Они способны обучаться на больших объёмах данных и выявлять сложные закономерности, что позволяет им достигать высокой точности распознавания.

Часто для обработки звуковых сигналов в ИИ используется метод Фурье-анализа. Методы Фурье-анализа позволяют преобразовать звуковые сигналы из временной области в частотную. Это позволяет выделить основные частоты в сигнале и определить его спектральный состав [3].

Применение методов Фурье-анализа в ИИ позволяет улучшить качество распознавания речи за счёт выделения ключевых характеристик голоса. Например, можно использовать методы Фурье-анализа для определения высоты тона голоса, его громкости и тембра.

Суть метода Фурье заключается в следующем [1-3]:

1. Функция $f(x)$, определённая на некотором интервале $[a, b]$, представляется в виде суммы бесконечного числа синусов и косинусов с различными частотами и амплитудами. Это представление называется рядом Фурье.

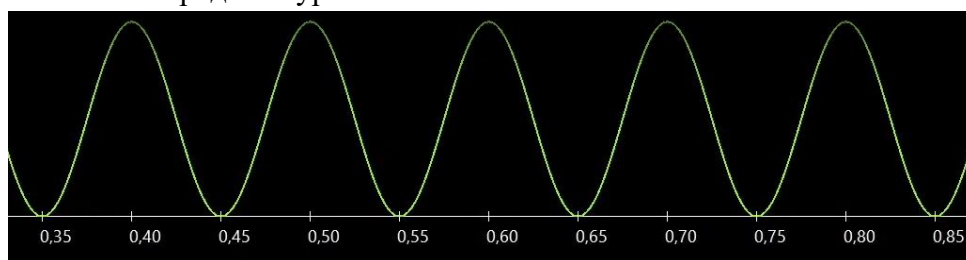


Рисунок 1 – Ряд Фурье.

2. Коэффициенты ряда Фурье вычисляются через интегралы от функции $f(x)$. Они зависят от амплитуды и фазы каждой синусоиды в разложении.

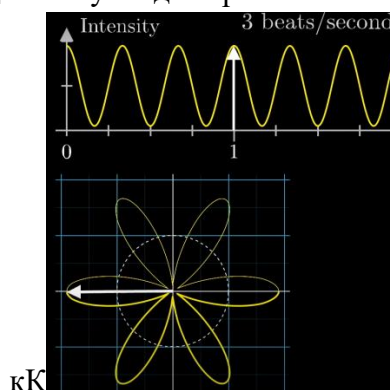


Рисунок 2 - Коэффициенты ряда Фурье.

3. После вычисления коэффициентов ряда Фурье мы получаем функцию, которая описывает зависимость интенсивности от времени. Данная функция не имеет времени в качестве входных данных, а вместо этого принимает частоту, которая и является частотой намотки. Выходные данные этой функции представляют собой комплексное число, некоторую точку на плоскости (центр масс воображаемой намотки).

$$g(f) = \int_{-\infty}^{+\infty} g(t)e^{-2\pi ift} dt$$

4. Метод Фурье позволяет анализировать сложные функции, разлагая их на более простые синусоидальные составляющие. Это упрощает анализ и позволяет выявить закономерности в данных

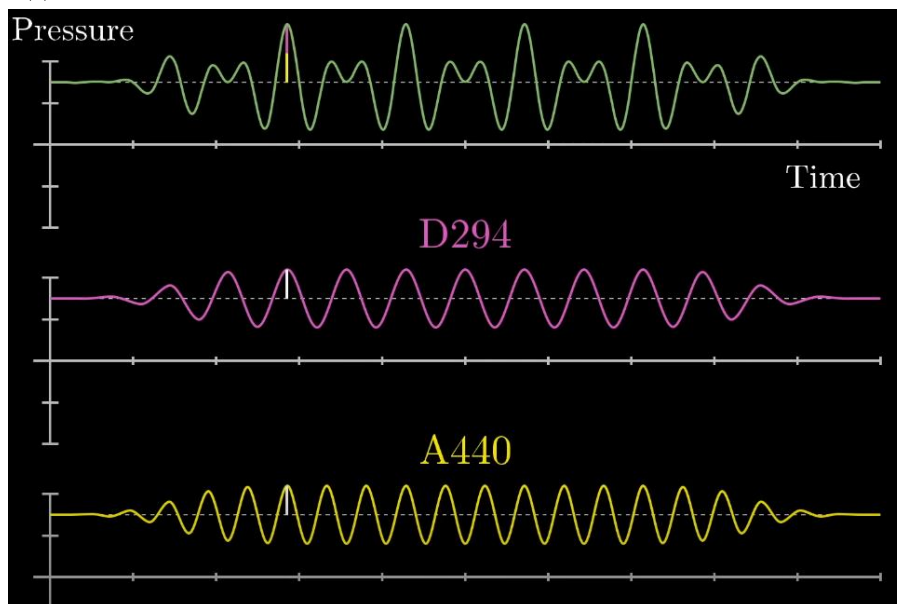


Рисунок 3 - Синусоидальные составляющие.

5. В контексте обработки сигналов и изображений метод Фурье используется для анализа частотных составляющих сигнала или изображения. Это позволяет выделить важные частоты и удалить шум из данных.

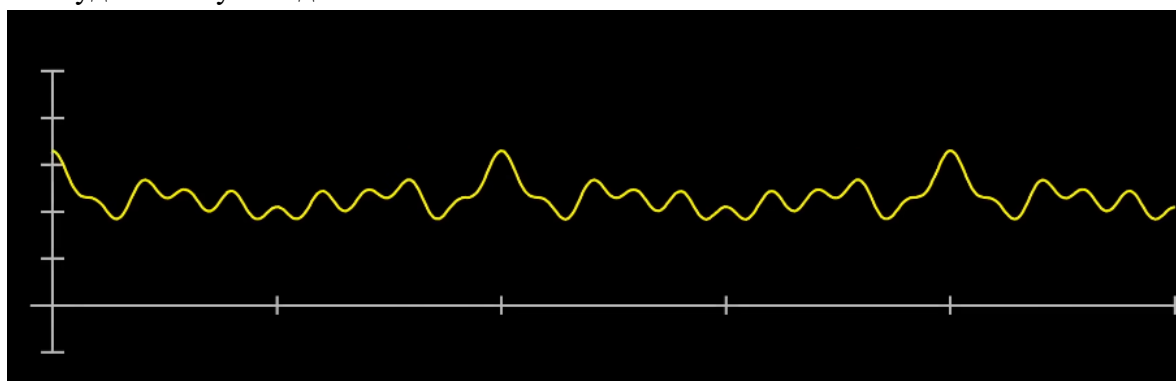


Рисунок 4 – Выделение частот и удаление шума из данных.

6. Преобразование Фурье переводит функцию из временной области в частотную. Оно показывает, какие частоты присутствуют в сигнале и с какой амплитудой они проявляются.

7. Обратное преобразование Фурье возвращает нас из частотной области обратно во временную, восстанавливая исходный сигнал.

8. Быстрое преобразование Фурье (БПФ) — это алгоритм, который позволяет вычислить коэффициенты ряда Фурье гораздо быстрее, чем при использовании прямого

подхода. БПФ широко используется в различных областях, таких как обработка сигналов, спектральный анализ, сжатие данных и т.д.

Далее рассмотрим примеры использования ИИ для анализа человеческого голоса.

Управление воздушным движением. Системы распознавания голоса могут быть использованы для управления воздушным движением, позволяя диспетчерам отдавать команды пилотам и получать от них информацию с помощью голосовых команд. Это может упростить процесс коммуникации и снизить нагрузку на диспетчеров.

Автоматизация рутинных операций. В авиации существует множество рутинных задач, которые можно автоматизировать с помощью распознавания голоса. Например, системы распознавания могут использоваться для автоматического заполнения форм, составления отчётов и других административных задач.

Обучение пилотов. Системы распознавания голоса также могут быть полезны для обучения пилотов. Они могут использоваться для оценки произношения команд, понимания акцентов и интонаций, а также для выявления ошибок в речи пилотов.

Обеспечение безопасности полётов. Системы распознавания голоса могут помочь обеспечить безопасность полётов, обнаруживая необычные или подозрительные звуки, такие как крики, стоны или другие звуки, которые могут указывать на проблемы с оборудованием или здоровьем экипажа.

Улучшение коммуникации между экипажем. Распознавание голоса может улучшить коммуникацию между членами экипажа, позволяя им быстро и точно обмениваться информацией во время полёта. Это особенно полезно в условиях стресса или ограниченной видимости.

Помощь в навигации. Системы распознавания голоса могут использоваться для помощи пилотам в навигации, предоставляя им информацию о высоте, скорости, курсе и других параметрах полёта.

Диагностика оборудования. Распознавание голоса также может быть использовано для диагностики оборудования, позволяя пилотам быстро выявлять и устранять неисправности.

Технологии искусственного интеллекта уже достигли значительных успехов в области распознавания и анализа человеческого голоса. Однако существуют определённые ограничения и проблемы, связанные с точностью и эффективностью этих технологий. Для этого мы решили изучить эту тему и найти пробелы в совершенстве распознавания голоса. Но мы также должны осознавать необходимость разработки этических принципов и норм, регулирующих использование технологий искусственного интеллекта для восприятия человеческого голоса. Необходимо учитывать возможные риски и негативные последствия, связанные с нарушением конфиденциальности, дискриминацией и другими проблемами. Важно подчеркнуть развитие данной технологии для использования ее в целях обеспечения безопасности, как и в домашних условиях, так и в рабочих.

Список литературы

1. Латыпова Н.В., Тучинский Л.И. (2011). РЯДЫ ФУРЬЕ (Ижевск).
2. А. Х. Шахмейстер(2014). Комплексные Числа (Москва).
3. К. Н. Гурьянова, У. А. Алексеева, В. В. Бояршинов (2014). Математический Анализ (Екатеринбург).

References

1. Latypova N.V., Tuchinsky L.I. (2011). FOURIER SERIES (Izhevsk).
 2. A. H. Shakhmeister (2014). Complex Numbers (Moscow).
 3. K. N. Guryanova, U. A. Alekseeva, V. V. Boyarshinov (2014). Mathematical Analysis (Yekaterinburg).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.932.7

АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ СЕТЕЙ С КОМПЛЕМЕНТАРНОЙ РАЗРЕЖЕННОСТЬЮ

¹Варбанский К.С., ²Городничев М.Г.

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФГБОУ ВО "МОСКОВСКИЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ", Москва, Россия,
(111024, город Москва, Авиамоторная ул., д.8а), e-mail: ¹varbanskik@gmail.com,
²m.g.gorodnichev@mtuci.ru

Проведен анализ и исследование подхода к оптимизации нейронных сетей с использованием разреженных-разреженных сетей. Работа направлена на выявление преимуществ и потенциала данного подхода в области машинного обучения, в частности в области больших языковых моделей и компьютерного зрения. В статье описываются подходы с использованием разреженности весов, разреженности активации, а также двойной разреженности.

Ключевые слова. Разреженность, нейронные сети, разреженность весов, разреженность активаций, комплементарная разреженность, глубокое обучение, компьютерное зрение.

ANALYSIS OF TRENDS IN THE DEVELOPMENT OF NETWORKS WITH COMPLEMENTARY SPARSITY

¹Varbansky K.S., ²Gorodnichev M.G.

OF THE ORDER OF THE RED BANNER OF LABOR OF THE MOSCOW TECHNICAL
UNIVERSITY OF COMMUNICATIONS AND INFORMATICS, Moscow, Russia, (111024, Moscow,
Aviamotornaya str., 8a), e-mail: ¹varbanskik@gmail.com, ²m.g.gorodnichev@mtuci.ru

The analysis and research of the approach to optimization of neural networks using sparse-sparse networks is carried out. The work is aimed at identifying the advantages and potential of this approach in the field of machine learning, in particular in the field of large language models and computer vision. The article describes approaches using sparsity of weights, sparsity of activation, as well as double sparsity.

Keywords: Sparsity, neural networks, sparsity of weights, sparsity of activations, complementary sparsity, deep learning, computer vision.

Введение

В современном мире нейронные сети широко применяются в различных областях, начиная от распознавания образов до автономного управления технологическими процессами. Однако их широкое применение вызывает вопрос о вычислительной эффективности и ресурсозатратности.

В последние годы глубокие нейронные сети (DNN) стали больше и сложнее, что привело к значительному прогрессу в области искусственного интеллекта (AI). Однако экспоненциальный рост этих моделей угрожает дальнейшему развитию. Для обучения требуется большое количество процессоров, графических (GPU) или тензорных (TPU), и обучение может занимать дни или даже недели, что приводит к большому углеродному следу и растущим расходам на облачные вычисления [1].

Разреженность в нейронных сетях представляет собой перспективное направление для решения этой проблемы. Существует ряд исследований, демонстрирующих потенциал разреженных моделей в улучшении производительности и уменьшении затрат вычислительных ресурсов. Данные исследования подчеркивают важность комплементарной разреженности, включающей не только разреженность весов, но и разреженность активаций, в контексте улучшения эффективности нейронных сетей.

Разреженность

Разреженность в нейронных сетях – это концепция, которая означает, что большинство весовых или активационных параметров в сети равны нулю, тогда как некоторые значения остаются ненулевыми. В результате такой структуры большая часть параметров не участвует в вычислениях, что позволяет существенно снизить вычислительную нагрузку и использование памяти, не влияя значительно на качество работы сети. Таким образом, разреженность в нейронных сетях позволяет оптимизировать процессы обучения, выполнения и хранения, что становится все более востребованным с увеличением сложности моделей и требований к ресурсам.

Разреженность весов (*Weight sparsity*)

Существуют два основных метода достижения разреженности весов в нейронных сетях: обрезание (*pruning*) и рост (*growth*). Обрезание заключается в удалении или занулении некоторых весов в нейронной сети. Этот процесс может быть проведен как во время обучения, так и после его завершения. Обрезание ненужных весов сокращает размер модели, уменьшает требуемый объем памяти и также снижает вычислительные затраты.

Подход роста весов, напротив, заключается в увеличении количества связей нейронной сети во время обучения. Таким образом может выявляться значимость определенных признаков, присутствующих в данных. Рост весов гипотетически может помочь уменьшить потери точности, возникающие при чрезмерном обрезании и улучшить обобщающую способность модели.

В научной сфере и в индустрии в целом обрезание весов применяется гораздо более широко, нежели рост весов; имеет значительный научный и практический фон. Метод обрезания весов сравнительно прост в реализации что делает его более привлекательным для практического использования так как этот метод может быть применен без изменения архитектуры модели и после ее обучения. Уменьшение размера нейронных сетей очень важно для их имплементации в малые устройства, такие как мобильные телефоны, часы и умные бытовые приборы.

Разреженность активаций (*Activation sparsity*)

Сеть с разреженностью активаций — это сеть, в которой алгоритм активации нейрона настроен таким образом, что в каждом слое в каждый момент времени активна лишь очень небольшой процент всех нейронов слоя.

Для имплементации разреженности активаций используются методы обучения и оптимизации, которые сводят слабые активаций к нулю. Применяются различные методы регуляризации, например методы *L1 (Lasso)* или *L2 (Ridge)*, которые добавляют к функции

потерь модели штрафное слагаемое. Также может быть использован метод прореживания (*Dropout*), который случайным образом обнуляет некоторые активации во время обучения.

В научной сфере и в индустрии в целом принцип разреженности активаций имплементируется гораздо реже чем принцип разреженности весов.

Веса – это параметрами модели, которые оптимизируются во время обучения различными методами (например, градиентный спуск). Активации — это промежуточные выходные значения нейронов, которые не являются параметрами модели и не могут быть прямо оптимизированы во время обучения.

Разреженность весов существенно уменьшает количество вычислений, поскольку многие пропускаются. В то время как для учета разреженности активаций требуется дополнительная логика, так как активации являются результатом применения функций активации к взвешенным суммам входов. Это усложняет реализацию еще при управлении процессом обучения.

В целом практика показала, что разреженность весов приводит к существенному уменьшению размера модели и ускорению работы, что делает ее более привлекательной для широкого применения. Разреженность активаций также может улучшить производительность модели, но в меньшей степени по сравнению с разреженностью весов.

Комплементарная разреженность (*Complementary sparsity*)

В принципе, разреженные нейронные сети должны быть значительно эффективнее традиционных плотных сетей. Нейроны в мозге демонстрируют два типа разреженности: они редко связаны друг с другом и редко активны. Пирамидальные нейроны коры головного мозга обладают высокой разреженной связью друг с другом и получают относительно мало возбуждающих входов от большинства окружающих нейронов [2]. Когда эти два типа разреженности используются вместе, предполагается потенциал для снижения вычислительной сложности нейронных сетей на два порядка. Несмотря на этот потенциал, современные нейронные сети обеспечивают лишь умеренные преимущества используя в основном только разреженность весов.

Вдохновившись нейробиологией, разреженность была предложена в качестве решения проблемы быстрого роста размера моделей. Разреженные сети либо ограничивают связность или активность своих нейронов, значительно уменьшая размер и вычислительную сложность модели. Обычно эти методы применяются изолированно для создания разреженных-плотных сетей. Однако весовая и активационная разреженности являются синергетическими, и при совместном использовании вычислительная экономия умножается.

Например, когда сеть имеет 90% разреженность весов, только 1 из 10 весов не нулевой, облегчая вычисления в 10 раз. Когда сеть имеет 90% разреженность активаций, только 1 из 10 входов не нулевой, также обеспечивая уменьшение вычислительной нагрузки в 10 раз. При совместном применении нулевые значения взаимодействуют таким образом, что в среднем только 1 из 100 результатов будет не нулевым, обеспечивая кратность эффективности в 100 раз, если будут разработаны эффективные методы избежания обработки, извлечения, умножения и хранения нулевых элементов. Однако, несмотря на потенциальные преимущества данного подхода, его изучение и практическое применение пока еще остаются ограниченными.

Комплементарная разреженность — это решение, обращающее проблему разреженности.

Вместо создания аппаратных средств для поддержки неструктурированных разреженных сетей, предлагается как разреженность может быть структурирована так, чтобы соответствовать требованиям целевого аппаратного обеспечения.

Обзор литературы

Исследователи анализируют масштабируемость и компромиссы, связанные с использованием ресурсов для различных ядер, характерных для коммерческих сверточных сетей, таких как ResNet-50 или MobileNetV2. Результаты, полученные при использованиях комплементарной разреженности, показывают, что сочетание разреженности весов и активаций может быть мощным инструментом для эффективного масштабирования будущих моделей искусственного интеллекта. Применяемая реализация использует комплементарную разреженность с помощью конкурентного алгоритма *k-winner-takes-all* (k-WTA) [3].

Прямая обработка репрезентации (*representation*) разреженной матрицы неэффективна из-за наличия нулевых элементов. Техники, такие как блочная и разделенная разреженность (*block and partitioned sparsity*), помогают выравнивать структуру ненулевых элементов с аппаратными требованиями, но они фундаментально противоречат созданию точных высокоразреженных сетей. Оптимальная производительность требует больших блоков и уменьшенных размеров разбиения, но это ограничивает возможную разреженность и точность [4]. Это, в свою очередь, подрывает возможность этих подходов достичь теоретических преимуществ высокоразреженных сетей.

Альтернативный подход обращает проблему разреженности, структурируя разреженные матрицы таким образом, чтобы они были практически неотличимы от плотных матриц. Это достигается путем наложения нескольких разреженных матриц для формирования одной, плотной матрицы. Возможно оптимально соединить две разреженные матрицы в одну более плотную, если в обеих разреженных матрицах нет ненулевого элемента в одном и том же месте. Для данных поступающих активаций выполняется покомпонентное умножение (плотная операция), а затем воссоздается каждая индивидуальная сумма.

Эта техника вводит ограничения на местоположение ненулевых элементов, но не определяет их относительные положения. А также не устанавливает допустимые уровни разреженности. Техника может быть применена к сверточным ядрам (*convolutional kernels*) путем наложения нескольких трехмерных разреженных тензоров (*tensors*) из четырехмерного разреженного тензора весов слоя. Гипотетически эта техника обеспечивает линейное улучшение производительности по мере уменьшения количества ненулевых элементов, даже для очень высоких уровней разреженности.

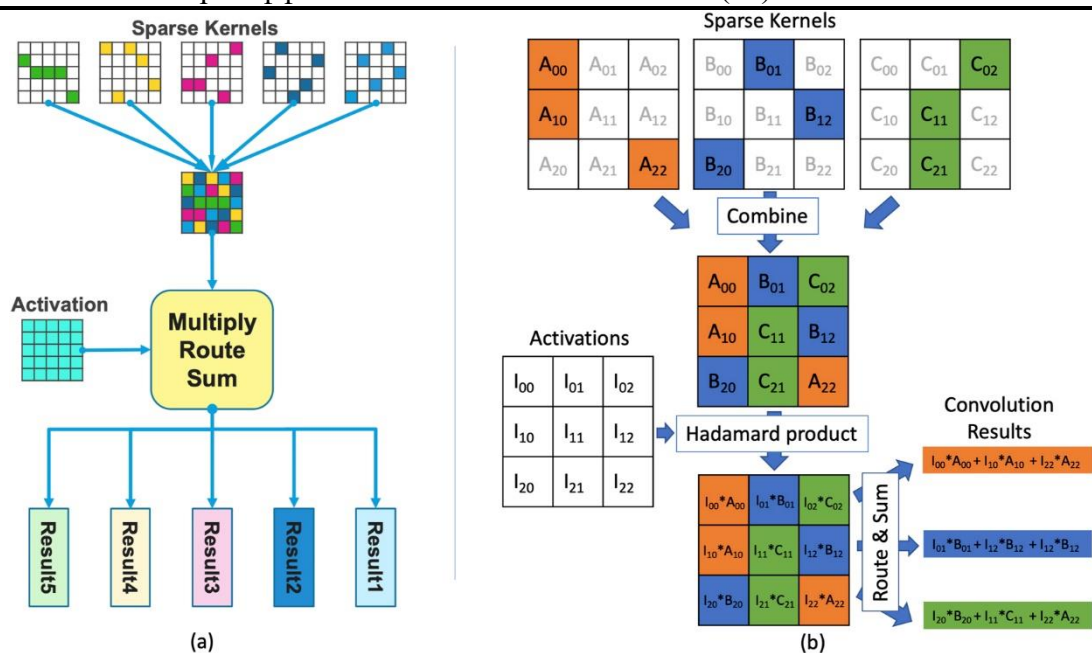


Рисунок 1. - «Упаковка» нескольких разреженных сверточных ядер в одно плотное ядро. Затем сеть маршрутизации вычисляет каждую индивидуальную сумму.

Источник: статья «Two Sparsities Are Better Than One»

Учитывая, что комплементарная разреженность сводит N разреженных сверток к одной плотной операции, существует потенциал для линейного улучшения производительности в N раз. Основная сложность заключается в снижении затрат, связанных с маршрутизацией и накоплением «упакованных» результатов. С помощью этой техники проблема разреженности-разреженности упрощается до проблемы с разреженными активациями и плотными весами, что устраняет накладные расходы.

Эксперименты были проведены на комплексной системе распознавания речи (*end to end speech recognition system*). Сверточная нейронная сеть обучалась распознавать короткие, однословные речевые команды, используя датасет *Google Speech Commands (GSC)*. Задача — распознать произнесенное слово из аудиодорожки. Разработка предназначена для встраиваемых умных домашних предметов и платформ, реагирующих на речевые команды.

Например, одна сеть представляет собой конвейерную реализацию одной сети *GSC*, обрабатывающую один поток речевых команд на *FPGA (Field Programmable Gate Array)* на платформе *U250*. Разреженная реализация достигает более чем 33-кратного увеличения пропускной способности по сравнению с плотной реализацией [5].

Рассматриваются и другие подходы имплементации комплементарной разреженности.

Изображения высокого разрешения позволяют нейронным сетям учить более богатые визуальные репрезентации. Однако, улучшенная производительность приходит с ростом вычислительной сложности, что затрудняет их использование в приложениях, требующих низкой задержки. Не все пиксели равнозначны, пропуск вычислений для менее важных областей - эффективный метод для снижения вычислительной нагрузки. Однако это сложно преобразовать в фактическое ускорение для сверточных нейронных сетей, так как это нарушает регулярность плотной нагрузки свертки.

SparseViT пересматривает разреженность активаций для оконных видов трансформеров (*ViTs*). Возможно ускорение с помощью обрезки активаций поскольку внимание окон естественным образом группируется по блокам, в отличие от сверток. Разные слои должны иметь разные коэффициенты обрезки из-за их разнообразной чувствительности и вычислительных затрат.

Внутри изображения пиксели, содержащие детальные признаки объектов более важны, чем пиксели фона. Очень естественной идеей является применение обрезки активаций для пропуска вычислений для менее важных областей. Однако разреженность активаций не может быть легко преобразована в фактическое ускорение на универсальном оборудовании.

Имплементируя подобное обрезание на каждом слое достигается 50% сокращения задержки при 60% разреженности активаций на уровне окон.

Адаптация, осведомленная о разреженности (*Sparsity-aware adaptation*), случайным образом обрезает различные подмножества активаций на каждой итерации. Это адаптирует модель к разреженности активаций и избегает необходимости энергозатратного переобучения для нахождения оптимальных обрезаний на каждом слое.

Подобная обрезка активаций отличается от статической обрезки весов тем, что она динамическая и зависит от ввода. В то время как существующие методы обрезки активаций обычно сосредотачиваются на снижении затрат памяти во время обучения [6], лишь немногие из них нацелены на улучшение задержки вывода, так как разреженность активаций не всегда приводит к ускорению вычислений на аппаратном обеспечении.

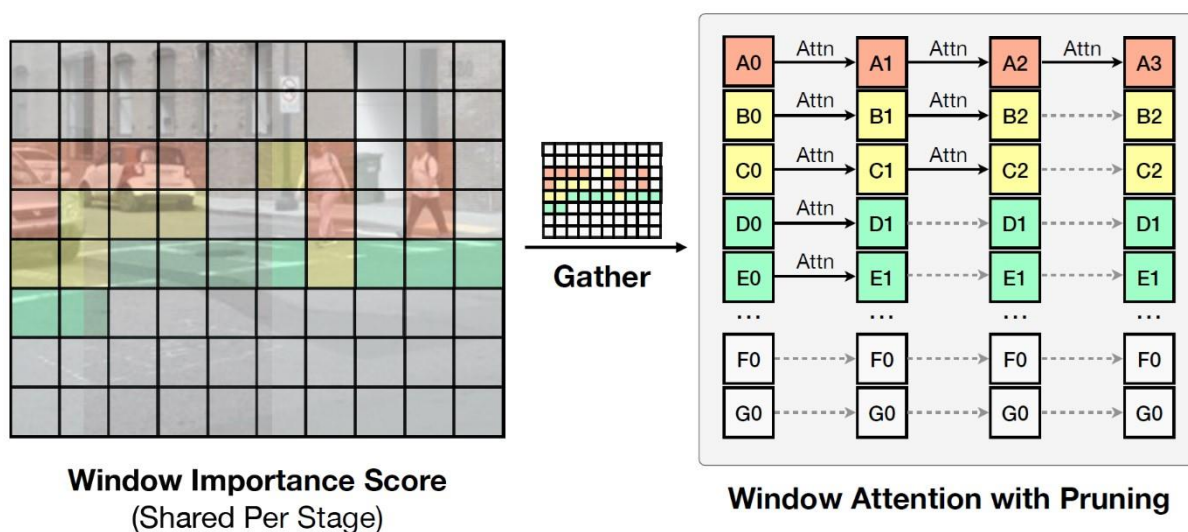


Рисунок 2. - Важность каждой активации - L_2 -нормы. Сбор признаков из окон с наивысшими оценками важности, а затем выполнение самовнимания на выбранных окнах.

Источник: статья «*SparseViT*»

Важность каждого окна определяется его L_2 -нормой активации. Учитывая коэффициент разреженности активации, сначала собираются окна с наивысшими оценками важности. И затем применяются механизм многоголового самовнимания (*MHSA*), сеть прямого распространения (*FFN*) и нормализация слоев (*LN*) только на этих выбранных окнах. Полученные результаты рассеиваются обратно в сеть.

В отличие от обычной обрезки весов, оценки важности зависят от ввода и должны соответственно быть вычислены во время вывода. Это может повлечь значительные накладные расходы на задержку. Поэтому вычисление важности окон выполняется только один раз на каждом этапе и повторно используется для всех блоков внутри этого этапа.

Использование одинакового уровня разреженности на всех слоях модели не эффективно по той причине, что различные слои оказывают различное воздействие на точность и эффективность. Например, начальные слои обычно требуют больше вычислений из-за их больших размеров карты признаков (*feature map*), в то время как более поздние слои больше поддаются обрезке, так как они ближе к выходу. Таким образом, более выгодно применять более активную обрезку к слоям с меньшей чувствительностью и более высокими затратами.

Для определения наилучшей конфигурации смешанной разреженности (*mixed-sparsity*) для модели критически важно оценивать ее точность при различных настройках разреженности. Однако непосредственная оценка точности исходной модели с разреженностью приведет к ненадежным результатам. Переобучение модели с каждой возможной конфигурацией разреженности перед оценкой ее точности непрактично из-за значительных временных и вычислительных затрат.

Для решения этой проблемы используется метод, основанный на осведомленности о разреженности (*Sparsity-aware adaptation*). Этот метод заключается в адаптации исходной модели, которая была обучена только с плотными активациями, путем случайной выборки слоев с разреженностью активаций.

После адаптации получаем более точную оценку производительности различных конфигураций разреженности без необходимости полного повторного обучения. Это позволяет эффективно оценивать различные конфигурации смешанной разреженности и определять оптимальную для модели.

Одним из ключевых аспектов дизайна является то, что лучше использовать ввод с высоким разрешением и более агрессивно проводить обрезание, чем начинать с ввода с низким разрешением и меньше обрезать. Начиная с высокого разрешения сохраняется детализированная информация изображения. Цель – обрезать окна, отображающие фон.

В отличие от однородных коэффициентов разреженности, применяемых ко всем слоям, *SparseViT* использует неоднородные коэффициенты разреженности для различных слоев на основе их близости к началу нейронной сети. Более маленькие размеры окон в первом и втором блоках позволяют более агрессивную обрезку, в то время как более крупные окна в более поздних слоях приводят к менее агрессивной обрезке. Этот выбор неоднородной разреженности приводит к лучшей точности.



Рисунок 3. - Цвет окна соответствует количеству слоев, в которых оно обрабатывалось.

Источник: статья «SparseViT»

Используется осведомленность о разреженности и эволюционный поиск для нахождения оптимальной конфигурации разреженности на уровне слоев в огромном пространстве поиска. Эта техника приводит к ускорению в 1.5, 1.4 и 1.3 раза по сравнению с ее плотным аналогом в монокулярном 3D-обнаружении объектов, 2D-сегментации экземпляров и 2D-семантической сегментации соответственно. Потери точности либо незначительны, либо отсутствуют в принципе [7].

Вывод

Результаты демонстрируют, что разреженность приводит к избеганию выполнения множества ненужных операций, улучшая пропускную способность и энергоэффективность. Возрос интерес к имплементации разреженности на платформах *GPU* так как, ограничения аппаратного обеспечения препятствуют развитию и внедрению разреженных сетей [8]. На сегодняшний день техники на основе *GPU* ограничены в своей способности достичь значительных приростов производительности на полных сетях. Также, они не предрасположены к использованию как сетей с разреженностью активаций, так и сетей с комплементарной разреженностью.

Список литературы

1. N. C. Thompson, K. H. Greenewald, K. Lee, and G. F. Manso. The Computational Limits of Deep Learning. CoRR, 2022. URL <https://arxiv.org/abs/2007.05558>
2. C. Holmgren, T. Harkany, B. Svennenfors, and Y. Zilberter. Pyramidal cell communication within local networks in layer 2/3 of rat neocortex. The Journal of Physiology, 551(1):139–153, 8 2003. ISSN 0022-3751. doi:10.1113/jphysiol.2003.044784. URL <http://www.jphysiol.org/cgi/doi/10.1113/jphysiol.2003.044784>
3. A. Makhzani и B. Frey. Winner-take-all autoencoders. Advances in Neural Information Processing, 2015. URL <http://papers.nips.cc/paper/5783-winner-take-all-autoencoders>
4. F. Lagunas, E. Charlaix, V. Sanh, and A. M. Rush. Block pruning for faster transformers. CoRR, 2017. URL <https://arxiv.org/abs/2109.04838>

5. Kevin Hunter, Lawrence Spracklen and Subutai Ahmad. Two Sparsities Are Better Than One: Unlocking the Performance Benefits of Sparse-Sparse Networks. CoRR, 2017. URL <https://arxiv.org/abs/2112.13896>
6. Md Aamir Raihan, Tor M. Aamodt. Sparse Weight Activation Training. CoRR, 2020. URL <https://arxiv.org/abs/2112.13896>
7. Xuanyao Chen, Zhijian Liu, Haotian Tang, Li Yi, Hang Zhao, Song Han. SparseViT: Revisiting Activation Sparsity for Efficient High-Resolution Vision Transformer. CoRR, 2023. URL <https://arxiv.org/abs/2303.17605>.
8. S. Hooker. The Hardware Lottery, 2020. URL <http://arxiv.org/abs/2009.06489>.

References

1. . N. C. Thompson, K. H. Greenewald, K. Lee, and G. F. Manso. The Computational Limits of Deep Learning. CoRR, 2022. URL <https://arxiv.org/abs/2007.05558>
 2. C. Holmgren, T. Harkany, B. Svennenfors, and Y. Zilberter. Pyramidal cell communication within local networks in layer 2/3 of rat neocortex. The Journal of Physiology, 551(1):139–153, 8 2003. ISSN 0022-3751. doi:10.1113/jphysiol.2003.044784. URL <http://www.jphysiol.org/cgi/doi/10.1113/jphysiol.2003.044784>
 3. A. Makhzani and B. Frey. Winner-take-all autoencoders. Advances in Neural Information Processing, 2015. URL <http://papers.nips.cc/paper/5783-winner-take-all-autoencoders>
 4. F. Lagunas, E. Charlaix, V. Sanh, and A. M. Rush. Block pruning for faster transformers. CoRR, 2017. URL <https://arxiv.org/abs/2109.04838>
 5. Kevin Hunter, Lawrence Spracklen and Subutai Ahmad. Two Sparsities Are Better Than One: Unlocking the Performance Benefits of Sparse-Sparse Networks. CoRR, 2017. URL <https://arxiv.org/abs/2112.13896>
 6. Md Aamir Raihan, Tor M. Aamodt. Sparse Weight Activation Training. CoRR, 2020. URL <https://arxiv.org/abs/2112.13896>
 7. Xuanyao Chen, Zhijian Liu, Haotian Tang, Li Yi, Hang Zhao, Song Han. SparseViT: Revisiting Activation Sparsity for Efficient High-Resolution Vision Transformer. CoRR, 2023. URL <https://arxiv.org/abs/2303.17605>.
 8. S. Hooker. The Hardware Lottery, 2020. URL <http://arxiv.org/abs/2009.06489>.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.15

СРАВНЕНИЕ РЕЛЯЦИОННЫХ СУБД С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Ветров С.Ю.

ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: vetrov241201@yandex.ru

Статья представляет собой обзор наиболее популярных реляционных систем управления базами данных (СУБД) с открытым исходным кодом, таких как MySQL, PostgreSQL, MariaDB и SQLite. Она охватывает ключевые аспекты, которые отличают эти СУБД, включая архитектуру, сложность установки, расширяемость, мониторинг производительности и удобство изучения. Сравнительный анализ также включает в себя производительность, совместимость, возможности резервного копирования и восстановления данных, а также уровни поддержки ACID-транзакций и целостности данных.

Ключевые слова: СУБД, Реляционные СУБД, СУБД с открытым исходным кодом, SQL, Сравнение СУБД.

COMPARISON OF OPEN SOURCE RELATIONAL DBMS

Vetrov S.Y.

MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: vetrov241201@yandex.ru

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

Keywords: DBMS, Relational DBMS, Open source DBMS, SQL, DBMS comparison.

Введение

Реляционные системы управления базами данных с открытым исходным кодом (СУБД) играют ключевую роль в современной разработке программного обеспечения и корпоративных приложениях. Примеры таких систем — MySQL, PostgreSQL, MariaDB и SQLite. Эти базы данных предлагают функции, которые удовлетворяют широкому спектру потребностей: от простого хранения данных до сложной аналитики, делая их незаменимыми как для разработчиков, так и для бизнеса. Открытый исходный код способствует сотрудничеству сообщества, быстрой инновации и снижению затрат, что делает их еще более востребованными в эпоху, когда принятие решений на основе данных стало критически важным.[1][2][3]

Ряд архитектурных различий, особенности настройки и производительности делают каждую из этих СУБД уникальной. PostgreSQL, с его расширенными возможностями и строгим соблюдением стандартов, часто выбирают для приложений, требующих сложных запросов и работы с большими объемами данных. MySQL, известный своей простотой и

скоростью, чаще используется в веб-приложениях, таких как системы управления контентом и онлайн-сервисы.[4][5][6] Легкая бессерверная архитектура SQLite делает его идеальным для мобильных и встроенных приложений.[7]

Сравнение этих систем порой вызывает дискуссии по вопросам производительности, особенно в многозадачных сценариях. Например, PostgreSQL часто превосходит MySQL при высокой нагрузке, в то время как MySQL показывает лучшие результаты в операциях с большим объемом чтения. Разные подходы к обеспечению ACID и варианты механизмов хранения данных в MySQL приводят к вопросам надежности транзакций в сравнении с PostgreSQL, где эти принципы соблюдаются более последовательно.[8]

В конечном итоге выбор реляционной СУБД с открытым исходным кодом определяется конкретными потребностями проекта, включая масштабируемость, целостность данных и сложность взаимосвязей. Осведомленность о ключевых особенностях и ограничениях каждой системы позволяет разработчикам принимать обоснованные решения, отвечающие требованиям приложения и его эксплуатационным нуждам.[9][10][11]

Архитектура баз данных

При сравнении реляционных СУБД с открытым исходным кодом, таких как MySQL, PostgreSQL, MariaDB и SQLite, важную роль играет их архитектура. Несмотря на принадлежность к реляционным системам, у каждой из них есть архитектурные особенности, влияющие на производительность и масштабируемость. Например, PostgreSQL известен своей объектно-реляционной моделью, которая поддерживает сложные типы данных и взаимосвязи, в то время как MySQL следует более простому реляционному подходу, подходящему для менее сложных приложений.[1][2]

Сложность установки и настройки

Проще всего развертывается SQLite благодаря бессерверной архитектуре и настройке с нулевой конфигурацией. MariaDB и MySQL также легко устанавливаются, что удобно для быстрой проверки концепции. Настройка PostgreSQL может быть более трудоемкой и требует дополнительных шагов, что может быть сложным для новичков.[2]

Расширяемость и настройка

PostgreSQL ценится за широкие возможности расширяемости, включая поддержку пользовательских функций и типов данных, что позволяет адаптировать его под уникальные случаи использования. В то время как MySQL также можно настроить, уровень его расширяемости не так высок, как у PostgreSQL.[1][3]

Мониторинг производительности

Производительность — важный критерий сравнения, и каждая СУБД предлагает различные средства мониторинга. MySQL предоставляет performance schema для отслеживания событий и выполнения запросов, позволяя администраторам выявлять узкие места. PostgreSQL включает встроенные функции для анализа производительности, хотя иногда требуется дополнительная настройка.[4][5]

Совместимость и миграция

При переходе с проприетарных систем на открытые СУБД возникают вопросы совместимости с устаревшими приложениями. Простота интеграции и поддержки старых систем различается в зависимости от базы данных, что может повлиять на успешность миграции.[5] Оценка этих аспектов помогает выбрать наиболее подходящую для проекта СУБД с открытым исходным кодом.

Обзор популярных СУБД с открытым исходным кодом

СУБД с открытым исходным кодом, такие как MySQL, PostgreSQL, MariaDB и SQLite, широко используются благодаря надежности, производительности и поддержке сообщества. MySQL и PostgreSQL особенно выделяются своими функциями и подходят для использования в корпоративных ИТ-системах.

MySQL

Запущенная в 1995 году MySQL зарекомендовала себя как надежная СУБД для веб- и корпоративных приложений. Ее отличают высокая производительность, простота и масштабируемость. MySQL поддерживает транзакции ACID, что обеспечивает целостность данных, и широко используется, с учетом исследования Stack Overflow 2020 года, где ее выбрали 55,6% респондентов.[7]

Ключевые особенности MySQL

- Многопользовательская поддержка для одновременного доступа к базе данных.
- Гибкость: бесплатная версия MySQL Community Server и коммерческая MySQL Enterprise Edition.
- Совместимость с Windows, macOS и Linux, что делает ее удобной для разных сред.[4]–[8]

PostgreSQL

PostgreSQL считается одной из самых надежных баз данных с открытым исходным кодом, часто сравниваемой с коммерческими решениями вроде Oracle и DB2. Она поддерживает расширенные типы данных и мощные индексации, что делает ее привлекательной для аналитических и транзакционных приложений.

Сравнение и примеры использования

Выбор между PostgreSQL и MySQL зависит от требований приложения. PostgreSQL отлично подходит для задач с высокой нагрузкой и сложными запросами, тогда как производительность и простота MySQL делают ее оптимальным выбором для веб-приложений. Обе системы продолжают развиваться, чтобы соответствовать требованиям современного рынка.

Ключевые отличия

- Соответствие ACID и целостность данных: PostgreSQL последовательно поддерживает принципы ACID, что делает его более надежным для транзакций. Не все механизмы хранения MySQL (например, MyISAM) обеспечивают соответствие ACID, в отличие от InnoDB, который это поддерживает.

- Масштабируемость и параллелизм: PostgreSQL использует многоверсионность и позволяет эффективно обрабатывать параллельные соединения, тогда как модель потоков в MySQL может снижать производительность при высокой нагрузке. [4][11]
- Возможности и гибкость: PostgreSQL поддерживает пользовательские типы данных и JSON/JSONB, что делает его более универсальным для современных приложений, тогда как MySQL ориентирован на базовые реляционные функции.
- Резервное копирование и восстановление: PostgreSQL предлагает потоковую репликацию и другие инструменты для резервного копирования, в то время как возможности MySQL зависят от механизма хранения.

Заключение

Выбор между MySQL и PostgreSQL, а также другими СУБД с открытым исходным кодом, зависит от конкретных требований проекта и особенностей его реализации. Оба решения предоставляют мощные функции и возможности, однако их характеристики могут быть более или менее подходящими в зависимости от задач, которые необходимо решить.

Разработчики должны учитывать такие факторы, как производительность, масштабируемость, соответствие ACID, возможность кастомизации и поддержки различных типов данных. Понимание сильных и слабых сторон каждой СУБД поможет принимать обоснованные решения и создавать более эффективные и надежные приложения.

С учетом быстрого развития технологий и изменения требований рынка, остаётся актуальным постоянное изучение и оценка новых функций и возможностей, которые предлагают эти системы, чтобы гарантировать, что выбор остаётся актуальным и соответствует современным стандартам и ожиданиям пользователей.

Список литературы

1. PostgreSQL против MySQL: Подробное сравнение для инженеров по обработке данных. — Текст : электронный // airbyte : [сайт]. — URL: <https://airbyte.com/data-engineering-resources/postgresql-vs-mysql>.
2. Реляционные базы данных: PostgreSQL Vs. MariaDB Vs. MySQL Vs. SQLite. — Текст : электронный // dev.to : [сайт]. — URL: <https://dev.to/strapi/relational-databases-postgresql-vs-mariadb-vs-mysql-vs-sqlite-5dn7>.
3. Частичные индексы. — Текст : электронный // sqlite : [сайт]. — URL: <https://sqlite.org/partialindex.html>.
4. Современное руководство по мониторингу производительности MySQL. — Текст : <url> // среда : [сайт]. — URL: <https://medium.com/@MetricFire/a-modern-guide-to-mysql-performance-monitoring-bd74bb89b22c>.
5. От проприетарного к открытому исходному коду: Полное руководство по миграции баз данных. — Текст : электронный // страница : [сайт]. — URL: <https://www.percona.com/blog/the-complete-guide-to-database-migration>.
6. В чем разница между MariaDB и PostgreSQL. — Текст : электронный // хеводата : [сайт]. — URL: <https://hevodata.com/learn/differences-between-mariadb-vs-postgresql/>.
7. Краткая история управления базами данных. — Текст : электронный // dataversity : [сайт]. — URL: <https://www.dataversity.net/brief-history-database-management/>.

-
8. Что такое MySQL?. — Текст : электронный // geeksforgeeks : [сайт]. — URL: <https://www.geeksforgeeks.org/what-is-mysql/>.
 9. SQLite против MySQL против PostgreSQL – Поиск “Лучшей” Системы Управления Реляционными Базами Данных. — Текст : <url> // runcloud : [сайт]. — URL: <https://runcloud.io/blog/sqlite-vs-mysql-vs-postgresql>.
 10. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОПУЛЯРНЫХ СУБД С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ: ОЦЕНКА ЭФФЕКТИВНОСТИ ДЛЯ ИТ-СПЕЦИАЛИСТОВ. — Текст : электронный // academia : [сайт]. — URL: https://www.academia.edu/11664600/BENCHMARKING_POPULAR_OPEN_SOURCE_RDBMS_A_PERFORMANCE_EVALUATION_FOR_IT_PROFESSIONALS.
 11. PostgreSQL против MySQL: 11 критических отличий. — Текст : электронный // данные : [сайт]. — URL: <https://hevodata.com/learn/postgresql-vs-mysql/>.

References

1. PostgreSQL vs MySQL: A Detailed Comparison for Data Engineers. — Текст : электронный // airbyte : [сайт]. — URL: <https://airbyte.com/data-engineering-resources/postgresql-vs-mysql>.
 2. Relational Databases: PostgreSQL Vs. MariaDB Vs. MySQL Vs. SQLite. — Текст : электронный // dev.to : [сайт]. — URL: <https://dev.to/strapi/relational-databases-postgresql-vs-mariadb-vs-mysql-vs-sqlite-5dn7>.
 3. Partial Indexes. — Текст : электронный // sqlite : [сайт]. — URL: <https://sqlite.org/partialindex.html>.
 4. A Modern Guide to MySQL Performance Monitoring. — Текст : электронный // medium : [сайт]. — URL: <https://medium.com/@MetricFire/a-modern-guide-to-mysql-performance-monitoring-bd74bb89b22c>.
 5. From Proprietary to Open Source: The Complete Guide to Database Migration. — Текст : электронный // percona : [сайт]. — URL: <https://www.percona.com/blog/the-complete-guide-to-database-migration>.
 6. What’s the Difference Between MariaDB vs PostgreSQL. — Текст : электронный // hevodata : [сайт]. — URL: <https://hevodata.com/learn/differences-between-mariadb-vs-postgresql/>.
 7. A Brief History of Database Management. — Текст : электронный // dataversity : [сайт]. — URL: <https://www.dataversity.net/brief-history-database-management/>.
 8. What is MySQL?. — Текст : электронный // geeksforgeeks : [сайт]. — URL: <https://www.geeksforgeeks.org/what-is-mysql/>.
 9. SQLite vs MySQL vs PostgreSQL – The Search For The “Best” Relational Database Management System. — Текст : электронный // runcloud : [сайт]. — URL: <https://runcloud.io/blog/sqlite-vs-mysql-vs-postgresql>.
 10. BENCHMARKING POPULAR OPEN SOURCE RDBMS: A PERFORMANCE EVALUATION FOR IT PROFESSIONALS. — Текст : электронный // academia : [сайт]. — URL: https://www.academia.edu/11664600/BENCHMARKING_POPULAR_OPEN_SOURCE_RDBMS_A_PERFORMANCE_EVALUATION_FOR_IT_PROFESSIONALS.
 11. PostgreSQL vs MySQL: 11 Critical Differences. — Текст : электронный // hevodata : [сайт]. — URL: <https://hevodata.com/learn/postgresql-vs-mysql/>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

ОСНОВНЫЕ ИСТОЧНИКИ УГРОЗ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Чвала Д.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:
chvala_d@mail.ru

В данной статье обзревается основные источники угроз безопасности персональных данных. В повседневной жизни человека безопасность информации о его жизни зависит от него самого. Но ситуация совершенно иная, когда мы обязаны предоставлять данные о нас третьим лицам, в частности работодателю, в соответствии с законом. В этой ситуации сотрудник передает конфиденциальную информацию о себе для хранения. Кроме того, работодатель уже отвечает за безопасность данных. Он обязан защищать информацию о сотрудниках от посягательств третьих лиц и несет ответственность за передачу этих данных. Возрастающая сложность методов и средств организации машинной обработки, широкое использование глобальной сети Интернета приводят к тому, что информация становится все более уязвимой

Ключевые слова: Угрозы, безопасность, персональные данные, классификация угроз.

MAIN SOURCES OF THREATS IN PERSONAL DATA INFORMATION SYSTEMS

Chvala D.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: chvala_d@mail.ru

This article reviews the main sources of threats to the security of personal data. In a person's daily life, the security of information about his life depends on him. But the situation is completely different when we are obliged to provide data about us to third parties, in particular to the employer, in accordance with the law. In this situation, the employee transfers confidential information about himself for storage. In addition, the employer is already responsible for data security. He is obliged to protect information about employees from the encroachments of third parties and is responsible for the transfer of this data. The increasing complexity of methods and means of organizing machine processing, the widespread use of the global Internet network lead to the fact that information is becoming more vulnerable

Keywords: Threats, security, personal data, classification of threats.

Введение

Сначала стоит вспомнить само понятие о персональных данных:

- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
- Информация может храниться в разных видах:
- Устная;

- Визуальная;
- Цифровая форма.

Информация в устном виде передается по акустическим путям: аудио воспроизведение, речь и т.д. Визуальная – отображение на каких-либо физических носителях: печатные документы, отображение на экранах девайсов и т.д., и, наконец, цифровая – информация, располагающаяся на цифровых носителях, хранящаяся в системах информационной среды и прочее. [1]

К разной информации есть разные варианты несанкционированного доступа, которые может использовать нарушитель. Все зависит от уровня его доступа к системе, которая стала его целью. Также это может зависеть от таких факторов, как неаккуратность работающего персонала в компании, которая причастна к работе системы хранения персональных данных, или от имеющихся методов несанкционированного доступа у нарушителя, либо произошедший случай инцидента был случайным и лицо, ставшее нарушителем, не имело целей прийти к таким результатам.

Общая характеристика источников угроз в информационных системах персональных данных.

НСД может быть реализован в ИСПД с использованием программного и аппаратного обеспечения, если осуществление несанкционированного, в том числе случайного, доступа, которое нарушает конфиденциальность, целостность и доступность ПДн, и включает в себя:

- угрозы несанкционированного доступа к операционной среде компьютера со стандартным программным обеспечением (инструменты операционной системы или общие прикладные программы);
- угрозы создания нестандартных режимов работы программных (программных) средств путем преднамеренного изменения официальных данных, игнорирования ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных. [2]

Кроме того, возможны комбинированные угрозы, которые представляют собой комбинацию этих угроз. Например, внедрение вредоносного ПО может создать условия для NRD в операционной среде компьютера, в том числе путем формирования нетрадиционных информационных каналов для доступа. Угрозы несанкционированного доступа к операционной среде программного обеспечения по умолчанию делятся на прямые и удаленные угрозы. Прямой доступ осуществляется через программный и аппаратный ввод-вывод компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевой связи. Такие угрозы угрожают ISPD как на основе рабочего места, которое не является членом общедоступной сети связи, так и на всех интернет-провайдерах, которые подключаются к сетям связи и международным сетям для обмена информацией.

Классификация угроз информационной безопасности персональных данных.

Под угрозой информационной безопасности понимается угроза нарушения свойств информационной безопасности – доступности, целостности или конфиденциальности информационных активов организации. Перечень угроз, оценка вероятности их реализации, а также модель злоумышленника составляют основу для анализа риска угроз и формулировки требований по защите автоматизированной системы. Помимо выявления возможных угроз,

необходимо проанализировать выявленные угрозы на основе их классификации по ряду признаков. Угрозы, соответствующие каждому признаку классификации, позволяют вам подробно изложить требования, отраженные в этом признаке. Поскольку информация, которая хранится и обрабатывается в современных автоматизированных системах управления, подвергается воздействию чрезвычайно большого количества факторов, формализовать задачу и описать полный набор угроз становится невозможным. Чтобы поделить нарушителей на категории, надо проанализировать их отношение к системе персональных: человек может быть либо сотрудником организации, имеющей доступ к системе персональных данных, либо может быть не связан с ней, но иметь цель получить несанкционированный доступ к данным.

Отсюда можно поделить нарушителей на две категории:[3]

- 1 категория: лица, имеющие доступ в информационной системе персональных данных;
- 2 категория: лица, не имеющие доступ к информационной системе персональных данных.

Еще одна категория, на которую можно разделить нарушителей, это категория относительно местоположения: внутри или вне контролируемой зоны.

Отсюда еще две группы: внешние нарушители и внутренние нарушители.

Несмотря на две последние группы, 1 категория нарушителей имеет как внутренних нарушителей, так и внешних. Последними могут быть те же лица из внутренней категории, находящиеся за территорией контролируемой зоны. Такие лица имеют достаточное количество знаний об информационной системе персональных данных для совершения атаки или создания инцидента.[4]

Нормативно-правовое регулирование.

Федеральный закон «О персональных данных» предусматривает, что данные граждан, их личная жизнь, имущественный статус и состояние здоровья, хранимые и обработанные в информационных системах, не может быть неправомерно передано третьим лицам. Несовершенство системы обработки информации нередко приводит к утечке важных данных, включая персональные данные. Утечка может быть случайной или преднамеренной. Для того, чтобы избежать подобных ситуаций, которые могут причинить вред гражданам, разработаны специальные стандарты для информационных систем. Для организации, признанной в соответствии с законом оператором персональной информации, технические требования к системам обработки данных устанавливаются приказами ФСТЭК РФ. В настоящее время действует распоряжение №21, вступившее в силу 2013 года, которое определяет технические, организационные и технические мероприятия по обеспечению защиты персональной информации. Оно неоднократно было дополнено и изменено в зависимости от требований времени. В структуре документа в приложении о составе мер содержатся рекомендации о регулировании:

- Идентификацию и аттестацию лиц, допускаемых операторами к обработке данных;
- Управление доступом к ним;
- Программную среду и ограничения;
- Физическую защиту компьютеров, в которых содержатся данные, связанные с персональной информацией;
- Правила регистрации происшествий безопасности;

- Правила организации антивирусных защит;
- Правила фиксации попадания в защищенные информационные периметры;
- Отслеживание защищенности личных данных;
- Защита технического обеспечения.

Выбор мер технической и организационной защиты личных данных будет зависеть от класса защиты информационных систем, определённого по правилам, предусмотренными постановлением Правительства №1119.[5]

Заключение.

В заключение можно отметить, что защита персональных данных в информационных системах является одной из ключевых задач современной кибербезопасности. Множество угроз, таких как несанкционированный доступ к операционной среде, преднамеренное искажение данных или внедрение вредоносного программного обеспечения, требуют комплексного подхода к обеспечению безопасности. Важно не только выявлять потенциальные угрозы, но и классифицировать их для разработки эффективных мер защиты. Федеральные нормативно-правовые акты, такие как закон «О персональных данных» и распоряжения ФСТЭК, играют важную роль в создании четких требований к защите данных. Комплекс мер, включающий управление доступом, контроль за информационными потоками, защиту физической и программной среды, должен применяться с учетом специфики информационной системы и степени угроз, что позволит минимизировать риски и обеспечить надежную защиту персональных данных.

Список литературы

1. Цветков, А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux/А.Ю.Цветков//Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662
2. Исследование существующих механизмов защиты операционных систем семейства Linux / А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662.
3. Багомедова А.Р., Ушаков И.А., Цветков А.Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник статей VII Международной научно-технической и научно-методической конференции. 2018. С. 58-63.
4. Катасонов А. И. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU Linux /А.И.Катасонов, С.И.Штеренберг, А.Ю.Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – No 2. – С. 50-56.
5. Захарова Т.Е., Цветков А.Ю. Анализ существующих нормативных документов для формирования политики безопасности в системе электронного документооборота

вуза//В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. СПб.: СПбГУТ, 2017. С. 337-343.

References

1. Tsvetkov, A.Yu. Research of existing mechanisms of protection of operating systems of the Linux family / A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VII International Scientific, Technical and scientific-methodological conference: collection of scientific articles in 4 volumes St. Petersburg: St. Petersburg State University, 2018. pp. 657-662
 2. Investigation of the existing protection mechanisms of the operating systems of the family Linux / A.Y. Tsvetkov // Actual problems of infotelecommunications in science and education. VII International Scientific, Technical and scientific-methodological conference: collection of scientific articles in 4 volumes St. Petersburg: St. Petersburg State University, 2018. pp. 657-662.
 3. Bagomedova A.R., Ushakov I.A., Tsvetkov A.Yu. Development of methods for verifying the compliance of virtualization servers with security requirements according to GOST R 56938-2016 standard // Actual problems of infotelecommunications in science and education (APINO 2018): collection of articles of the VII International Scientific, Technical and scientific-methodological Conference. 2018. pp. 58-63.
 4. Katasonov, A. I. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in GNU Linux operating systems / A. I. Katasonov, S. I. Shterenberg, A. Yu. Tsvetkov // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 2. – pp. 50-56.
 5. Zakharova T.E., Tsvetkov A.Y. Analysis of existing regulatory documents for the formation of a security policy in the electronic document management system university // In the collection: Current problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International Scientific , technical and scientific-methodical Conference. In 4 volumes. Edited by S.V. Bachevsky. St. Petersburg: St. Petersburg State University, 2017. pp. 337-343.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.65:004.623

ПРИМЕНЕНИЕ МЕТОДОВ РЕСТРУКТУРИЗАЦИИ И ДУБЛИРОВАНИЯ ДЛЯ ОТОБРАЖЕНИЯ РЕЗУЛЬТАТОВ ЗАПРОСОВ В ООСУБД НИКА

Тищенко В.А.

ФГУ "ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР "ИНФОРМАТИКА И УПРАВЛЕНИЕ" РОССИЙСКОЙ АКАДЕМИИ НАУК", Москва, Россия, (119333, город Москва, ул. Вавилова, д.44 к.2), ОЧУ ВО "ПРАВОСЛАВНЫЙ СВЯТО-ТИХОНОВСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ" (115184, город Москва, Новокузнецкая ул., д. 23б), e-mail: vtischenko@isa.ru

Альтернативным методом представления данных по отношению к методам отображения, инкапсулируемыми объектами БД, является реструктуризация иерархических объектов базы данных. В частности в ООСУБД НИКА данный метод позволяет изменить ключ основного массива для представления результатов запроса в виде дерева, упорядоченного на основе другого ключа. Данный метод представляет вершины дерева результата в нужном пользователю порядке. Ограничением процесса реструктуризации является то, что терминальная вершина, выбираемая в качестве нового ключа, должна уникальным образом идентифицировать элемент массива. Для иллюстрации процесса реструктуризации приводится пример объекта 'Дела' типа массив, в котором изменяется ключевая вершина 'Номер' на ключевую вершину 'ФИО'. Метод дублирования используется для расширения отображения ключей дополнительной информацией, содержащей значения терминальных вершин с подчиненного уровня.

Ключевые слова: Реструктуризация иерархических объектов, запросная система ООСУБД НИКА, методы отображения объектов.

APPLICATION OF RESTRUCTURING AND DUPLICATION METHODS FOR REPRESENTATION QUERY RESULTS IN NIKA OODBMS

Tishchenko V.A.

FEDERAL RESEARCH CENTER "INFORMATICS AND MANAGEMENT" OF THE RUSSIAN ACADEMY OF SCIENCES", Moscow, Russia, (119333, Moscow, Vavilova str., 44, bldg. 2), ST. TIKHON'S ORTHODOX HUMANITARIAN UNIVERSITY (115184, Moscow, Novokuznetskaya str., 23b), e-mail: vtischenko@isa.ru

An alternative method of data representation in relation to the representation methods encapsulated by DB objects is the restructuring of hierarchical database objects. In particular, in the NIKA OODBMS this method allows changing the key of the main array to present the query results as a tree ordered based on another key. This method presents the nodes of the result tree in the order required by the user. A limitation of the restructuring process is that the terminal node selected as the new key must uniquely identify the array element. To illustrate the restructuring process, an example of the 'Case' object of the array type is given, in which the key vertex 'Number' is changed to the key vertex 'FullName'. The duplication method is used to expand the representation of keys with additional information containing the values of terminal nodes from a subordinate level.

Keywords: Restructuring of hierarchical objects, request system of OODBMS NIKA, methods of objects representation.

Введение

Идею реструктуризации иерархических объектов развивает в своей статье [1] Абитебул. Исходной предпосылкой для реструктуризации является понятие “релятивизма данных”, т.е. одни и те же данные могут быть представлены различными способами посредством различных схем описания данных. Абитебул основывает релятивизм данных на структурном преобразовании типов. Рассмотрим преобразование типа, которое приводит к массиву с ключом, соответствующим другой терминальной вершине той же самой структуры. Тогда с преобразованием типов можно связать функцию преобразования объектов этих типов. Такая функция называется *функцией реструктуризации*.

Обоснование применения функции реструктуризации

Методы (спецификации) отображения объектов БД в гипертекстовые документы описаны в статье [2]. В [3,4] показано, что существует только четыре общих типа представления данных на двумерной плоскости (в документе): последовательность — одномерное представление, таблица — двумерное представление, иерархия — n -мерное представление и их комбинации. Среди методов отображения объектов существует метод RN (rename), который присваивается элементу массива типа структура. Он не меняет общего типа представления данных, а позволяет отображать ключ элемента массива в виде одной или нескольких подчиненных терминальных вершин. При этом элементы массива остаются упорядоченными в соответствии с исходным ключом. Проблему, связанную с изменением порядка следования элементов всего массива и идентификации элементов по новому ключу, решает реструктуризация.

Формальное определение функции реструктуризации

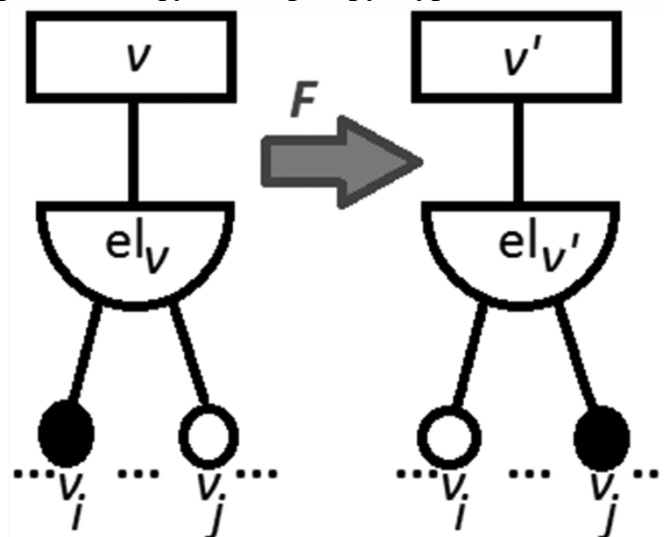


Рисунок 1.- Преобразование типа F , изменяющее ключ массива (закрашенный кружок)

Более формально, в соответствии с определением в статье [2] тип объекта БД — это граф с тремя основными подмножествами вершин: V^* — терминальные вершины, $V^\#$ — массивы, V° — структуры. Вершины указанных поименованных типов составляют иерархию вершин в БД. Типы естественным образом именуются названиями вершин. Также определяют два дополнительных типа вершин: V^p — ссылка на шаблон и V^r — ссылка на значение. Вершины типа ссылка на значение позволяют строить граф произвольной сложности. Таким образом, имеются базовые типы данных V^* , конструкторы новых типов $V^\#$, V° и повторное использование

типов V^p , V^r . Тип нетерминальных вершин определяется рекурсивно через типы подчиненных им вершин. Тогда преобразование типа, изменяющее ключ массива имеет вид $F: T(v) \rightarrow T(v')$, где $v, v' \in V^\#$, т.е. $T(v) = [T(e_{lv})]$ и $T(v') = [T(e_{lv'})]$, причем $T(e_{lv}) = \{T(v_1), \dots, T(key_v), \dots, T(v_n)\}$, $T(e_{lv'}) = \{T(v_1), \dots, T(key_{v'}), \dots, T(v_n)\}$, $key_v = v_i$, $key_{v'} = v_j$, $v_i, v_j \in V^*$, $i \neq j$, терминальные вершины v_i и v_j должны однозначно идентифицировать элементы массивов v и v' соответственно (см. Рис.1).

Здесь символ el обозначает элемент массива типа структура, а key — ключевую вершину массива. Массивы v и v' отличаются только ключами и *мощность* их структур данных будет одинаковой, но упорядочены они будут по разным ключам v_i и v_j соответственно. Остальные вершины структуры e_{lv} , если это необходимо, преобразование F тождественно переводит в самих себя в структуре $e_{lv'}$. Реструктуризацию, изменяющую ключ массива v , определим как функцию f преобразования объектов типа $T(v)$ в объекты $T(v')$: $f(O(v)) = O(v')$, причем типы $T(v)$ и $T(v')$ связаны преобразованием типов F в определенном выше смысле. Функция реструктуризации f преобразует каждый объект типа $O(v)$ в соответствующий объект типа $O(v')$.

Реструктуризация посредством OOML

(a) Home page NIKA_ROOT Дела ▼

Дела
001.107
Вихрев Илья Николаевич
Фамилия Вихрев
Год рождения 1869
Место рождения Владимирская губ., г.Суздаль
Из мещан г.Суздаль
ПЕРИОДЫ - [1]
ЖИЗНИ
Реабилитация
Документы

001.1074
Браиловский (Брайловский?) Александр Николаевич
Фамилия Браиловский
Год рождения 1880
протоиерей

(b) Home page NIKA_ROOT Прославленные новомученики ▼

Прославленные новомученики
Абакумова (Аббакумова) Надежда Петровна
Номер oc4.1549
=>
Абиссов Александр Александрович
Номер oc4.1550
=>
Абрамов Михаил Иванович
Номер oc4.1551
=>
Абросимов Федор Семенович
Номер oc2.140
=>
Августа (Защук) Лидия Васильевна
Номер okn.32
=>
Августин (Беляев) Александр Александрович
Номер oc32.962

(c) Home page NIKA_ROOT ОписанияГруппДел ▼

ОписанияГруппДел
d01.1
"дело епископа Гавриила (Абалымова) и др., 1931г."
Архив ЦА ФСБ РФ. ДР-35500.
КолЧеловек 33
ПриблКолЧеловек 1 епископ
ОсновныеОбвиняемые
ПериодСледствия
Ор
СписокПострадавших

d01.10
"Дело "Южно-Русского Синода", под руководством митр
Архив Архив УКГБ Краснодарского края. ДП-48721.
КолЧеловек 31
ПриблКолЧеловек 1 митрополит. 1 епископ. 1 архиепископ. неог

(d) Home page NIKA_ROOT ГрупповыеДела ▼

ГрупповыеДела
"Антисоветское церковное подполье", 1943
Номер_пт d01.8
=>
"Дело "Антисоветской группы черносотен
ГрупповыеДела
S
ГрупповоеДело
Номер_пт
=> -> .ОписанияГруппДел.*(-Номер_пт)
"Дело "Южно-Русского Синода", под руко
Номер_пт d01.10
=>
"Дело 1934г. Оболенского М.Ф. и др. Ленин
Номер_пт d01.13

Рисунок 2. - Пример реструктуризации результатов запроса к массиву 'Дела' в виде массива 'Прославленные новомученики': ключ 'Номер' (a) изменяется на ключ 'ФИО' (b); пример реструктуризации массива 'ОписанияГруппДел' в виде массива 'ГрупповыеДела': ключ 'Номер_пт' (c) изменяется на ключ 'ГрупповоеДело' (d)

Object Oriented Markup Language (OOML) — объектно-ориентированный язык разметки [5] был создан для описания документного интерфейса ООСУБД НИКА. OOML является предшественником SGML [6]. Преимуществом OOML перед SGML является то, что схема документа описывается отдельным файлом (макетом), а сам документ хранится отдельно. Посредством языка OOML можно осуществлять реструктуризацию БД, выкачивая данные из БД по одному макету, а затем загружая те же самые данные в БД по другому макету.

В качестве примеров реструктуризации можно рассмотреть две дополнительные ветки в БД “За Христа пострадавшие” [7]: ‘Прославленные новомученики’ и ‘Групповые Дела’. В первом примере дополнительная корневая вершина создается как результат выгрузки данных в документ по исходному макету результатов запроса по полю ‘ЧинСвятости’ массива ‘Дела’ и последующей загрузкой документа в БД по результирующему макету. При этом исходный и результирующий макеты отличаются порядком полей ‘Номер’ и ‘ФИО’. В исходном макете первое поле (оно является ключевым) — ‘Номер’, а в результирующем макете первое поле — ‘ФИО’. Остальные вершины не загружаются в дополнительную ветку, а получаются посредством ссылочной вершины ‘=>’ по полю ‘Номер’ из массива ‘Дела’. В результирующей ветке элементы массива будут упорядочены по полю ‘ФИО’, а не по полю ‘Номер’ как в массиве ‘Дела’ (Рисунок 2 а, b). Во втором примере создается массив ‘Групповые Дела’ как результат переупорядочивания в результате реструктуризации массива ‘Описания Групп Дел’. Аналогично первому примеру в реструктуризации участвуют две терминальных вершины: ‘Номер_пп’ и ‘Групповое Дело’ (Рисунок 2 с, d). На Рисунке 2 также для каждого пункта приводится соответствующий фрагмент схемы описания данных. Определенные выше преобразование F и функция реструктуризации f отображают соответственно типы и объекты (a) в (b) и (c) в (d).

Построение индексов

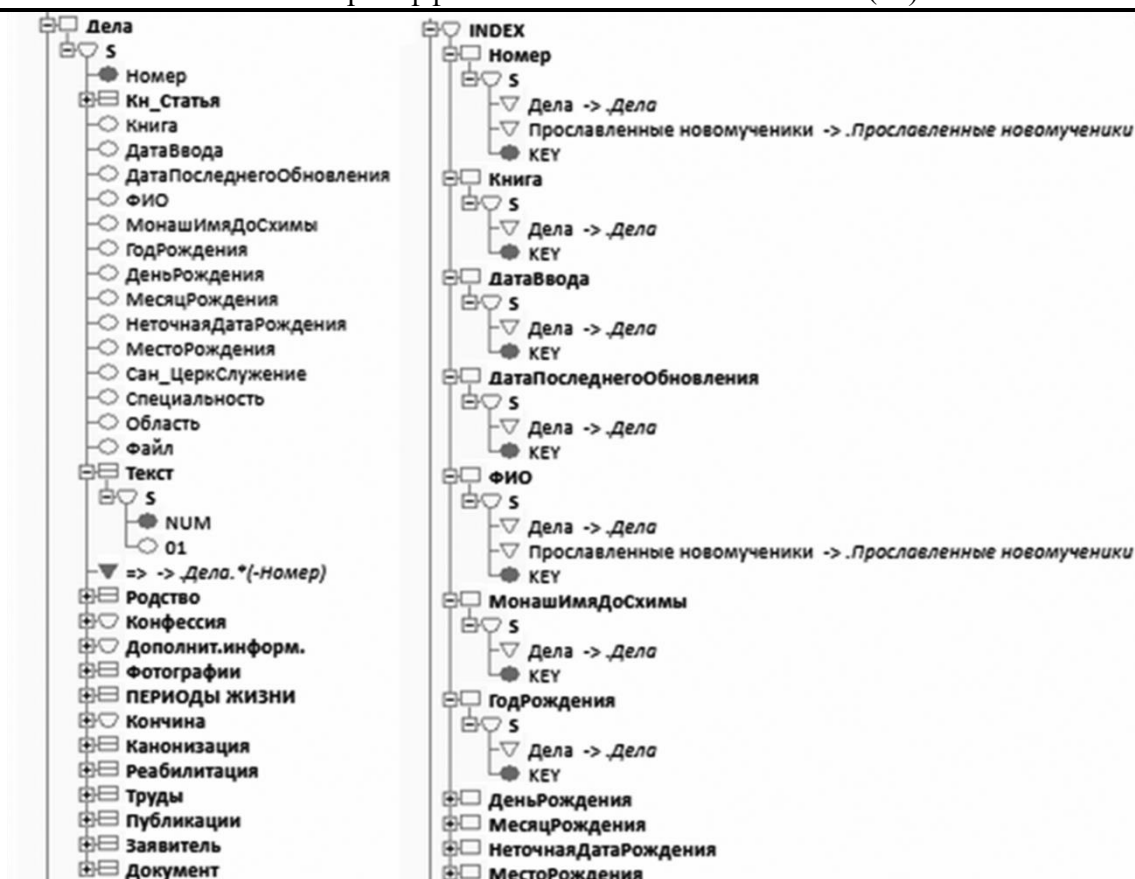


Рисунок 3. - Индексирование в ООСУБД НИКА: слева — массив ‘Дела’, справа — ‘INDEX’

Интересным применением реструктуризации служит построение индексов для атрибутивных вершин основного массива, т.е. тех терминальных вершин, которые могут участвовать в запросах. На основе описанного выше механизма, проиллюстрированного примерами, под корневой структурой ‘INDEX’ строятся одноименные с атрибутивными вершинами массивы (индексы), являющиеся результатом реструктуризации основного массива. Ключами индексов являются соответствующие атрибутивные вершины. Все значения ключей в индексах упорядочены в возрастающем порядке. Как видно из Рисунка 3 атрибутивным вершинам основного массива ‘Дела’: ‘Номер’, ‘Книга’, ‘ДатаВвода’, ‘ДатаПоследнегоОбновления’, ‘ФИО’ и т.д. соответствуют одноименные массивы под вершиной ‘INDEX’. Структура ‘INDEX’ используется как набор точек входа в основной массив, а также для выполнения запросов к БД.

Отображение результатов запроса

Приведенные примеры реструктуризации не затрагивают структуры основного массива, а представляют собой некоторые “надстройки” над основным массивом в той же БД. Однако существуют случаи, в которых требуется сделать реструктуризацию самого основного массива и построить на основе реструктуризованного массива отдельную БД, в которой все подмассивы индексов основного массива будут перестроены на основе нового ключа.

Результатом запроса [8] является массив, структура которого повторяет структуру объекта запроса, являющегося корневым массивом или его подмассивом. Интерфейс информационно-поисковой системы представляет собой обозреватель интернет, являющийся гипертекстовой системой. О близости моделей гипертекста и ООСУБД НИКА говорится в статье [9]. Результат запроса отображается в виде иерархии вершин объекта запроса, которые удовлетворяют

условиям запроса. В случае *суррогатных* ключей в основном массиве и его подмассивах просмотр иерархии результатов запроса может быть затруднительным. Результат применения реструктуризации к основному массиву ‘Дела’ показан на Рисунке 4.

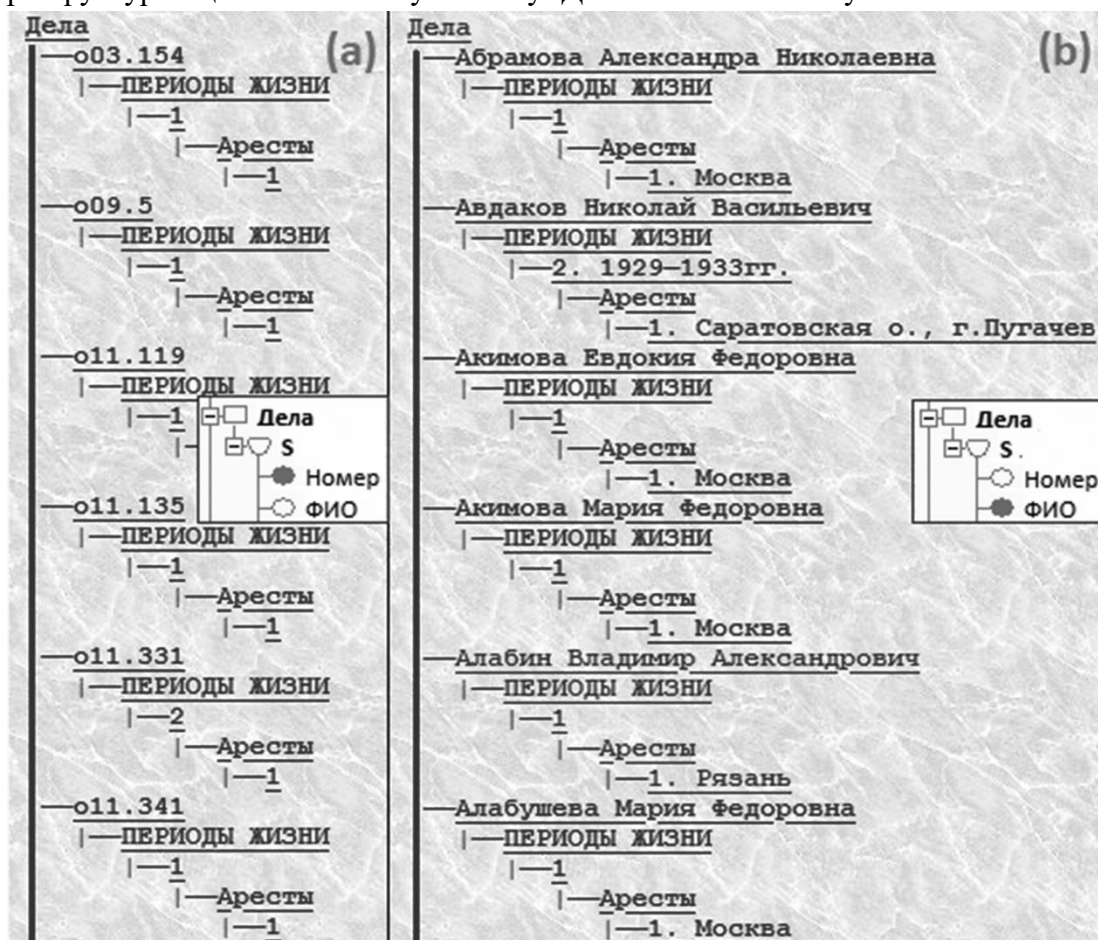


Рисунок 4.- Результат запроса до (а) и после (b) реструктуризации со схемными вставками

На Рисунке 4 также приведены фрагмент исходной схемы (а) и результирующей схемы (b), на которых обозначены ключевые вершины ‘Номер’ (а) и ‘ФИО’ (b).

Метод дублирования данных

Все подмассивы основного массива ‘Дела’ являются нумерованными. Результат запроса на Рисунке 4,а получается малоинформативным для подмассивов ‘ПЕРИОДЫ ЖИЗНИ’ и ‘Аресты’. Для повышения информативности выдаваемого результата метод реструктуризации был дополнен методом дублирования данных отдельных подчиненных терминальных вершин в ключи подмассивов. Вопрос, связанный с нарушением целостности БД при дублировании данных (например, при модификации сдублированных терминальных полей) и т.п. обсуждается в статье [10]. Результат применения метода показан на Рисунке 4,б. Если для данного элемента массива существуют терминальные вершины ‘Период жизни’ и ‘Место Ареста’, то они добавляются к ключу соответствующего подмассива.

Другие виды реструктуризации

Кроме рассмотренного в статье вида реструктуризации существует множество иных способов изменения иерархической структуры БД. Например, можно объединять в структуры

по смыслу предметной области определенные вершины, вводя новые уровни иерархии. Возможен и обратный процесс — удаление структур и расположение содержащихся в них вершин на одном уровне. При этом мощность структуры данных основного объекта, в который вложены эти вершины остается одинаковой, просто выделяются или расформируются подобъекты. В отличие от упомянутых видов реструктуризации рассмотренный вид реструктуризации основного массива “по ключу” требует перестройки всех индексов для атрибутивных вершин. Элементы массивов этих индексов содержат тип объекта “ссылка на шаблон”, повторно использующий тип основного массива. Это означает, что при смене ключа на другую терминальную вершину в основном массиве во всех “ссылках на шаблон” на этот массив произойдет такое же структурное изменение.

Цель рассмотренного преобразования улучшить читаемость отображаемой для пользователя иерархической структуры данных, полученной в результате запроса, а также всех подструктур индексов основного массива. Метод реструктуризации основного массива “по ключу” был дополнен методом дублирования данных для модификации суррогатных ключей подмассивов основного массива содержательными данными предметной области. Результаты данного исследования применяются в информационно-поисковой системе при публикации БД в интернет.

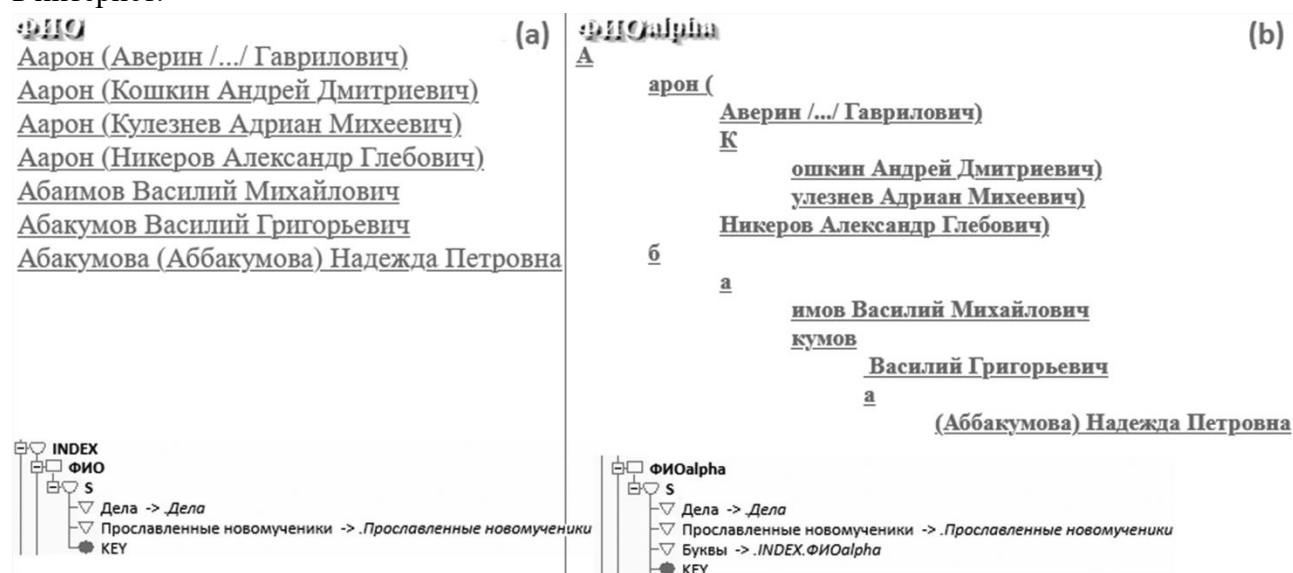


Рисунок 5. - Реструктуризация индекса по полю ‘ФИО’. Внизу схемы описания данных

Наконец, можно привести примеры видов реструктуризации, затрагивающие не только структурные вершины, но и терминальные. Неключевую вершину ‘ФИО’ можно разделить на три терминальных вершины ‘Фамилия’, ‘Имя’, ‘Отчество’, по которым строятся отдельные индексы. Если в этом примере добавить четвертую вершину — ‘Пол’, то увеличится мощность структуры данных при реструктуризации:

Более сложным является вид реструктуризации посредством разделения ключевых вершин на части для построения многоуровневых индексов. Пример такого классификатора показан на Рисунке 5. Этот вид реструктуризации является предметом отдельного исследования. Он используется для построения оптимальных многомерных классификаторов по лексикографическому признаку [11,12].

Список литературы

1. Abiteboul S., Hull R. Restructuring hierarchical database objects. Theoretical Computer Science. v.62, 1988, pp.3-38.
2. Емельянов Н.Е., Тищенко В.А. Методы отображения объектов для построения web-сервера объектно-ориентированной базы данных // Развитие безбумажных технологий в организационных системах / Сборник трудов ИСА РАН / Под ред. д.т.н. проф. Арлазарова В.Л. и д.т.н. проф. Емельянова Н.Е. М.: URSS. 1999. С. 96-109.
3. Емельянов Н.Е. “Теоретический анализ документного интерфейса”, препринт - М: ВНИИСИ, 1987.
4. Богачева А.Н., Емельянов Н.Е. "Семантическая модель документа // Системные исследования. Ежегодник 2001 / "Едиториал УРСС", М.2003, С. 360-375.
5. Bogacheva A.N., Emeljanov N.E., Romanov A.P. Object Oriented Markup Language and Restructuring Hierarchical Database Objects // Proceeding ADBIS '95 Proceedings of the Second International Workshop on Advances in Databases and Information Systems. pp. 137-142, June 27 - 30, 1995.
6. Price L.A. Practical SGML as an introduction to SGML // ACM SIGDOC Asterisk Journal of Computer Documentation, Vol.20, Issue 2, pp.36-38. <https://doi.org/10.1145/381815.381861>
7. База данных «За Христа пострадавшие». <http://martyrs.pstbi.ru/>.
8. Богданов А.С., Емельянов Н.Е., Ерохин В.И., Романов Б.Л. Реализация запросной системы на основе XPath для ООСУБД НИКА // Труды ИСА РАН. М.: Едиториал УРСС. 2003.С. 130-146.
9. Емельянов Н.Е., Тищенко В.А. Представление гипертекста в СУБД НИКА // Технология программирования и хранения данных / Сб. трудов ИСА РАН. Т.45. Под ред. чл.-корр. РАН Арлазарова В.Л. и д.т.н. проф. Емельянова Н.Е. - М. 2009. С.17-36.
10. Арлазаров В.Л., Емельянов Н.Е. Революция 2005 года в реляционных базах данных // Технология программирования и хранения данных / Сб. трудов ИСА РАН. Т.45. Под ред. чл.-корр. РАН Арлазарова В.Л. и д.т.н. проф. Емельянова Н.Е. - М. 2009. С.10-18.
11. Тищенко В.А. OPC-trie: спецификация оптимального классификатора для СУБД НИКА // труды ИСА РАН, 2021. Т. 71. Вып. 1. С.67-71.
12. Тищенко В.А. Структура OPC-trie как новый тип индекса в СУБД НИКА // Труды ИСА РАН, 2021. Т. 71. Вып. 4. С.76-81.

References

1. . Abiteboul S., Hull R. Restructuring hierarchical database objects. Theoretical Computer Science. v.62, 1988, pp.3-38.
2. Emelyanov N.E., Tishchenko V.A. Object mapping methods for building an object-oriented database web server. Development of paperless technologies in organizational systems // Proceedings of the ISA RAS. Ed. by Doctor of Technical Sciences prof. V.L. Arlazarov and Doctor of Technical Sciences prof. Emelyanov – М.: URSS. 1999. pp. 96-109.
3. Emelyanov N.E. Theoretical analysis of the document interface. М., preprint VNIISI, 1987, p.40
4. Bogacheva A.N., Emeljanov N.E. Semantic model of a document // System research. Yearbook 2001 – М.: URSS. 2003. pp. 96-109.
5. Bogacheva A.N., Emeljanov N.E., Romanov A.P. Object Oriented Markup Language and Restructuring Hierarchical Database Objects // Proceeding ADBIS '95 Proceedings of the Second

- International Workshop on Advances in Databases and Information Systems. pp. 137-142, June 27 - 30, 1995.
6. Price L.A. Practical SGML as an introduction to SGML // ACM SIGDOC Asterisk Journal of Computer Documentation, Vol.20, Issue 2, pp.36-38. <https://doi.org/10.1145/381815.381861>
 7. Database 'for Christ suffered' <http://martyrs.pstbi.ru/> .
 8. Bogdanov A.S., Emelianov N.E., Erokhin V.I., Romanov B.L. Implementation of a query system based on XPath for the OODBMS NIKA // Organizational management and artificial intelligence. Proceedings of the ISA RAS. Ed. by Doctor of Technical Sciences prof. Arlazarov V.L. and d.t.s. prof. Emelyanov N.E. M.: URSS. 2003. pp. 130-146.
 9. Emelyanov N.E., Tishchenko V.A. Representation of hypertext in the NIKA DBMS // Technology of programming and data storage / Sat. Proceedings of the ISA RAS. T.45. Ed. Corresponding Member RAS Arlazarov V.L. and Doctor of Technical Sciences prof. Emelyanov N.E. - M. 2009. pp. 17-36.
 10. Arlazarov V.L., Emelyanov N.E. The 2005 revolution in relational databases // Technology of programming and data storage / Sat. Proceedings of the ISA RAS. T.45. Ed. by Corresponding Member RAS Arlazarov V.L. and Doctor of Technical Sciences prof. Emelyanov N.E. - M. 2009. pp. 10-18.
 11. Tishchenko V.A. OPC-trie: specification of an optimal classifier for the NIKA DBMS // Proceedings of ISA RAS, 2021, 71, No. 1. pp.67-71.
 12. Tishchenko V.A. OPC-trie structure as a new type of index in NIKA DBMS // Proceedings of ISA RAS, 2021, 71, No. 1. pp. 76-81.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

УЯЗВИМОСТИ КОНТЕЙНЕРОВ: РИСКИ, ПРИМЕРЫ И МЕТОДЫ ЗАЩИТЫ

Пивоварова У.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: pivovarova.ulyana2017@yandex.ru

С ростом популярности контейнеров и технологий контейнеризации, таких как Docker и Kubernetes, киберпреступники стали активно искать уязвимости в этих средах. Контейнерные уязвимости представляют серьезный риск для безопасности, так как могут привести к выполнению вредоносного кода и несанкционированному доступу к данным. В статье рассматриваются ключевые типы уязвимостей контейнеров, примеры реальных атак, а также способы защиты, такие как обновление образов, настройка контроля доступа и регулярное сканирование уязвимостей.

Ключевые слова: Уязвимости контейнеров, контейнеризация, Docker, Kubernetes, безопасность, контроль доступа, сканирование уязвимостей.

CONTAINER VULNERABILITIES: RISKS, EXAMPLES, AND PROTECTION METHODS

Pivovarova U.A.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevnikov, 22, bldg. 1), e-mail: pivovarova.ulyana2017@yandex.ru

As the popularity of containers and containerization technologies like Docker and Kubernetes grows, cybercriminals are actively seeking vulnerabilities within these environments. Container vulnerabilities pose serious security risks, potentially leading to malicious code execution and unauthorized data access. The article covers key types of container vulnerabilities, examples of real attacks, and protection methods such as updating images, configuring access controls, and regular vulnerability scanning.

Keywords: Container vulnerabilities, containerization, Docker, Kubernetes, security, access control, vulnerability scanning.

Введение

В последние годы технологии контейнеризации, такие как Docker и Kubernetes, завоевали огромную популярность в мире разработки и эксплуатации приложений. Эти технологии позволяют разворачивать и управлять приложениями в независимых контейнерах, что повышает гибкость, масштабируемость и эффективность использования ресурсов. Однако контейнеризация имеет и обратную сторону — она открывает новые векторы атак для киберпреступников, стремящихся использовать уязвимости в контейнерах и связанных инфраструктурах.

Контейнерные уязвимости могут привести к серьезным последствиям, включая утечку данных, выполнение вредоносного кода, повышение привилегий и распространение атак в

пределах корпоративной сети. Поскольку контейнеры часто используются для развертывания критически важных приложений, такие уязвимости могут серьезно подорвать безопасность организации. В этой статье мы рассмотрим основные виды уязвимостей, примеры реальных атак, связанные с ними риски и рекомендуемые методы защиты.

Уязвимости контейнеров

Контейнерные уязвимости могут возникать на разных уровнях архитектуры контейнеризации: от уязвимых образов контейнеров и неправильно настроенных конфигураций до недостатков в безопасности контейнерных оркестраторов, таких как Kubernetes. Одной из самых распространенных уязвимостей контейнеров является использование ненадежных или устаревших образов, в которых содержатся уязвимые библиотеки и зависимости. По мере добавления новых слоёв и приложений в контейнеры, уязвимости могут накапливаться, создавая риски для безопасности всех систем, зависящих от таких контейнеров. Даже если контейнер безопасен при развёртывании, его зависимости могут устареть со временем и стать мишенью для атак[1].

Также одним из распространённых видов уязвимостей является ошибка настройки прав доступа и изоляции контейнеров. Контейнеры должны быть полностью изолированы друг от друга и от основной операционной системы, но в случае неправильно настроенной системы злоумышленник может выйти за пределы контейнера и получить доступ к другим контейнерам или даже к хост-системе. Этот тип уязвимости, известный как "контейнерный побег", даёт атакующему возможность расширить атаку за пределы одного контейнера, что может привести к компрометации всей сети или инфраструктуры[2].

Реальным примером уязвимости контейнеров стала уязвимость в Kubernetes CVE-2018-1002105, которая позволяла злоумышленникам отправлять запросы напрямую на серверные API, обходя стандартные проверки доступа. Это позволило атакующим получить привилегированный доступ к кластерам Kubernetes, в том числе к данным и конфиденциальной информации внутри кластера. Подобные атаки демонстрируют важность регулярного обновления и настройки доступа в Kubernetes и Docker, чтобы избежать использования устаревших версий с известными уязвимостями[3].

Сканирование контейнеров и их образов на наличие уязвимостей стало одной из критически важных практик в процессе разработки. Инструменты, такие как Docker Security Scanning, Clair и Trivy, помогают идентифицировать и устранять уязвимые зависимости, прежде чем контейнеры попадут в продакшен. Регулярное сканирование контейнерных образов на этапе сборки позволяет разработчикам быстро выявлять и исправлять потенциальные уязвимости до развертывания[4].

Помимо регулярного сканирования, важной мерой защиты является применение минимизации привилегий. В идеале каждый контейнер должен выполнять только минимально необходимые функции, а его конфигурация должна исключать возможность выполнения команд с привилегиями на уровне суперпользователя. Для этого рекомендуется использовать Docker-контейнеры с минимальным набором прав доступа и отказаться от выполнения контейнеров от имени "root". Более того, использование "модуля безопасности контейнера" (AppArmor, SELinux) может значительно уменьшить риски, связанные с доступом к хост-системе.

Ещё одна важная мера — сегментация сети для контейнеров. Контейнеры не должны иметь неограниченный доступ к ресурсам сети и другим контейнерам, если это не требуется для их работы. Сегментация и настройка сетевых политик позволяет ограничить взаимодействие контейнеров и тем самым минимизировать возможности атак, при которых злоумышленники могут получить доступ к незащищённым данным или сервисам внутри контейнерной инфраструктуры. Kubernetes Network Policies и Calico помогают ограничить сетевые взаимодействия между контейнерами, создавая дополнительные уровни защиты[5].

Также важно учитывать необходимость регулярного обновления и патчей для контейнерных систем. Обновления образов, Docker и Kubernetes являются ключевыми для предотвращения эксплуатации известных уязвимостей. Поскольку уязвимости, как правило, обнаруживаются и исправляются довольно быстро, оперативное применение обновлений минимизирует риск атак на основе известных эксплойтов.

Заключение

Контейнерные технологии, такие как Docker и Kubernetes, кардинально изменили подход к разработке и развертыванию приложений, предложив гибкие и масштабируемые решения для современных ИТ-систем. Однако вместе с их преимуществами появились и новые угрозы безопасности. Уязвимости контейнеров, такие как использование ненадёжных образов, ошибки в настройке привилегий и конфигураций, а также недостаточная изоляция, создают серьёзные риски для данных и инфраструктуры организаций.

Эффективная защита контейнерных сред требует комплексного подхода: регулярного сканирования образов и контейнеров, минимизации привилегий, настройки сетевой изоляции и своевременного обновления всех компонентов. В условиях, когда контейнеризация становится стандартом в мире ИТ, меры безопасности должны занимать центральное место в процессе разработки и эксплуатации контейнеров.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.
 2. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 5. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Current problems of infotelecommunications in science and education. - 2021. – pp. 409-414.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 007:331.5

РОСТ АВТОМАТИЗАЦИИ И ЕГО ВЛИЯНИЕ НА РЫНОК ТРУДА

¹Гулов Т.У., ²Иванченко С.А., ³Сысоев Н.Д.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ¹gulovvvv@icloud.com, ²siam5599@mail.ru, ³sysoevnikita1748@mail.ru

В данной статье рассматриваются как вызовы, связанные с сокращением рабочих мест и ростом безработицы, так и возможности, открываемые автоматизацией для создания новых профессий и повышения производительности. Автоматизация стремительно растет, меняя ландшафт рынка труда. В статье также рассматриваются стратегии, которые могут помочь работникам приспособиться к изменениям, вызванным автоматизацией, включая: приобретение новых навыков, повышение квалификации и переподготовку.

Ключевые слова: Автоматизация, роботы, глобальные проблемы, экономический рост, социальная напряженность.

THE GROWTH OF AUTOMATION AND ITS IMPACT ON THE LABOR MARKET

¹Gulov T.U., ²Ivanchenko S.A., ³Sysoev N.D.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹gulovvvv@icloud.com, ²siam5599@mail.ru, ³sysoevnikita1748@mail.ru

This article examines both the challenges associated with job cuts and rising unemployment, as well as the opportunities offered by automation to create new professions and increase productivity. Automation is growing rapidly, changing the landscape of the labor market. The article also discusses strategies that can help employees adjust to the changes caused by automation, including: acquiring new skills, advanced training and retraining.

Keywords: Automation, jobs, global problems, economic growth, social tension.

Автоматизация, процесс использования технологий для выполнения задач, которые ранее выполнялись людьми, переживает стремительный рост во многих отраслях. Развитие искусственного интеллекта, робототехники и машинного обучения открывает новые возможности для автоматизации как простых, так и сложных задач.

Этот рост автоматизации оказывает значительное влияние на рынок труда, порождая как вызовы, так и возможности. С одной стороны, автоматизация может привести к сокращению рабочих мест, поскольку машины становятся способными выполнять задачи, которые ранее требовали человеческого труда. Это особенно актуально для рутинных и повторяющихся задач, которые легко поддаются алгоритмизации.

С другой стороны, автоматизация создает новые рабочие места в сферах, связанных с разработкой, внедрением и обслуживанием автоматизированных систем. Специалисты в области информационных технологий, робототехники, анализа данных и управления процессами будут востребованы в условиях растущей автоматизации.

Четвертая промышленная революция, основанная на роботизации и автоматизации, кардинально меняет мир труда. Автоматизация, охватывающая все сферы от производства до обслуживания, повышает производительность, но также трансформирует рынок труда.

Промышленные роботы берут на себя рутинные и физически сложные задачи, освобождая людей для творческой и интеллектуальной деятельности. В связи с этими динамичными изменениями образование должно стать гибким и инновационным. Необходимо внедрять современные технологии, адаптировать учебные программы под потребности цифровой экономики, и предоставлять доступ к онлайн-ресурсам для дистанционного обучения [1].

Ключом к успешному переходу к будущему труда является баланс между автоматизацией и человеческим фактором. Необходимо создавать стратегии, которые не только повышают производительность, но и сохраняют уникальные человеческие качества в тех областях, где они незаменимы.

Однако быстрый рост роботизации таит в себе серьезные вызовы. Многие традиционные рабочие места могут быть автоматизированы, что может привести к росту безработицы и неравенству в распределении экономических возможностей.

Чтобы успешно справиться с этими вызовами, необходимо подготовить рабочую силу к новым требованиям. Ключевую роль играет переосмысление образовательных программ, внедрение технологий в обучение, и развитие универсальных навыков критического мышления, творческого решения проблем и коммуникации.

Сотрудничество между образовательными учреждениями, компаниями и технологическими инноваторами необходимо для создания устойчивой и справедливой системой труда в будущем.

Вопрос о роли роботов в обществе изучают многие исследователи, как отечественные (Л.Ю. Андреева, В.Е. Гимпельсон, М.И. Гусенко, С.П. Роцин), так и зарубежные (Дж. Бессен, Р. Гордон, К. Сандрин, Г. Хольцер). Данный вопрос также исследуется международными организациями, такими как Международная федерация роботов, Европейская комиссия, ОЭСР, Глобальный институт McKinsey и Бостонская консалтинговая группа [2].

Рост интереса к робототехнике и автоматизации обусловлен как привлекательностью их потенциала для упрощения жизни, так и опасениями по поводу влияния на рабочие места.

Эти опасения связаны с более широкими геополитическими и социальными проблемами, такими как торговая политика и иммиграция, что усиливает чувство неуверенности в будущем занятости.

Несмотря на потенциальные негативные последствия автоматизации, нельзя игнорировать ее реальный вклад в повышение производительности, конкурентоспособности и создание рабочих мест.

Эксперты Международной Федерации роботов утверждают, что роботы играют ключевую роль в экономическом росте и благополучии.

1. Повышение конкурентоспособности. Роботы повышают продуктивность и делают компании более конкурентоспособными, особенно для малых и средних предприятий, являющихся основой экономики. Крупные компании также могут повысить свою конкурентоспособность за счет более быстрой разработки и производства. Настоящая угроза занятости не в автоматизации, а в неспособности оставаться конкурентоспособными.

2. Рост спроса. Повышение производительности может привести к росту спроса и созданию новых рабочих мест. Эффект наблюдается как внутри компаний, так и в цепочке поставок промышленного сектора, а также в сфере услуг.

3. Положительное влияние на занятость. Автоматизация, как правило, приводит к росту спроса на рабочую силу и повышению заработной платы. Роботы требуют работников с более высокой квалификацией, что стимулирует повышение заработной платы. Ключевой вопрос – как помочь работникам с низкой и средней квалификацией получить новые навыки.

4. Дополнение, а не замена. Роботы дополняют и усиливают труд человека, работая совместно. Роботы заменяют отдельные задачи, но не рабочие места. Большая часть роботов используется для усиления и повышения эффективности работы людей, а не для полной автоматизации.

5. Необоснованность налога на роботов. Введение налога на роботов необоснованно, учитывая их положительное влияние на занятость и заработную плату. Налог может ограничить инвестиции в робототехнику, снизить конкурентоспособность и привести к сокращению рабочих мест.

6. Необходимость подготовки кадров. Правительствам и компаниям необходимо сосредоточиться на предоставлении новых навыков работникам, чтобы они могли воспользоваться преимуществами робототехники. Важно инвестировать в исследования робототехники и программы переподготовки, чтобы обеспечить положительное влияние роботов на занятость, качество работы и заработную плату.

Развитие искусственного интеллекта (ИИ) и автоматизации открывает новые возможности для бизнеса, экономики и общества в целом.

Автоматизация, роботизация и искусственный интеллект преобразуют рынок труда, изменяя количество и качество доступных рабочих мест. Технологии способны облегчить жизнь, повысить производительность и качество жизни, а также продлить ее продолжительность. Благодаря этому, у нас появится больше времени и возможностей для самореализации.

Хотя автоматизация и ИИ не являются новыми понятиями, современный технологический прогресс существенно расширяет их возможности. Исследования Института McKinsey показывают, что для достижения устойчивого роста бизнеса, экономики и решения социальных проблем, необходимо развивать следующие направления.

1. Быстрый технологический прогресс.

Помимо традиционной промышленной автоматизации и роботов, появляются новые поколения автономных систем: от беспилотных автомобилей до автоматических касс в магазинах. Этот прогресс обусловлен улучшением механизмов, датчиков и программного обеспечения. Искусственный интеллект (ИИ) демонстрирует значительные успехи благодаря развитию алгоритмов машинного обучения, увеличению вычислительной мощности и быстрому росту объемов данных. В некоторых областях ИИ уже превосходит человеческие возможности, например, в анализе видеoinформации, обработке естественного языка и сложных играх, таких как Го.

2. Потенциал для преобразования бизнеса и экономического роста.

Искусственный интеллект уже используется в различных продуктах и услугах, позволяя компаниям из разных секторов персонализировать рекомендации, выявлять аномалии в

производстве, предотвращать мошеннические операции и т. д. Новое поколение алгоритмов ИИ, решающих задачи классификации, оценки и кластеризации, обещает еще более значительный прогресс. По оценкам Института McKinsey, самые передовые методы глубокого обучения на основе искусственных нейронных сетей могут генерировать от 3,5 до 5,8 триллионов долларов США ежегодной стоимости, что составляет 40 процентов от стоимости, созданной всеми методами аналитики.

Широкое внедрение ИИ и автоматизации может стимулировать рост глобальной экономики и повысить уровень жизни. Однако демографические изменения, такие как старение населения и снижение рождаемости, могут стать тормозом экономического роста.

Согласно прогнозам Всемирного экономического форума, население Земли увеличится с 7,2 миллиардов человек сегодня до 8 миллиардов в 2030 году и 9 миллиардов в 2050 году. Это приведет к увеличению совокупного спроса. Однако демографическая тенденция к старению населения наблюдается не только в богатых западных странах. Рождаемость падает ниже уровня воспроизводства во многих регионах мира, включая Европу, Южную Америку, страны Карибского бассейна, многие страны Азии, включая Китай и южную Индию, и даже некоторые страны Ближнего Востока и Северной Африки [3].

Рост производительности труда, являющийся ключевым фактором экономического роста, замедлился во многих странах. В период с 2010 по 2014 год этот показатель снизился на 0,5 процента по сравнению с предыдущим десятилетием, в течение которого рост составлял 2,4 процента в США и крупных европейских странах.

ИИ и автоматизация способны изменить эту тенденцию: рост производительности может достичь 2 процентов в год в течение следующего десятилетия, причем 60 процентов этого увеличения будет обусловлено цифровыми технологиями.

3. Потенциал для решения глобальных проблем.

Искусственный интеллект используется в различных областях, от материаловедения до медицинских исследований, и имеет потенциал для решения таких проблем, как:

- борьба с изменением климата;
- улучшение системы здравоохранения;
- создание более справедливого и доступного образования.

Внедрение ИИ и автоматизации сопряжено с определенными рисками, например, с потерей рабочих мест. Однако эти изменения также открывают новые возможности для создания новых рабочих мест, повышения уровня жизни и решения глобальных проблем.

Изменения, которые мы должны предвидеть.

Искусственный интеллект и автоматизация обещают революционизировать бизнес и общество, но вместе с этим несут и серьезные вызовы для рынка труда. Внедрение этих технологий может вызвать нестабильность в обществе, политическую и экономическую напряженность, если блага от их развития не распределены равномерно.

Масштабы автоматизации.

Исследования показывают, что около половины задач, выполняемых людьми, уже сегодня могут быть автоматизированы. Это означает, что многие профессии, от сварщиков до ипотечных брокеров, столкнутся с изменениями, так как часть их работы будет выполняться машинами.

Автоматизация задач.

В первую очередь автоматизация затронет рутинные физические задачи, а также сбор и обработку данных. Это освободит людей от этих задач, но также может привести к сокращению рабочих мест в некоторых отраслях.

К 2030 году некоторые профессии могут столкнуться с существенным сокращением рабочих мест из-за автоматизации. По оценкам экспертов, около 15% мировой рабочей силы, или 400 миллионов рабочих, могут быть заменены машинами.

Факторы, влияющие на темпы автоматизации.

Темпы и масштабы внедрения ИИ и автоматизации будут зависеть от различных факторов, таких как:

- техническая возможность: насколько легко автоматизировать конкретную задачу;
- стоимость: сколько стоит внедрение автоматизации;
- динамика рынка труда: количество рабочей силы, уровень заработной платы, социальные нормы.

Разные сценарии автоматизации.

В развитых странах, таких как Франция, Япония и США, автоматизация может вытеснить от 20 до 25% рабочей силы к 2030 году. В Индии этот показатель может быть значительно ниже.

Создание новых рабочих мест.

Несмотря на сокращение рабочих мест в некоторых секторах, внедрение ИИ и автоматизации также будет создавать новые рабочие места. Это будет связано с ростом спроса на специалистов в области ИИ, автоматизации, анализа данных и других сферах.

Важность адаптации.

Чтобы справиться с этими вызовами, нам необходимо подготовиться к изменениям на рынке труда. Правительства и бизнес должны инвестировать в образование и переподготовку, чтобы люди могли адаптироваться к новым реалиям.

Внедрение ИИ и автоматизации — это сложный процесс с различными последствиями. Чтобы извлечь максимальную пользу от этих технологий и минимизировать негативные последствия, нам необходимо действовать предвидеть изменения и принять необходимые меры для адаптации [4].

Экономический рост и технологическое развитие продолжают создавать новые рабочие места. Помимо традиционных профессий, появляются новые, которые пока даже трудно представить. Согласно прогнозам, к 2030 году они могут составить до 10% от общего количества рабочих мест.

История демонстрирует, что технологические изменения всегда стимулировали рост занятости. Так, появление персональных компьютеров в 70-х и 80-х годах привело к появлению миллионов рабочих мест для разработчиков, специалистов по обслуживанию и аналитиков.

Технологии также способствуют развитию удаленной работы и самозанятости. Платформенные решения, такие как Uber и Airbnb, становятся всё более популярными, увеличивая число самозанятых на 17% к 2025 году только в Европе.

Изменения в сфере труда.

Автоматизация всё чаще внедряется в рабочие процессы, дополняя человеческий труд. Например, алгоритмы искусственного интеллекта помогают врачам в диагностике и выборе лечения, а роботы в розничной торговле освобождают персонал от рутинных задач.

Основные трансформации и вызовы.

Несмотря на ожидаемый рост числа рабочих мест, автоматизация и искусственный интеллект вызовут значительные изменения на рынке труда. Профессии будут трансформироваться, меняются требования к квалификации и образованию.

Новым требованиям к рабочим местам.

Автоматизация ускорит спрос на передовые технические навыки, такие как программирование. В то же время возрастает спрос на социальные, эмоциональные и когнитивные навыки, например, креативность, критическое мышление и комплексная обработка информации.

Экономический рост и технологическое развитие создают новые возможности и вызовы для рынка труда. Чтобы успешно адаптироваться к изменениям, необходимо развивать новые навыки и быть готовыми к трансформации профессий.

Изменения в сфере труда: неизбежный переход к новым профессиям.

Согласно исследованиям Глобального Института McKinsey, к 2030 году 3% мировой рабочей силы, а возможно, и больше, столкнутся с необходимостью переквалификации. Эти изменения коснутся не только отдельных компаний и отраслей, но и целых регионов.

Профессии, связанные с физическим трудом в рутинных условиях, а также обработкой и сбором данных, вероятно, будут сокращаться. Напротив, спрос возрастет на специалистов, чья деятельность трудно автоматизируется, таких как менеджеры, а также тех, кто работает в непредсказуемых условиях, например, сантехники. Учителя, младшие медсестры, техники и другие специалисты также будут востребованы.

Совместная работа человека и машин: новые реалии.

Интеграция искусственного интеллекта и программного обеспечения в рабочие процессы приведет к появлению новых форм взаимодействия между людьми и машинами. Например, кассиры в магазинах могут стать помощниками при оформлении заказов, отвечая на вопросы и устраняя технические неполадки.

Возможные последствия для заработной платы.

Автоматизация, скорее всего, окажет негативное влияние на среднюю заработную плату в развитых странах. Среднеквалифицированные профессии, например, в производстве или бухгалтерском учете, будут вытесняться более эффективными автоматизированными процессами. В то же время спрос на высококвалифицированных специалистов будет значительно расти.

Неравенство и социальная напряженность.

Хотя автоматизация может создать новые рабочие места, в том числе в сфере образования и здравоохранения, она также может усилить неравенство в доходах и усугубить поляризацию заработной платы. В результате может возникнуть социальная и политическая напряженность.

Подготовка к будущим вызовам.

Мир уже столкнулся с нехваткой квалифицированных кадров, соответствующих потребностям рынка. Чтобы подготовиться к будущим изменениям, необходимо

инвестировать в образование и профессиональную подготовку. Необходимо также учитывать влияние автоматизации на работников и разработать механизмы смягчения негативных последствий.

Автоматизация неизбежно изменит рынок труда, открывая новые возможности, но также создавая новые вызовы. Важным является подготовка к этим изменениям, чтобы обеспечить устойчивое развитие и социальное благополучие в будущем [6].

В условиях стремительного развития технологий, особенно искусственного интеллекта и автоматизации, нам важно не тормозить прогресс, а использовать его потенциал для повышения производительности и улучшения жизни людей. Технологии создают новые возможности, которые, в свою очередь, требуют адаптации рынка труда.

Ключевые шаги для смягчения социальных последствий автоматизации.

1. Экономический рост и производительность. Для создания новых рабочих мест и повышения благосостояния необходим устойчивый экономический рост, который достигается за счет повышения производительности. Важно инвестировать в экономику и использовать автоматизацию для ее повышения.

2. Поддержка динамизма бизнеса. Создание благоприятной среды для развития малого бизнеса и конкуренции между крупными компаниями стимулирует рост занятости. Необходимо упростить правила, налоговую систему и другие стимулы для поддержки малого бизнеса.

3. Развитие системы образования и обучения. Современные требования рынка труда требуют компетенций в области STEM (наука, технологии, инженерия, математика) и развития творческого, критического и системного мышления. Необходимы программы обучения, как в школьной системе, так и для повышения квалификации работающих.

4. Инвестирование в человеческий капитал. Государство и частный сектор должны инвестировать в повышение квалификации, обучение и создание новых рабочих мест. Стимулирование компаний к инвестированию в человеческий капитал, а также в научно-исследовательскую деятельность, является важным фактором для устойчивого развития рынка труда.

Данные меры помогут смягчить последствия автоматизации, создать новые рабочие места и подготовить население к вызовам будущего.

5. Улучшение динамизма рынка труда.

Улучшение информационного обмена. Цифровые платформы должны быть оптимизированы для быстрого и эффективного сопоставления вакансий и соискателей.

Адаптация к новой экономике. Необходимо решать вопросы, связанные с "гиг-экономикой" - гибкими формами занятости, включая классификацию работников и стабильность заработка.

6. Перестройка рабочей среды.

Совместная работа человека и машины. Необходимо создавать безопасные и эффективные рабочие пространства, где люди взаимодействуют с машинами.

Изменение организационных структур. Компании должны стать более гибкими и неиерархическими, чтобы максимально эффективно использовать возможности совместной работы.

7. Переосмысление систем дохода.

Смягчение последствий автоматизации. Необходимо рассмотреть меры, такие как условные переводы, поддержка мобильности, гарантированный базовый доход и модернизированные системы социальной защиты, чтобы справиться с потенциальным сокращением занятости.

Поиск смысла и цели. Важно обеспечить людям не только финансовую стабильность, но и ощущение ценности и значимости их труда.

8. Создание системы поддержки перехода и безопасности.

Помощь работникам в адаптации к изменениям. Необходимо обеспечить доступную помощь в обучении и переквалификации, учитывая постоянные изменения в требованиях к навыкам.

Развитие системы поддержки. Необходимо разработать и внедрить эффективные программы социальной защиты и поддержки для работников в период перехода.

9. Инвестирование в драйверы спроса на работу.

Развитие инфраструктуры. Правительствам следует инвестировать в инфраструктурные проекты, создающие новые рабочие места, например, в сфере строительства, энергетики и экологии.

Создание рабочих мест со средней заработной платой. Эти рабочие места менее подвержены автоматизации и могут служить важным фактором экономического роста.

10. Безопасное внедрение искусственного интеллекта и автоматизации.

Защита от рисков. Необходимо активно предотвращать негативные последствия технологических изменений, такие как потеря рабочих мест и дискриминация.

Обеспечение этичности использования данных. Следует уделить особое внимание вопросам защиты данных, конфиденциальности и предотвращения предвзятости в использовании искусственного интеллекта.

11. Непрерывное образование и переподготовка.

Развитие навыков. Для успешной адаптации к будущему труда необходимо развивать навыки, необходимые для работы с новыми технологиями.

Обучение на протяжении всей жизни. Важно обеспечить доступ к качественному обучению и переподготовке как для работников среднего возраста, так и для молодых специалистов.

В целом, успешная адаптация к изменениям в мире труда требует комплексного подхода, включающего развитие новых технологий, модернизацию рынка труда, повышение уровня образования и переподготовки, а также создание эффективных систем социальной защиты.

Автоматизация – это неумолимое течение времени, которое стремительно меняет наш мир. Роботы, алгоритмы и искусственный интеллект проникают во все сферы жизни, от производства и логистики до здравоохранения и образования. Этот стремительный прогресс несет с собой как огромные возможности, так и серьезные вызовы для рынка [5].

В заключение, рост автоматизации представляет собой как вызов, так и возможность для рынка. С одной стороны, она может привести к сокращению рабочих мест и социальной нестабильности. С другой стороны, она открывает двери для новых возможностей, повышает производительность и создает новые рабочие места в высокотехнологичных секторах.

Список литературы

1. Быковская, Е. В. Развитие технологического предпринимательства как составляющей инновационно-технологической трансформации экономики: проблемы, перспективы роста, роль технического вуза региона: монография / Е. В. Быковская. – Тамбов: Издательский центр ФГБОУ ВО «ТГТУ», 2021. — 84 с.
2. Сергиевич, Т. В. Экономика роботизации машиностроительного комплекса Республики Беларусь / Т. В. Сергиевич. – Минск: БНТУ, 2023. – 89 с.
3. Сивоплясова С.Ю. Цифровизация социально-экономических процессов. Цифровые технологии в повседневных практиках населения: Учебное пособие. — М.: Изд-во МАИ, 2022. — С.47-48.
4. Современные проблемы обеспечения устойчивого развития социально-экономических систем: монография / Л. Л. Бунтовская, О. Ю. Сердюк, Н. А. Балтачеева [и др.]; под общей редакцией д-ра экон. наук, доц. Л. Л. Бунтовской; Донецкий национальный университет, экономический факультет, кафедра управления персоналом и экономики труда. – Донецк: ДонНУ, 2023. – 73 с.
5. Султанова Д. Ш. Управление инновациями в области повышения производительности труда: монография / Д. Ш. Султанова, А. А. Хаертдинова, Р. Ф. Бурганов; М-во образ. и науки России, Казан. нац. исслед. технол. ун-т. – Казань: Изд-во КНИТУ, 2015. – 75 с.
6. Юсупова М.Д. Экономическая теория: учебное пособие / М.Д. Юсупова [Текст]. – Грозный: Издательство ФГБОУ ВО "Чеченский государственный университет", 2020. – 89 с.

References

1. Bykovskaya, E. V. Development of technological entrepreneurship as a component of innovative and technological transformation of the economy: problems, growth prospects, the role of a technical university in the region: monograph / E. V. Bykovskaya. – Tambov: Publishing center of FGBOU VO "TSTU", 2021. — p.84
 2. Sergievich, T. V. Economics of robotization of the machine–building complex of the Republic of Belarus / T. V. Sergievich. – Minsk: BNTU, 2023. - p.89
 3. Sivoplyasova S.Yu. Digitalization of socio-economic processes. Digital technologies in everyday practices of the population: A textbook. — M.: Publishing House of MAI, 2022. - pp.47-48
 4. Modern problems of ensuring sustainable development of socio-economic systems: monograph / L. L. Buntovskaya, O. Y. Serdyuk, N. A. Baltacheeva [et al.]; under the general editorship of Dr. of Economics, Associate Professor L. L. Buntovskaya; Donetsk National University, Faculty of Economics, Department of Personnel Management and Labor Economics. – Donetsk: DonNU, 2023. – p.73
 5. Sultanova D. Sh., Khaertdinova A. A., Burganov R. F. Innovation Management in the Field of Increasing Labor Productivity: Monograph; M-vo obraz. and Science of Russia, Kazan. national. research. Technol. University. – Kazan: KNRTU Publ., 2015. – p.75
 6. Yusupova M.D. Economic Theory: Textbook / M.D. Yusupova [Text]. – Grozny: Chechen State University Publishing House, 2020. – p.89
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.736

HIDDENEYE: ИНСТРУМЕНТ ДЛЯ ФИШИНГА

Бютнер С.И.

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

HiddenEye — это популярный инструмент для создания фишинговых страниц, который активно используется злоумышленниками для кражи учётных данных и другой конфиденциальной информации. Статья раскрывает технические возможности HiddenEye, типы атак, которые могут быть осуществлены с его помощью, а также методы защиты от фишинговых угроз, включая фильтрацию почты, использование многофакторной аутентификации и обучение пользователей распознаванию фишинга.

Ключевые слова: HiddenEye, фишинг, кибербезопасность, фишинговые атаки, кража данных, защита.

HIDDENEYE: A PHISHING TOOL

Buetner S.I.

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: serafimkavasaki@gmail.com

As the popularity of containers and containerization technologies like Docker and Kubernetes grows, cybercriminals are actively seeking vulnerabilities within these environments. Container vulnerabilities pose serious security risks, potentially leading to malicious code execution and unauthorized data access. The article covers key types of container vulnerabilities, examples of real attacks, and protection methods such as updating images, configuring access controls, and regular vulnerability scanning.

Keywords: HiddenEye, phishing, cybersecurity, phishing attacks, data theft, protection.

Введение

С ростом цифровизации и внедрением онлайн-сервисов, фишинг остаётся одной из самых распространённых и эффективных кибератак. Злоумышленники всё активнее используют специализированные инструменты для создания фальшивых сайтов и приложений, которые маскируются под популярные веб-сайты, с целью кражи учётных данных и личной информации. Одним из таких инструментов является HiddenEye — универсальный фишинговый инструмент с широким набором функций, позволяющий злоумышленникам создавать убедительные копии веб-сайтов, собирать данные и отправлять вредоносные ссылки.

HiddenEye изначально был создан для исследовательских целей, однако быстро завоевал популярность среди киберпреступников благодаря своей доступности и простоте использования. Этот инструмент поддерживает создание фальшивых страниц для таких популярных платформ, как Facebook, Instagram, Google, PayPal и многих других. Он предоставляет возможности не только для фишинга, но и для таких операций, как захват IP-

адресов и мониторинг активности жертвы в реальном времени. В данной статье рассмотрим, как HiddenEye работает, какие риски он создаёт для пользователей, а также меры безопасности, которые помогают защититься от фишинга.

HiddenEye

HiddenEye позволяет злоумышленникам легко создавать фальшивые страницы, которые внешне неотличимы от настоящих веб-сайтов, и отправлять их пользователям в виде ссылок через электронную почту, социальные сети или мессенджеры. В зависимости от предпочтений злоумышленника, HiddenEye может использоваться для создания страниц логина таких сервисов, как Instagram, Google, Twitter и многих других. Когда пользователь вводит свои данные на поддельной странице, HiddenEye записывает введённые данные и отправляет их злоумышленнику, предоставляя ему доступ к учётной записи жертвы[1].

Благодаря широкому набору функций, HiddenEye позволяет настраивать страницу фишинга под любой выбранный сайт, предоставляя шаблоны, которые максимально похожи на оригинальные веб-страницы. Это усложняет распознавание поддельных страниц для пользователей, которые могут случайно передать свои конфиденциальные данные в руки злоумышленников. Помимо этого, HiddenEye предоставляет инструменты для скрытия своего присутствия, например, изменяя адреса отправки ссылок и маскируя поддельные страницы за доменными именами, которые выглядят надёжно[2].

Вдобавок, HiddenEye поддерживает множество технических функций, которые помогают усилить атаки. Например, инструмент может отслеживать местоположение жертвы с помощью IP-логирования, что особенно полезно для целевых атак. Также HiddenEye позволяет отправлять массовые сообщения и уведомления для вовлечения множества пользователей, что увеличивает вероятность успешного получения данных. Из-за этого инструмент получил популярность среди киберпреступников и стал одной из угроз в киберпространстве[3].

Использование HiddenEye представляет собой серьёзную угрозу для компаний и индивидуальных пользователей, так как успешные фишинговые атаки могут привести к краже финансовых данных, корпоративной информации и персональных данных, которые могут быть проданы или использованы для дальнейших атак. Базовая защита, такая как уникальные пароли и базовое антивирусное ПО, не всегда способна предотвратить подобные атаки, особенно если пользователь не подозревает, что взаимодействует с поддельной страницей[4].

Защита от HiddenEye и аналогичных инструментов фишинга требует комплексного подхода. Одним из наиболее эффективных методов является многофакторная аутентификация (MFA), которая добавляет дополнительный уровень защиты, затрудняя доступ к учётной записи даже при компрометации пароля. Фильтрация электронной почты также играет ключевую роль, так как многие атаки начинают с фишингового письма. Использование надёжных антивирусных решений с функцией фильтрации ссылок и веб-контента может помочь заблокировать доступ к вредоносным страницам до их открытия[5].

Обучение пользователей также играет критически важную роль. Поскольку фишинговые атаки всё чаще используют социальную инженерию, необходимо повышать осведомлённость о признаках поддельных ссылок, таких как орфографические ошибки, подозрительные домены и неожиданные запросы на ввод учётных данных. Компании могут внедрять регулярные тренировки по безопасности для сотрудников, что способствует снижению вероятности успешного фишинга.

Заключение

HiddenEye демонстрирует, насколько опасными могут быть современные фишинговые инструменты, доступные даже для неопытных пользователей. С помощью таких программ злоумышленники могут получить доступ к конфиденциальной информации, компрометировать финансовые и корпоративные данные и нанести значительный ущерб. Инструменты вроде HiddenEye продолжают развиваться, становясь всё более эффективными и сложными для обнаружения.

Для защиты от таких угроз пользователям важно соблюдать лучшие практики кибербезопасности, включая использование многофакторной аутентификации, регулярное обновление антивирусного ПО, фильтрацию электронной почты и обучение сотрудников. Комплексный подход к безопасности помогает минимизировать риски, связанные с фишинговыми атаками, и противостоять инструментам, подобным HiddenEye, которые угрожают информационной безопасности каждого пользователя в цифровом пространстве.

Список литературы

1. Цветков А. Ю., Рузманов Е. Ю. РАССМОТРЕНИЕ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ //ББК 3 П27. – 2021. – С. 55.
2. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
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. 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.
5. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

References

1. Tsvetkov A. Yu., Rozanov E. Yu. CONSIDERATION OF PENETRATION TESTING IN INFORMATION SECURITY TASKS //PC 3 P27. – 2021. – p. 55.
2. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.
3. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
4. Kushnir D. V. Research and development of methods for distributing confidential data via quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.

5. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using large data //High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.89

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЗДРАВООХРАНЕНИИ

¹Гулов Т.У., ²Иванченко С.А., ³Сысоев Н.Д.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ¹gulovvvv@icloud.com, ²siam5599@mail.ru, ³sysoevnikita1748@mail.ru

В данной статье анализируется применение Искусственного Интеллекта (ИИ) в здравоохранении, рассматривая его потенциал для революционного преобразования медицинской практики. Искусственный интеллект (ИИ) трансформирует здравоохранение, предлагая беспрецедентные возможности для улучшения оказания медицинской помощи. В статье исследуется растущая роль ИИ в различных аспектах медицинской практики, включая диагностику, лечение и прогнозирование результатов. Рассматривается, как алгоритмы машинного обучения используются для анализа сложных медицинских данных, выявления закономерностей и прогнозирования рисков для здоровья.

Ключевые слова: Искусственный интеллект, медицина, ВОЗ, психология, неврология.

ARTIFICIAL INTELLIGENCE IN HEALTHCARE

¹Gulov T.U., ²Ivanchenko S.A., ³Sysoev N.D.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹gulovvvv@icloud.com, ²siam5599@mail.ru, ³sysoevnikita1748@mail.ru

This article analyzes the application of Artificial Intelligence (AI) in healthcare, considering its potential for a revolutionary transformation of medical practice. Artificial intelligence (AI) is transforming healthcare by offering unprecedented opportunities to improve healthcare delivery. The article explores the growing role of AI in various aspects of medical practice, including diagnosis, treatment, and predicting outcomes. It examines how machine learning algorithms are used to analyze complex medical data, identify patterns, and predict health risks.

Keywords: Artificial intelligence, medicine, WHO, psychology, neurology.

Искусственный интеллект (ИИ) стремительно меняет облик здравоохранения, предлагая новые решения для диагностики, лечения и профилактики болезней. ИИ-системы способны анализировать огромные объемы данных, выявляя закономерности и прогнозируя риски, недоступные для человеческого разума.

Несмотря на обширные знания врачей, они используют лишь малую часть доступной медицинской информации. В то время как искусственный интеллект (ИИ) может анализировать все 100% медицинских данных в Сети, обрабатывая тысячи страниц текста в секунду. Это позволяет ИИ находить информацию, которую человек просто не может охватить.

Подумайте только: каждые 20 минут появляется новая медицинская статья, и в 2019 году их было опубликовано целых 870 000! Врачи, увы, не в силах справиться с таким потоком информации. Это приводит к ошибкам: 10% случаев лечения неэффективны, а 20-25% смертей происходит из-за неверных диагнозов.

Искусственный интеллект способен снизить риск ошибок при диагностике и лечении на 70%. Он становится реальным помощником врача, существенно повышая эффективность медицинской помощи. Внедрение ИИ в медицинскую практику становится все более широким, отражая очевидное превосходство электронного врача над человеком [2].

Сегодня медицина и здравоохранение активно внедряют искусственный интеллект (ИИ), который уже сейчас считается одним из самых перспективных направлений. ИИ способен значительно улучшить точность диагностики, облегчить жизнь пациентов, ускорить разработку лекарств и многое другое.

Как работает ИИ в медицине?

1. Диагностика: Google Deepmind Health и IBM Watson Health предлагают "умные" решения для оценки состояния пациента и предварительной диагностики, увеличивая точность диагностики на 40% и снижая стоимость медицинской помощи вдвое.

2. Мобильные приложения: ВОЗ внедрила мобильное приложение mHealth, позволяющее получить предварительный диагноз по ответам на вопросы. Приложение Sense.ly отслеживает ход реабилитации пациентов после выписки из больницы.

3. Генетика: Sophia Genetics использует ИИ для точной диагностики заболеваний по анализу ДНК. Human Longevity и Deep Genomics собирают информацию для создания генетических баз данных.

4. Дерматология: приложение DermaCompare с использованием облачной технологии ИИ анализирует фотографии с телефона, позволяя каждому человеку идентифицировать родинки меланомы на коже.

5. Подбор лекарств: MedClueRx помогает выбрать наиболее эффективные лекарства для каждого пациента, а MedWhat заменяет личного врача, отвечая на медицинские вопросы и отслеживая состояние пациента.

6. Голосовые консультанты: Microsoft Health bot, основанный на технологии распознавания речи Cortana, позволяет общаться с медицинским консультантом голосом.

Преимущества ИИ в медицине:

- повышение точности диагностики;
- ускорение разработки лекарств;
- облегчение жизни пациентов;
- снижение стоимости медицинской помощи;
- увеличение доступности медицинских услуг.

Искусственный интеллект уже сегодня меняет лицо медицины, открывая новые возможности для лечения и профилактики заболеваний. В будущем ИИ продолжит развиваться, предлагая новые решения и улучшая жизнь каждого человека.

Искусственный интеллект (ИИ) в медицине предлагает множество преимуществ, способствуя улучшению качества медицинской помощи и оптимизации процессов.

1. Повышение качества и эффективности лечения.

Снижение смертности: ИИ ускоряет диагностику и лечение, сокращая время ожидания помощи от специалистов, тем самым повышая шансы на выживание.

Повышение точности диагностики: ИИ помогает врачам анализировать большие объемы данных, что позволяет им устанавливать более точные диагнозы.

Доступ к актуальной информации: ИИ предоставляет врачам доступ к новейшим исследованиям и тенденциям в медицине, что позволяет им принимать более обоснованные решения.

Освобождение времени для специалистов: ИИ автоматизирует рутинные задачи, освобождая время врачей для более сложных и индивидуальных взаимодействий с пациентами.

2. Улучшение качества жизни пациентов.

Снижение зависимости от социальных услуг: роботы, управляемые ИИ, могут оказывать помощь пациентам с хроническими заболеваниями, такими как болезнь Альцгеймера, что позволяет им дольше оставаться дома и поддерживать независимость.

Увеличение продолжительности жизни: ИИ позволяет предотвращать заболевания, проводить более точную диагностику и получать более эффективное лечение, что увеличивает продолжительность жизни людей.

3. Повышение безопасности и точности.

Сокращение ошибок: ИИ позволяет минимизировать ошибки, связанные с человеческим фактором, например, утомлением или невнимательностью.

Повышение точности хирургических операций: роботы, управляемые ИИ, обеспечивают хирургам более точные и менее инвазивные операции, что сокращает период восстановления пациентов.

4. Оптимизация медицинских расходов.

Сокращение госпитализаций: ИИ позволяет проводить дистанционную диагностику и лечение, сокращая необходимость госпитализации и связанные с ней затраты.

Повышение эффективности ведения документации: ИИ оптимизирует процесс ведения медицинской документации, снижая количество ошибок и затраты на административные расходы.

5. Перспективы роста рынка.

Увеличение инвестиций в ИИ: рынок приложений для машинного обучения активно растет, а к 2028 году ожидается значительное увеличение использования ИИ в медицине.

В целом, искусственный интеллект в медицине представляет собой мощный инструмент, способный существенно улучшить качество медицинской помощи, повысить эффективность лечения и оптимизировать медицинские расходы.

Платформа искусственного интеллекта для здоровья: новая эра профилактики и персонализации.

Глобальное снижение уровня здоровья в последние два десятилетия стало тревожным сигналом. Нездоровый образ жизни, неблагоприятные условия жизни и стресс являются ключевыми факторами, влияющими на состояние здоровья 80% населения планеты [1].

Важно раннее выявление рисков и коррекция состояния здоровья, особенно в детском возрасте, чтобы не допустить перехода предболезни в болезнь.

Персонализированный подход к оценке состояния человека, определению факторов риска и разработке индивидуальной программы профилактических мероприятий становится все более актуальным.

Российская академия наук представила инновационную платформу искусственного интеллекта для диагностики уровня здоровья. Эта технология, разработанная Институтом автоматики и процессов управления, основана на принципах искусственного интеллекта и позволяет определить физическое и психическое здоровье человека с учетом его конституционного типа и особенностей развития.

Данная технология обещает повышение эффективности медицинской помощи и сохранение здоровья граждан.

В фокусе внимания разработчиков — комплексный подход, охватывающий все аспекты здоровья: физическое, психическое и социальное. Платформа позволит выявлять зоны риска и предлагать индивидуальные программы профилактики, включающие традиционную медицину, медикаментозную коррекцию и психологическую помощь.

Данная разработка представляет собой значительный шаг в развитии здравоохранения, обеспечивая индивидуальный подход к каждому пациенту и фокусируясь на ранней профилактике и сохранении здоровья.

Исследовательская группа получила задание разработать комплексный подход, основанный на искусственном интеллекте, для улучшения диагностики и лечения заболеваний. В задачи входило:

- 1) создание интегрированной системы моделей, методов и алгоритмов, способных извлекать из данных о здоровье пациентов новые знания, учитывая индивидуальные особенности, и генерировать персональные рекомендации по коррекции состояния;
- 2) разработка технологии адаптивной оценки уровня здоровья, позволяющей определить степень влияния факторов риска и наличие признаков социально значимых заболеваний;
- 3) создание системы автоматического дополнения и обогащения существующих моделей данными, с помощью методов машинного обучения.
- 4) разработка интеллектуальной системы поддержки принятия решений, основанной на интеграции онтологий, баз знаний и машинного обучения, для дифференциальной диагностики состояний, связанных с изменениями здоровья;
- 5) разработка технологии интеллектуального назначения лечения, включающей как оперативное вмешательство с прогнозом возможных осложнений и продолжительности жизни, так и медикаментозную терапию, в том числе превентивную, с учетом персональных факторов риска. В эту технологию также входит комплексное восстановительное лечение, сочетающее традиционную китайскую медицину с современными западными методиками, особенно в области сердечно-сосудистых заболеваний;
- 6) разработка интеллектуальных сервисов и систем мониторинга и оценки функционального состояния пациента, на всех этапах восстановительного лечения.

Статусы о восстановительном лечении.

Статус 1 (Начало лечения).

"Мы рады объявить о начале восстановительного лечения, основанного на передовых методах искусственного интеллекта. Наш подход объединяет знания об онтологии и искусственный интеллект, чтобы создать индивидуальную программу восстановления."

"Мы используем передовые технологии, чтобы создать персонализированную программу лечения. Наша цель - оптимизировать процесс восстановления с помощью искусственного интеллекта."

Статус 2 (Сбор информации).

"Мы собираем ценную информацию о вашем здоровье, используя клинические данные, результаты исследований и информацию с ваших мобильных устройств. Это позволит нам разработать идеальный план лечения."

"Мы работаем над созданием вашего индивидуального плана лечения, используя ваши личные данные и новейшие научные достижения. Ваше восстановление - наш приоритет!"

Статус 3 (Разработка плана лечения).

"Мы разработали план лечения, основанный на ваших индивидуальных потребностях и данных о вашем здоровье. Наш подход учитывает совместимость различных методов лечения и современные исследования."

"Благодаря анализу ваших данных мы можем создать наиболее эффективный план лечения, который поможет вам максимально быстро и комфортно восстановиться."

Статус 4 (Мониторинг и корректировка).

"Мы постоянно следим за вашим прогрессом и корректируем план лечения в режиме реального времени. Наше стремление - обеспечить вам наилучшие результаты."

"Мы используем искусственный интеллект для оптимизации вашего лечения. Наш подход позволяет своевременно корректировать план лечения в зависимости от вашего состояния."

Статус 5 (Дополнительные технологии).

"Мы применяем передовые технологии виртуальной реальности с обратной связью для ускорения процесса восстановления. Это помогает нам обеспечить индивидуальный подход к лечению."

"Мы разрабатываем инновационные компьютерные тренажеры, которые помогут вам быстрее восстановиться и научиться более эффективно управлять своим здоровьем."

Статус 6 (Общий прогресс).

"Мы продолжаем работать над совершенствованием методов лечения и используем накопленные данные для оптимизации процесса восстановления и улучшения качества жизни пациентов."

"Благодаря использованию искусственного интеллекта и современных технологий, мы стремимся улучшить качество жизни и обеспечить долгосрочное восстановление здоровья наших пациентов."

Интеллектуальная диагностика и лечение коронавируса с помощью КТМ.

В январе 2020 года китайское Министерство здравоохранения опубликовало протокол по диагностике и лечению коронавируса методами традиционной китайской медицины (КТМ).

Ученые Института информатики и процессов управления ДВО РАН интегрировали эти рекомендации в систему интеллектуальной диагностики болезней. Благодаря облачным вычислениям и искусственному интеллекту (ИИ), китайские врачи получили доступ к системе через платформу Китайской Ассоциации неправительственных медицинских учреждений, объединяющей 56 тысяч частных клиник по всей стране [3].

Система работает следующим образом: врач вводит в нее личные данные пациента, его жалобы и симптомы. ИИ, при необходимости, запрашивает дополнительную информацию. На основании полученных данных, система выносит вердикт о наличии или отсутствии заболевания. Затем, с учетом пола, возраста, общего состояния, стадии заболевания, система предлагает персональный план лечения, используя исключительно методы КТМ.

На сегодняшний день эта система, разработанная ИАПУ ДВО РАН на основе официальных данных Министерства здравоохранения Китая, является единственной официальной системой ИИ для диагностики и лечения коронавируса.

Внедрение системы в мировую практику осуществляется Центром учебных и образовательных программ ВОЗ при ВГУЭС.

Искусственный интеллект: новый шаг в психотерапии?

Психология традиционно считается неточной наукой, поскольку использует множество противоречивых подходов и не гарантирует абсолютную точность результатов. Внедрение искусственного интеллекта (ИИ) может изменить эту ситуацию, переводя психологию в разряд точных наук.

Уже сейчас существуют виртуальные психологи, работающие по принципу "искусственного интеллекта", и их эффективность сравнима с работой реальных специалистов. Эти приложения объединяют ИИ с виртуальной реальностью, позволяя общаться с клиентами в режиме реального времени.

Как же это работает?

Виртуальные психологи используют базы данных для формирования ответов, подбирая их в зависимости от заданного вопроса и добавляя эмоциональную окраску. Они способны не только давать советы, но и выражать сочувствие, предлагая несколько вариантов решения проблемы.

Популярные примеры таких виртуальных психологов.

1. Quartet Health: чат-бот с ИИ, который диагностирует состояние пациента и предлагает индивидуальный план лечения.

2. Элли: виртуальный терапевт, разработанный для лечения посттравматического стрессового расстройства (ПТСР).

3. X2A: платформа, объединяющая различные сервисы, такие как Карим (помощь сирийским беженцам), Эмма (помощь людям с тревогой) и Nema (педиатрическая помощь при диабете).

ИИ может также успешно справляться с лечением депрессии, одним из самых распространенных психических заболеваний. Он позволяет:

- обеспечить анонимность, что важно для многих людей, не желающих обращаться к реальному специалисту;
- устранить барьер незнания, помогая пользователям определить наличие депрессии;
- обеспечить доступность и доступную стоимость лечения, что особенно важно в условиях растущего разрыва между ценой и доступностью реальной терапии.

Примеры проектов, использующих ИИ для лечения депрессии.

Touchskin: чат-бот Wysa, который диагностирует депрессию и предлагает управляемые и неуправляемые медитации, напоминания и отслеживание прогресса.

Woebot: чат-бот, использующий когнитивно-поведенческую терапию (КПТ) для лечения депрессии.

Нейросетевая модель MIT: система, анализирующая текстовые и аудиоданные из интервью, выявляя признаки депрессии в речи.

В целом, ИИ предлагает новые, удобные и доступные решения для борьбы с психическими заболеваниями, обеспечивая поддержку и лечение даже без прямой встречи со специалистом.

Искусственный интеллект на службе неврологии: от диагностики до лечения.

Искусственный интеллект (ИИ) прочно интегрируется в сферу неврологии, предлагая новые подходы к диагностике и лечению.

Персонализированная медицина становится реальностью благодаря ИИ. Он позволяет создавать индивидуальные схемы лечения, учитывая особенности каждого пациента. Это особенно актуально при таких заболеваниях, как эпилепсия.

Управление припадками получило новый инструмент – Embrace – умные часы, разработанные MIT, способные отслеживать физиологические изменения, предшествующие припадку, без использования ЭЭГ. Часы отслеживают электрические импульсы в коже, предупреждают о припадке и предоставляют информацию о местоположении пациента.

Открытие лекарств также претерпевает революцию благодаря ИИ. Проекты Atomwise и MedClueRx анализируют огромные базы данных и помогают определять наиболее эффективные препараты для лечения различных неврологических расстройств, включая эпилепсию и заболевания желудочно-кишечного тракта [4].

Виртуальные помощники в психологии обеспечивают безопасную и комфортную среду для общения, особенно для людей, которые боятся или стесняются обращаться к реальным специалистам. Пациенты с большей вероятностью откроются и будут честны с виртуальным помощником, что повышает эффективность терапии.

В целом, ИИ открывает новые возможности в неврологии, позволяя улучшить диагностику, лечение и качество жизни пациентов.

Укрепление иммунитета с помощью искусственного интеллекта: новый подход к борьбе с вирусами

В борьбе с вирусными заболеваниями ключевую роль играет укрепление иммунной системы. Поскольку эффективные лекарственные иммуномодуляторы пока недоступны, на первый план выходит психоиммунология — наука, изучающая связь между психическим состоянием и иммунитетом [6].

Этот подход основан на активации иммунной системы через снижение стресса и достижение состояния глубокого спокойствия. Для этого применяются психотерапевтические методы, использующие "чистое квантовое состояние" и поддерживающие практику "майндфулнес" между сеансами.

С апреля 2020 года Центр учебных и образовательных программ ВОЗ при ВГУЭС предоставляет доступ к психоиммунологическим сеансам на платформе с искусственным интеллектом.

Роботы в хирургии: от помощников до микрохирургов будущего.

В 2018 году уже более 5 тысяч роботов ассистировали хирургам в более чем миллионе операций различной сложности. Хотя полноценные роботы-хирурги пока не стали реальностью, роботы-ассистенты уже демонстрируют свою эффективность, особенно в микрохирургии.

Роботы идеально подходят для повторяющихся задач, поскольку не устают и не допускают ошибок, характерных для человека. Кроме того, искусственный интеллект позволяет роботам достигать субмиллиметровой точности в хирургических манипуляциях.

Исследование, проведенное на 379 пациентах, прошедших ортопедические операции, показало, что использование роботов-ассистентов с ИИ снизило количество осложнений в 5 раз по сравнению с традиционными операциями. Также роботизированная хирургия с применением ИИ сокращает время пребывания пациентов в больнице на 21% за счет уменьшения количества осложнений и ошибок, что экономит отрасли 40 миллиардов долларов в год.

В 2022 году ученые из Northwestern University представили микроробота-краба толщиной 0,5 мм, способного не только двигаться, но и прыгать, крутиться и ползать. Этот прорыв открывает двери для создания роботов, способных выполнять ремонтные работы на наноуровне. В перспективе такие роботы, управляемые хирургами, смогут проводить малоинвазивные операции, избавляя пациентов от закупорки артерий и даже от злокачественных новообразований, воплощая в реальность фантастику о наноботах.

Искусственный интеллект (ИИ) неумолимо проникает в сферу здравоохранения, революционизируя диагностику, лечение и управление заболеваниями. Его потенциал для улучшения качества жизни и повышения доступности медицинской помощи огромен [5].

ИИ уже помогает врачам ставить более точные диагнозы, анализируя медицинские изображения и данные пациентов с несравненной скоростью и точностью. Алгоритмы машинного обучения способны предсказывать вероятность развития заболеваний и создавать индивидуальные планы лечения, учитывая уникальные особенности каждого пациента. Это позволяет проводить раннюю диагностику, своевременно назначать лечение и предотвращать развитие осложнений.

Особенно важную роль ИИ играет в области телемедицины. Он позволяет врачам удаленно консультировать пациентов, анализировать данные с носимых устройств и предоставлять персонализированные рекомендации. Это особенно актуально для жителей отдаленных регионов, где доступ к медицинской помощи ограничен.

Применение ИИ в здравоохранении также оптимизирует работу медицинских учреждений. Он автоматизирует рутинные задачи, освобождая время врачей для более сложных задач, а также позволяет анализировать огромные объемы данных и выявлять закономерности, недоступные человеческому глазу.

В целом, ИИ обладает потенциалом для значительного преобразования здравоохранения, делая его более эффективным, доступным и персонализированным. Несмотря на существующие вызовы, будущее здравоохранения тесно связано с ИИ. Важно продолжать развивать и совершенствовать ИИ-технологии в здравоохранении, чтобы максимально реализовать его потенциал и повысить качество жизни людей. Однако, несмотря на огромный потенциал, ИИ в здравоохранении сталкивается с рядом вызовов. К ним относятся вопросы конфиденциальности данных, этические аспекты использования ИИ-систем, а также необходимость их интеграции в существующие медицинские системы.

Список литературы

1. Баланов А. Н. Цифровизация в здравоохранении. Разработка, интеграция и внедрение современных систем: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — С.418-419.
2. Гуманитарные проблемы искусственного интеллекта и его применения: [монография] / А. Б. Гехт, Р. В. Душкин, А. В. Неровный, И. А. Цверидзашвили, К. Ю. Эйдемиллер; СПбГУТ. — Санкт-Петербург, 2024. — 207 с.

3. Идентичности: семиотика репрезентации и прагматика позиционирования: монография / под ред. А.А. Тесли, С.Т. Золяна, Г.Л. Тульчинского. — Калининград: Издательство БФУ им. И. Канта, 2022. — 309 с
4. Золкин, Александр Леонидович. Реализация принципов организации и использования средств машинного обучения и искусственного интеллекта в медицине: учебное пособие / А.Л. Золкин, В.Д. Мунистер. — Самара: Медицинский университет «Реавиз», 2024. — 72 с.
5. Кокорин, Валерий Николаевич Цифровые двойники биосистемы человека как механизм искусственного интеллекта в здравоохранении / В. Н. Кокорин. — Ульяновск: УлГТУ, 2023. — С. 8-9.
6. Францева, В.О. Современные тенденции в управлении здравоохранением: учеб. – метод. пособие / В.О. Францева, Д.С. Потапова, А.А. Федорова. — Ставрополь: Изд-во СтГМУ, 2022. — 39 с.

References

1. Balanov A. N. Digitalization in healthcare. Development, integration and implementation of modern systems: a textbook for universities / A. N. Balanov. — St. Petersburg: Lan, 2024. — pp.418-419.
 2. Humanitarian problems of artificial intelligence and its application: [monograph] / A. B. Geht, R. V. Dushkin, A.V. Nerovny, I. A. Tsverianashvili, K. Yu. Eidemiller; St. Petersburg State University. — St. Petersburg, 2024. — 207 p.
 3. Identities: semiotics of representation and pragmatics of positioning: monograph / edited by A.A. Tesli, S.T. Zolyan, G.L. Tulchinsky. — Kaliningrad: Publishing House of the BFU named after I. Kant, 2022. — 309 p.
 4. Zolkin, Alexander Leonidovich. Implementation of the principles of organization and use of machine learning and artificial intelligence in medicine: a textbook / A.L. Zolkin, V.D. Munister. — Samara: Medical University "Reaviz", 2024. — 72 p.
 5. Kokorin Valeriy Nikolaevich Digital Twins of Human Biosystem as a Mechanism of Artificial Intelligence in Health Care. — Ulyanovsk: UISTU, 2023. — pp.8-9.
 6. Frantseva, V.O. Sovremennye tendentsii v upravleniye zdravookhraneniym [Modern trends in health care]. —method. posobiye / V.O. Frantseva, D.S. Potapova, A.A. Fedorova. — Stavropol: StSMU Publ., 2022. — 39 p.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

¹Шаханова М.В., Четверик М.А., Шаханова В.С.

ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: ¹marinavl2007@yandex.ru

Защита информации в условиях чрезвычайных ситуаций представляет собой важную тему, которая охватывает множество аспектов, включая правовые, технические и организационные меры. Чрезвычайные ситуации, вызванные природными катастрофами и техногенными авариями, создают угрозу как для физической безопасности, так и для информационной инфраструктуры. В моменты опасности, данные и системы, обеспечивающие функционирование организаций и государственных структур, наиболее подвержены повреждению. Эффективная защита информации в условиях ЧС требует комплексного подхода, включающего не только анализ потенциальных угроз, уязвимостей и способы предотвращения потерь, но также методы защиты, не допускающие эти самые потери.

Ключевые слова: Чрезвычайная ситуация, угрозы, защита информации, информационные инфраструктуры, организации, методы защиты.

INFORMATION PROTECTION IN EMERGENCY SITUATIONS

¹Shakhanova M. V., Chetverik M.A., Shakhanova V.S.

MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: ¹marinavl2007@yandex.ru

Information protection in emergency situations is an important topic that covers many aspects, including legal, technical and organizational measures. Emergencies caused by natural disasters and man-made accidents pose a threat to both physical security and information infrastructure. In times of danger, the data and systems that ensure the functioning of organizations and government structures are most susceptible to damage. Effective protection of information in an emergency requires an integrated approach that includes not only analysis of potential threats, vulnerabilities and ways to prevent losses, but also protection methods that prevent these very losses.

Keywords: Emergency, threats, information protection, information infrastructures, organizations, protection methods.

Чрезвычайные ситуации. Угрозы и Уязвимости

Чрезвычайная ситуация (ЧС) - обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей. [1]

В условиях ЧС существует реальная угроза для защиты информации, что может привести к серьезным последствиям как для отдельных организаций, так и для национальной безопасности. Чрезвычайные ситуации могут вызвать разрушение инфраструктуры, включая

системы, отвечающие за хранение и обработку данных. В таких ситуациях организации рискуют потерять не только данные, но и доверие клиентов, партнеров и регуляторов.

Исходя из всего выше перечисленного, можно сформулировать потенциальные угрозы, которые могут коснуться информационных систем и повлиять на их функциональность в условиях чрезвычайных ситуациях.

Потенциальные угрозы:

1. Природные катастрофы

- Ураганы и торнадо: могут вызвать повреждение физической инфраструктуры и оборудования.
- Землетрясения: способны вызвать разрушение зданий и систем хранения данных.
- Наводнения: могут затопить серверные комнаты и офисы.

2. Техногенные аварии

- Пожары, утечки химических веществ.
- Поломка оборудования, сбой на сетях электроснабжения: приводит к отключению систем.

3. Кибератаки

- Кибератаки, атаки на инфраструктуру (DDoS, SQL-инъекции).
- Вредоносное ПО.

4. Человеческий фактор

- Ошибки сотрудников.
- Недостаточная осведомленность сотрудников.
- Умышленное или неумышленное раскрытие данных.

5. Террористические акты

- Уничтожение физической инфраструктуры.
- Кибератаки на критически важные системы.

Кроме физического разрушения, ЧС могут существенно ослабить или вовсе подорвать безопасность информационных систем. В хаотичной обстановке возрастает вероятность кибератак, когда злоумышленники могут воспользоваться ситуацией, чтобы получить доступ к системам, которые становятся менее защищенными. Поскольку внимание сотрудников и служб безопасности часто сосредоточено на разрешении текущих проблем, шанс на успешную кибератаку значительно увеличивается.

Уязвимости, возникающие при чрезвычайных ситуациях, могут возникать из-за повреждений оборудования, снижения качества обслуживания и человеческих ошибок. Рассмотрим наиболее критические из них:

1. Недостаточная защита данных

- Отсутствие шифрования и контроля доступа.
- Слабые пароли и их частая смена.

2. Системные уязвимости

- Отсутствие обновлений безопасности.
- Уязвимости в устаревших приложениях и ПО.
- Неправильные настройки, неверные конфигурации.

3. Отсутствие резервного копирования

- Неправильные или отсутствующие процедуры резервного копирования данных, как правило, в последующем, невозможность восстановления после утраты данных.
- 4. Неподготовленность персонала
- Недостаточная осведомленность о методах защиты информации.
- Отсутствие тренингов по действиям в условиях ЧС.
- Неполные или неэффективные процедуры реагирования на инциденты.
- Нехватка ресурсов для обеспечения безопасности.

Чрезвычайные ситуации могут возникнуть в любой момент, и не всегда люди и организации будут готовы к этому. Поэтому основной задачей в области защиты информации в условиях ЧС является не восстановление данных и поврежденного оборудования после происшествия, а минимизация или полное предотвращение нарушения работы оборудования в чрезвычайных условиях.

Это подчеркивает важность разработки комплексного подхода к защите информации, который учитывал бы риски, возникающие в условиях нестабильной обстановки, и указывал бы на методы повышения устойчивости информационных систем.

Законодательство и нормативные акты по защите информации в условиях ЧС

Существует множество законов и стандартов, регулирующих защиту информации в условиях чрезвычайных ситуаций. Эти документы определяют правовые рамки, обязательства и меры, которые должны принимать организации для обеспечения безопасности информации и минимизации последствий ЧС. Рассмотрим основные аспекты законодательства и нормативных актов:

1. Законодательные инициативы

В большинстве стран существуют специальные законы, касающиеся защиты информации и данных. К ним относятся законы о защите персональных данных, такие как Общий регламент по защите данных (GDPR) в Европейском Союзе и Закон о защите персональной информации (CIPA) в США. В России законом, регулирующим любые действия, связанные с информацией, выступает Федеральный закон "Об информации, информационных технологиях и о защите информации". Эти законы устанавливают требования относительно обработки, хранения и защиты данных, а также обязывают организации уведомлять пользователей о возможных утечках данных, что становится особенно актуальным в условиях ЧС. [4]

2. Нормативные акты по безопасности информации

На уровне национальных и международных стандартов разрабатываются нормативные акты, которые направлены на установление лучших практик в области информационной безопасности. Например:

- ISO/IEC 27001 — международный стандарт, который описывает требования к системам управления информационной безопасностью (СУИБ). Он включает рекомендации по идентификации и оценке рисков, что особенно актуально в условиях ЧС. [2]
- NIST SP 800-53 — набор рекомендаций от Национального института стандартов и технологий США, который предоставляет контрольные механизмы для управления рисками и защиты информации. [5]

Эти стандарты обеспечивают структуру для разработки внутренних политик и процедур, направленных на защиту информации и минимизацию потенциального ущерба.

3. Подготовка и реагирование на ЧС

Также имеются документы, описывающие порядок действий в случае возникновения ЧС. Например, в России действует Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», который определяет меру государственного реагирования на ЧС, включая обязательные требования для организаций по подготовке планов по защите информации.

Организации обязаны разрабатывать и внедрять планы реагирования на ЧС, которые включают процедуры по обеспечению устойчивости информационных систем, а также механизмов оперативного восстановления после инцидентов. Это включает в себя регулярные тренировки и учения, что позволяет поддерживать готовность и отрабатывать навыки реагирования. [3]

Методы предотвращения сбоев в информационных системах при ЧС

Обеспечение устойчивости информационных систем в условиях чрезвычайных ситуаций является критически важной задачей для организаций. Эффективные меры предосторожности позволяют минимизировать риски, связанные с потерей данных и нарушениями функционирования систем. Рассмотрим ключевые методы, которые можно использовать для предотвращения сбоев.

1. Разработка и внедрение планов реагирования

Первым шагом к предотвращению сбоя является создание детализированных планов реагирования на ЧС. Эти планы должны включать сценарии различных типов ЧС и четкие инструкции по действиям сотрудников. Необходимо определить ответственных лиц и создать рабочие группы, способные оперативно реагировать на угрозы. Регулярные тренировки помогут сотрудникам отработать действия в условиях стресса и нехватки ресурсов.

2. Обеспечение резервного копирования

Регулярное резервное копирование данных является основным компонентом защиты информации. Данные должны копироваться как на локальные устройства, так и в облачные хранилища, чтобы обеспечить доступ к ним в случае повреждения основной системы. Важно также тестировать процессы восстановления, чтобы убедиться, что в случае необходимости данные могут быть быстро восстановлены.

3. Использование технологий высокой доступности

Технологии высокой доступности позволяют минимизировать время простоя систем и обеспечить непрерывность бизнеса. Это может осуществляться с помощью кластеризации серверов, дублирования критически важных компонентов и использования географически распределенных дата-центров. Такие меры позволяют снизить вероятность полного отключения сервисов при возникновении ЧС.

4. Обучение сотрудников

Поддержание уровня осведомленности сотрудников о безопасности информации является важным аспектом предотвращения сбоев. Регулярные тренинги по вопросам безопасности, включая фишинг и другие киберугрозы, помогут предотвратить человеческие ошибки, которые могут привести к утечкам или повреждению данных.

5. Проведение регулярной оценки рисков

Организации должны регулярно проводить оценку рисков, связанных с защитой информации. Это включает в себя анализ потенциальных угроз и уязвимостей, а также определение возможности возникновения ЧС. На основе результатов такой оценки можно корректировать свои стратегии и планы реагирования, делая их более эффективными.

Применение этих методов способствует созданию безопасной и устойчивой инфраструктуры, что имеет решающее значение для обеспечения защиты информации в условиях нестабильной обстановки.

Заключение

Защита информации в условиях чрезвычайных ситуаций требует комплексного подхода, который основывается на тщательной оценке рисков и анализе угроз. Организации, осознающие риски и занимающиеся проактивной подготовкой к возможным инцидентам, способны значительно снизить вероятность потерь и сохранить свою репутацию. Внедрение эффективных планов реагирования, регулярное обучение сотрудников и взаимодействие с государственными структурами — ключевые элементы, позволяющие организациям адаптироваться и успешно действовать в изменчивой и неустойчивой обстановке.

Список литературы

1. Государственный стандарт РФ. Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий / авт. Всероссийский научно-исследовательский институт по проблемам ГО и ЧС с участием рабочей группы специалистов Технического комитета по стандартизации ТК 71 “Гражданская оборона, предупреждение и ликвидация чрезвычайных. - 1996 г.. - (ноябрь 2000 г.) с Изменением N 1, принятым в мае 2000 г. (ИУС N 8-2000).
2. Международный стандарт ISO/IEC 27001:2022. - 2022 г.. - Издание 3 .
3. Федеральный закон о защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера [В Интернете]. - 11 ноябрь 1994 г.. - https://www.consultant.ru/document/cons_doc_LAW_5295/.
4. Федеральный закон об информации, информационных технологиях и о защите информации [В Интернете]. - 8 июль 2006 г.. - https://www.consultant.ru/document/cons_doc_LAW_61798/.
5. Security and Privacy Controlsfor [В Интернете] / авт. FORCE JOINT TASK // Security and Privacy Controlsfor. - Sep 2020 г.. - NIST Special Publication 800-53 Revision 5. - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

References

1. The state standard of the Russian Federation. Safety in emergency situations. Terms and definitions of basic concepts / author. All-Russian Research Institute on Civil Defense and Emergency Situations with the participation of a working group of specialists of the Technical Committee for Standardization TC 71 “Civil Defense, prevention and liquidation of emergencies. - 1996. - (November 2000) with Amendment No. 1, adopted in May 2000 (IUS No. 8-2000).
2. International standard ISO/IEC 27001:2022. - 2022. - Edition 3 .

3. The Federal Law on the Protection of the Population and Territories from Natural and Man-made Emergencies [On the Internet]. - November 11, 1994. - https://www.consultant.ru/document/cons_doc_LAW_5295/.
 4. Federal Law on Information, Information Technologies and Information Protection [On the Internet]. - July 8, 2006. - https://www.consultant.ru/document/cons_doc_LAW_61798/.
 5. Security and Privacy Controlsfor [On the Internet] / auth. FORCE JOINT TASK // Security and Privacy Controlsfor. - Sep 2020. - NIST Special Publication 800-53 Revision 5. - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.42

RUSTSCAN: БЫСТРОЕ И ЭФФЕКТИВНОЕ СКАНИРОВАНИЕ ПОРТОВ С ИСПОЛЬЗОВАНИЕМ RUST

Бютнер С.И.

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

RustScan — это современный инструмент для быстрого сканирования открытых портов, созданный с использованием языка программирования Rust. RustScan помогает специалистам по информационной безопасности оперативно определять активные порты на устройствах и является альтернативой классическим инструментам, таким как Nmap, благодаря высокой скорости работы и эффективности. В статье рассматриваются ключевые особенности RustScan, его архитектура и технические возможности, а также приводятся рекомендации по его использованию в различных сценариях, включая интеграцию с другими средствами анализа безопасности.

Ключевые слова: RustScan, сканирование портов, безопасность, Rust, информационная безопасность, Nmap, сети.

RUSTSCAN: FAST AND EFFICIENT PORT SCANNING USING RUST

Buetner S.I.

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

RustScan is a modern tool for fast open port scanning, built using the Rust programming language. RustScan helps cybersecurity professionals quickly identify active ports on devices and serves as an alternative to traditional tools like Nmap, known for its speed and efficiency. This article explores the key features of RustScan, its architecture, and technical capabilities, while also providing recommendations for using it in various scenarios, including integration with other security analysis tools.

Keywords: RustScan, port scanning, security, Rust, cybersecurity, Nmap, networking.

Введение

Сканирование портов — это важная часть тестирования безопасности сети, позволяющая определить, какие порты открыты на устройстве, и выявить потенциальные точки входа для злоумышленников. Одним из классических инструментов для сканирования портов является Nmap, который стал стандартом в области сетевого анализа и информационной безопасности. Однако с увеличением количества подключённых устройств и потребностью в более быстрой обработке данных стало очевидным, что для эффективного анализа открытых портов нужны более производительные инструменты. Именно с этой целью был создан RustScan, написанный на языке программирования Rust. RustScan объединяет в себе высокую скорость работы, безопасность, присущую Rust, и продвинутые функции сканирования, что делает его отличным выбором для специалистов по кибербезопасности.

С помощью RustScan можно не только сократить время, затрачиваемое на обнаружение открытых портов, но и более гибко интегрировать его с другими инструментами для анализа сети и уязвимостей. Инструмент отличается производительностью и простотой использования, позволяя специалистам настраивать сканирование под различные задачи. RustScan разрабатывался с учётом последних стандартов безопасности, обеспечивая устойчивость к потенциальным ошибкам и утечкам памяти, что делает его надёжным и безопасным выбором.

RustScan

RustScan отличается от большинства инструментов для сканирования портов благодаря сочетанию производительности и стабильности, достигнутому благодаря использованию языка Rust. Rust обеспечивает безопасность памяти на уровне компиляции, что снижает риск утечек данных и других проблем, характерных для программ на C или C++. RustScan использует уникальную архитектуру многопоточности, что позволяет ему обрабатывать десятки тысяч запросов на проверку портов за секунды. Это даёт ему серьёзное преимущество перед аналогами, такими как Nmap, которые могут быть ограничены по скорости из-за особенностей своей архитектуры[1].

Одной из ключевых особенностей RustScan является возможность предварительной настройки для глубокого анализа. Пользователь может установить, какие порты сканировать, указать диапазон IP-адресов, выбрать степень детализации вывода и задать параметры, позволяющие автоматически передавать результаты для дальнейшей обработки в другие инструменты, например Nmap. Такая интеграция полезна для профессионалов, поскольку RustScan работает как мощный и быстрый инструмент первичного сканирования, а затем передаёт данные в Nmap для проведения глубокого анализа найденных портов. Это экономит значительное количество времени и позволяет оптимизировать процесс анализа безопасности сети[2].

RustScan может сканировать в несколько раз быстрее, чем большинство других доступных инструментов, благодаря тому, что он может обрабатывать до 3000 пакетов в секунду. Это делает его удобным инструментом для применения в условиях ограниченного времени или на сетях с большим количеством узлов. RustScan предлагает высокую степень настройки, что позволяет адаптировать его под задачи разного масштаба: от небольших сетей до крупных корпоративных инфраструктур. Пользователи могут задать максимальное количество потоков для оптимального использования ресурсов системы и установить ограничение на количество одновременных соединений для балансировки между скоростью и стабильностью работы[3].

Отдельного внимания заслуживает интерфейс RustScan, разработанный для удобства пользователей и легкости в освоении. Он включает интуитивно понятные опции командной строки, позволяющие гибко настраивать сканирование и указывать различные параметры, включая тайм-ауты, порты и уровень детализации. Интерфейс RustScan делает его привлекательным даже для начинающих специалистов, которым важно быстро начать работать с инструментом. Помимо этого, RustScan совместим с популярными операционными системами, включая Linux, macOS и Windows, что делает его универсальным решением для профессионалов по безопасности[4].

RustScan также предоставляет функции расширенного анализа и возможности интеграции с системами автоматизации сканирования, что позволяет настроить сканирование на регулярной основе и создавать отчёты. Инструмент может запускаться автоматически по расписанию, отправлять уведомления при обнаружении новых открытых портов или вносить данные в базу уязвимостей, что делает его особенно полезным в условиях непрерывного мониторинга безопасности сети. Таким образом, RustScan становится важным компонентом в системах безопасности, предоставляя не только высокую скорость и надёжность, но и возможности для масштабирования и автоматизации процессов.

Заключение

RustScan выделяется среди инструментов для сканирования портов благодаря высокой производительности, удобству настройки и поддержке интеграции с другими инструментами безопасности. В эпоху стремительного увеличения количества сетевых устройств и усиления угроз информационной безопасности быстрая и надёжная диагностика состояния сети является ключом к предотвращению атак. RustScan позволяет специалистам по кибербезопасности и сетевым администраторам быстро получать точные данные об активных портах, что помогает своевременно обнаруживать уязвимости и укреплять защиту.

Использование RustScan особенно выгодно в условиях, когда важно обеспечить скорость и безопасность анализа сети. Он объединяет достоинства языка Rust и проверенные методы сканирования, что делает его эффективным выбором как для небольших сетей, так и для крупных инфраструктур. Благодаря совместимости с Nmap и другими инструментами безопасности, RustScan представляет собой мощное средство, способное ускорить и упростить анализ сети. Внедрение RustScan в повседневные операции сетевого мониторинга помогает создать более устойчивую и защищённую среду, снижая риски и улучшая реакцию на возможные угрозы безопасности.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределённых 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. Method for evaluating the effectiveness of an information protection system geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
 3. Chmutov M. V. et al. 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 proceedings. – 2017. – pp. 535-537.
 4. Petrova T. V. et al. Approaches for 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 the classification of texts 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

РАЗРАБОТКА СИСТЕМЫ СБОРА НАБОРА ДАННЫХ ДЛЯ АНАЛИЗА ЭКСПЛОЙТОВ

Хихол Е.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: hiholl3@mail.ru*

В данной статье исследуется использование специальных сред для изолированного исполнения программ («песочниц») с целью сбора набора данных для последующего анализа эксплойтов. Представлены основные компоненты «песочницы», проведен их сравнительный анализ, описано использование вызовов API Windows для фиксации поведения вредоносных программ, а также предложена архитектура системы сбора набора данных для анализа эксплойтов.

Ключевые слова: Информационная безопасность; анализ вредоносных программ; кибербезопасность; набор данных; изолированная среда; классификация вредоносных программ; эксплойт.

DEVELOPING A DATA COLLECTION SYSTEM FOR EXPLOIT ANALYSIS

Khikhol E.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: hiholl3@mail.ru*

This paper examines the use of sandboxes to collect data for exploit analysis. The paper presents the main components of a sandbox, compares them, describes the use of Windows API calls to record malware behavior, and proposes an architecture for collecting data for exploit analysis.

Keywords: Information security; malware analysis; cyber security; dataset; sandbox environment; malware classification; exploit.

Введение.

Цель исследования заключается в разработке архитектуры системы сбора данных для анализа эксплойтов (т.е. компьютерных программ, использующих уязвимости в программном обеспечении). Система должна позволить собрать набор данных вызовов API в операционной системе Windows, выполненных эксплойтами, представленными в базе данных Exploit-DB¹. Для этого она должна включать в себя систему сбора и обработки данных от Exploit-DB (в том числе компиляции эксплойтов), песочницу, позволяющую запускать вредоносные файлы, и систему сбора и обработки информации о поведении и структурных характеристиках вредоносного программного обеспечения (ПО) [3, 6].

С помощью песочниц можно безопасно запускать вредоносное ПО в условиях, имитирующих реальную рабочую среду. Они применяются для анализа файлов и сбора

¹ <https://www.exploit-db.com/>

детализированной информации о поведении и структурных характеристиках вредоносного ПО, таких как вызовы API вредоносного ПО, дампы памяти, сетевой трафик и т.д. Песочница состоит из двух ключевых частей. Первая часть — это управляющая машина, на которой осуществляется анализ вредоносного ПО, сохраняются результаты в базу данных, и предоставляется веб-интерфейс для пользователей. Второй компонент — это анализирующие машины, на которых исполняется вредоносное ПО. Эти машины могут быть как виртуальными, так и физическими. В исследовании проведен подробный сравнительный анализ различных типов песочниц, доступных на рынке. Исследование охватывает ключевые характеристики, такие как поддерживаемая операционная система (ОС), стоимость, функциональность и требуемый уровень навыков для её использования. Были проанализированы следующие песочницы: Cuckoo Sandbox², FireEye Malware Analysis, Any.Run, Joe Sandbox, Check Point SandBlast Threat Emulation, FortiSandbox, Triage, Anubis, Falcon Sandbox, Hybrid analysis, CAPE Sandbox. В результате проведенного анализа, основанного на ключевых критериях, для разработки системы сбора данных была выбрана песочница Cuckoo Sandbox. Эта песочница поддерживает широкий спектр операционных систем, таких как Windows, Linux и macOS, что позволяет проводить анализ вредоносных программ на различных платформах. Одним из значимых преимуществ является наличие бесплатной версии с базовыми функциями, что делает её доступной для исследователей и разработчиков. Кроме того, Cuckoo Sandbox предоставляет информацию по каждому анализируемому объекту, включая скриншоты рабочего стола виртуальной машины, на которой запускается вредоносное ПО. При этом Cuckoo Sandbox имеет широкие функциональные возможности: она поддерживает анализ различных типов файлов, включая исполняемые файлы, документы, скрипты и даже URL-адреса, что помогает визуально оценить поведение вредоносной программы [4].

Cuckoo Sandbox включает в себя программное обеспечение для централизованного управления, которое контролирует процесс запуска и анализа образцов. Каждый анализ проводится на новой виртуальной машине в изолированной среде. Данная песочница состоит из управляющей машины (хоста, на котором работает управляющее ПО) и нескольких гостевых машин (виртуальных машин для выполнения анализа). Хост запускает основной компонент песочницы, который контролирует весь процесс анализа, а гостевые машины — это изолированные среды, где безопасно выполняются и исследуются образцы вредоносного ПО.

Вредоносные программы, действующие в операционной системе Windows, для достижения своих целей активно взаимодействуют с системными службами, используя API Windows. Предполагая, что вредоносное ПО работает на компьютере под управлением операционной системы Windows, оно должно использовать системные службы операционной системы. Все запросы к этим службам (вызовы Windows API) формируют вредоносное поведение. Программа, работающая в среде Windows, использует API для доступа к функциям, предоставляемым операционной системой. Когда приложение выполняется в операционной системе, оно вызывает различные API для выполнения своих задач. Анализ вызовов API позволяет получить подробное представление о том, как вредоносное ПО взаимодействует с операционной системой и как оно использует её ресурсы для реализации

² <https://github.com/cuckoosandbox>

своих функций. Таким образом, подход, основанный на вызовах API, широко используется для динамического анализа вредоносных программ, показывая точность их поведения [1, 5, 7].

Предлагаемая архитектура системы сбора данных для анализа эксплойтов включает следующие компоненты: (1) подсистема сбора и обработки данных от Exploit-DB, включая подсистему сбора данных, подсистему предобработки исходных кодов эксплойтов и подсистему компиляции эксплойтов; (2) Cuckoo Sandbox, включая сервер и кластер виртуальных машин; (3) систему сбора и обработки данных при запуске эксплойтов, включая систему сбора журналов API и их обработки и представления в JSON формате для последующего анализа [2].

Получаемые наборы данных могут применяться в различных исследованиях по анализу вредоносного ПО.

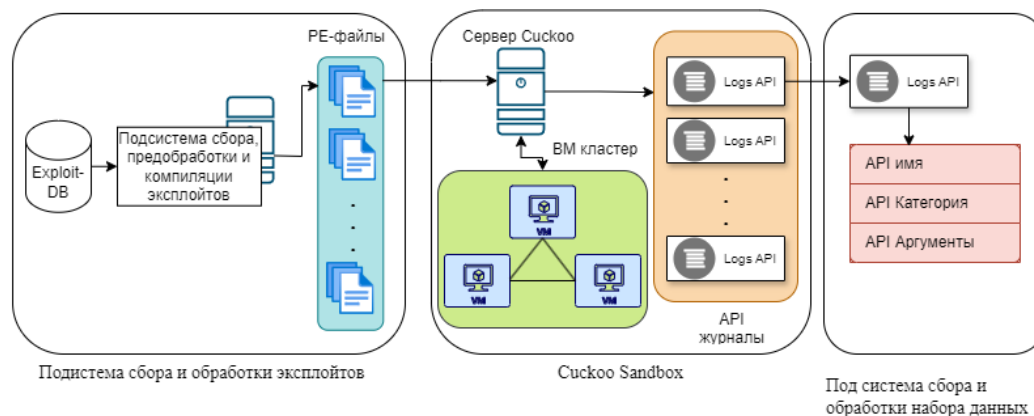


Рисунок 1. - Архитектура системы сбора набора данных для анализа эксплойтов

Заключение.

Основной целью было создание эффективной системы, которая может собирать, обрабатывать и анализировать данные о поведении вредоносных программ в безопасной и изолированной среде. Сбор данных о вызовах API имеет ключевое значение для понимания того, как вредоносное ПО использует ресурсы операционной системы для достижения своих целей. Через анализ этих вызовов можно выявить особенности поведения эксплойтов, которые не всегда очевидны при статическом анализе. Это делает подход, основанный на динамическом анализе с использованием вызовов API, критически важным для детального изучения методов эксплуатации уязвимостей. Важной частью системы является песочница, позволяющая безопасно исполнять вредоносное ПО. Cuckoo Sandbox обладает рядом преимуществ, таких как поддержка различных операционных систем, возможность анализа множества типов файлов и предоставление детализированной информации о поведении вредоносных программ. Эти возможности делают её идеальным кандидатом для целей данного исследования, так как она не только гибка и функциональна, но и доступна для широкого круга пользователей.

Список литературы

1. Ferhat Ozgur Catak, Cyber Security Institute Tubitak-Bilgem// 2021. A benchmark API call dataset for Windows PE malware classification. [Электронный ресурс] URL: [1905.01999](https://doi.org/10.19055/ijit.v9i12.1999).

2. Zhaoqi Zhang, Panpan Qi, Wei Wang. Dynamic Malware Analysis with Feature Engineering and Feature learning // School of Computing National University of Singapore. 2020. pp.1211-1212
3. Ferhat Ozgur Catak, Ahmet Faruk Yazı, Ogerta Elezaj and Javed Ahmed. Deep learning based Sequential model for malware analysis using Windows exe API Calls // PeerJ Computer Science. July 2020. pp.5-7.
4. **Cuckoo Sandbox Developers**. 2012. *Cuckoo Sandbox: Automated Malware Analysis*. URL: <https://cuckoosandbox.org>
5. Зайченко И.А., Большаков А.С. Об использовании системных вызовов WIN-API для обнаружения модифицированного вредоносного ПО // Телекоммуникации и информационные технологии. 2022. С. 28-36.
6. И. В. Гаврилов, Р. А. Смирнов. Предложения по реализации алгоритма автоматизации активного тестирования приложений. XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023)». 2. 2023. С. 513-518.
7. Я. А. Ильин, А. И. Катасонов. Определение характерных особенностей для обнаружения вредоносного программного обеспечения. XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023)». 4. 2023. С. 629-633.

References

1. Ferhat Ozgur Catak, Cyber Security Institute Tubitak-Bilgem// 2021. A benchmark API call dataset for Windows PE malware classification. [Electronic resource] URL: 1905.01999.
 2. Zhaoqi Zhang, Panpan Qi, Wei Wang. Dynamic Malware Analysis with Feature Engineering and Feature learning // School of Computing National University of Singapore. 2020. . pp.1211-1212
 3. Ferhat Ozgur Catak, Ahmet Faruk Yazı, Ogerta Elezaj and Javed Ahmed. Deep learning based Sequential model for malware analysis using Windows exe API Calls // PeerJ Computer Science. July 2020. . pp.5-7.
 4. Cuckoo Sandbox Developers. 2012. Cuckoo Sandbox: Automated Malware Analysis. URL: <https://cuckoosandbox.org>
 5. Zaichenko I.A., Bolshakov A.S. On the use of WIN-API system calls to detect modified malware // Telecommunications and Information Technologies. 2022. pp. 28-36.
 6. I.V.Gavrilov, R.A.Smirnov. Proposals for the implementation of an algorithm for automating active application testing. XII
 7. A. Ilyin, A. I. Katasonov. Identify features for malware detection. XII International Scientific, Technical and Scientific-Methodological Conference "Actual Problems of Infotelecommunications in Science and Education (APINO-2023)". 4. 2023. pp. 629-633.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.9(075.8)

ОБЪЕКТНО-ВИЗУАЛЬНЫЙ СПОСОБ МОДЕЛИРОВАНИЯ ЗАМКНУТОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕМПЕРАТУРОЙ С ДВУХСТУПЕНЧАТЫМ КОНТРОЛЛЕРОМ

¹Царегородцев Е.Л., ²Романенков А.А., ³Соколов А.Д.

¹ФГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Смоленск, Россия (214000, г. Смоленск, ул. Пржевальского, 4), e-mail: evgencar@rambler.ru.

^{2,3}ФГБОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МЭИ" (ФИЛИАЛ В Г.СМОЛЕНСКЕ) Смоленск, Россия (214013, Смоленская область, город Смоленск, Энергетический пр-д, д. 1).

Современное программное обеспечение позволяет проводить компьютерное моделирование с достаточной степенью правдоподобности, соответствующей реальным физическим технологическим процессам. Интерес вызывает объектно-визуальный способ, который не требует написания сложного программного кода и представляет результаты в реальном масштабе времени. В статье представлена модель замкнутой системы управления температурой на основе высокоуровневой программы для численного моделирования.

Ключевые слова: Замкнутая система, объектно-визуальный способ, блок-схема, система управления.

AN OBJECT-VISUAL METHOD FOR MODELING A CLOSED TEMPERATURE CONTROL SYSTEM WITH A TWO-STAGE CONTROLLER

¹Tsaregorodtsev E.L., ²Romanenkov A.A., ³Sokolov A.D.

¹SMOLENSK STATE UNIVERSITY, Smolensk, Russia (214000, Smolensk, Przhivalskogo str., 4.), e-mail: evgencar@rambler.ru.

^{2,3}"NATIONAL RESEARCH UNIVERSITY "MPEI" (BRANCH IN SMOLENSK) Smolensk, Russia (214013, Smolensk region, Smolensk, Energeticheskyy proezd, 1)

Modern software allows computer simulations to be carried out with a sufficient degree of plausibility corresponding to real physical technological processes. Of interest is the object-visual method, which does not require writing complex program code and presents the results in real time. The article presents a model of a closed temperature control system based on a high-level program for numerical simulation.

Keywords: Closed-loop system, object-visual method, flowchart, control system.

Любой технологический процесс предполагает строгое выполнение конкретной последовательности действий в соответствии со временем при соблюдении технологических параметров, таких, как температура, влажность, плотность и т.д. Системы управления температурой имеют широкое применение в различных отраслях, включая промышленность, бытовое оборудование и научные исследования [1].

Одним из важных аспектов проектирования таких систем является выбор алгоритма управления. В данной статье рассмотрен объектно-визуальный способ моделирования

замкнутой системы управления температурой с двухступенчатым контроллером, на основе использования программы Scilab Xcos.

Scilab — это высокоуровневая программа для численного моделирования, в которой Xcos предоставляет пользователям возможность визуально конструировать системы управления и моделировать динамические процессы [2].

Xcos основан на графическом интерфейсе и использует концепцию блочных диаграмм, что позволяет удобно создавать и настраивать модели систем различной сложности без глубокого погружения в программирование.

Все расчеты в компьютерной модели выполняются в системном времени, соответствующему реальному времени функционирования объекта исследования или системы. Воспроизведение на компьютере развернутого во времени процесса функционирования системы с учетом ее взаимодействия с внешней средой предполагает имитационное моделирование.

Имитационное моделирование наиболее мощный и универсальный метод исследования и оценки эффективности систем, поведение которых зависит от случайных факторов [3]. Модели являются хорошим средством для обучения и подготовки специалистов, а также средством прогнозирования поведения объектов и систем. Моделирование позволяет проводить контролируемые эксперименты в ситуациях, когда проведение экспериментов на реальных объектах является нецелесообразным, опасным, невозможным или достаточно дорогостоящим.

Замкнутая система управления температурой состоит из трех основных элементов: объекта управления (некоторое устройство, чья температура подлежит регулированию), контроллера и устройства измерения температуры. В данной модели мы рассмотрим двухступенчатый контроллер, который включает в себя два уровня управления: грубый (коэффициент пропорциональной регулировки) и тонкий (коэффициент интегральной регулировки).

Грубый контроль: на этом этапе контроллер реагирует на отклонение температуры от заданного значения, управляя, например, нагревательным элементом. Как только температура превышает установленное значение, контроллер отключает нагреватель.

Тонкий контроль: при малых отклонениях от заданного значения активируется интегральный регулятор, который более точно поддерживает стабильную температуру, управляя нагреванием с учетом накопленных отклонений.

Инициализация Xcos: запускаем Scilab и открываем Xcos. На графическом интерфейсе появляется рабочая область для построения модели.

Добавление блоков: с помощью библиотеки блоков Xcos добавляем необходимые элементы: блок для объекта управления, измерения температуры, а также два блока контроллера.

Настройка блоков: настраиваем параметры блоков, включая коэффициенты, которые управляют поведением контроллера. Это позволяет задать диапазон, в котором будет работать контроллер, и размеры откликов.

Соединение блоков: создаем соединения между блоками для формирования потока данных. Каждый блок будет передавать информацию о текущем состоянии системы другому блоку.

Запуск модели: после завершения настройки запускаем модель рис. 1 для наблюдения за динамикой изменения температуры во времени.

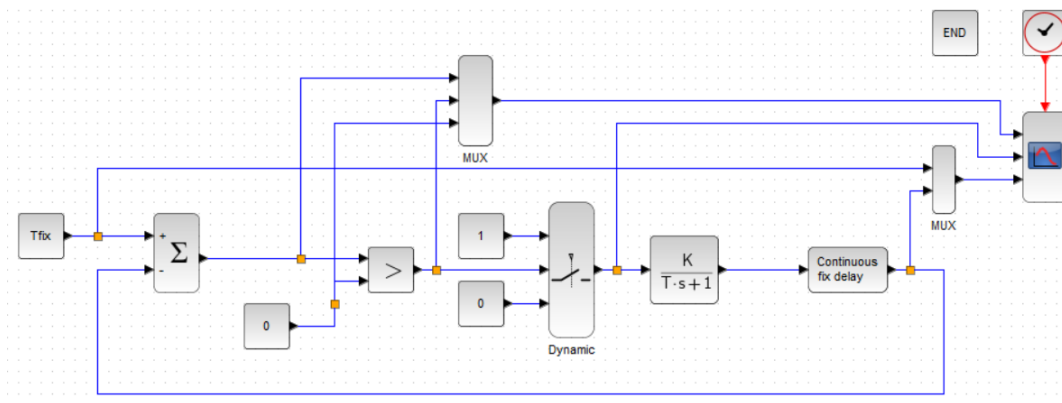


Рисунок 1. - Блок-схема замкнутой системы управления температурой

После запуска модели в Xcos становится видно, как система реагирует на изменения температуры в зависимости от заданных параметров контроллера рис. 2. Анализ результатов позволяет выявить, насколько эффективно работают два уровня управления: грубый и тонкий. Основными критериями оценки являются скорость достижения заданной температуры и стабильность состояния.

1-й график: черная линия – это разница температур; зелёная ступенчатая линия выход блока-решателя неравенства, иллюстрирующий переход через нуль; красная - линия $y = 0$

2-й график: режимы контроллера 1 – вкл, 0 – выкл

3-й график: красная линия на графике желаемая температура, синяя линия снимаемая датчиком температура.

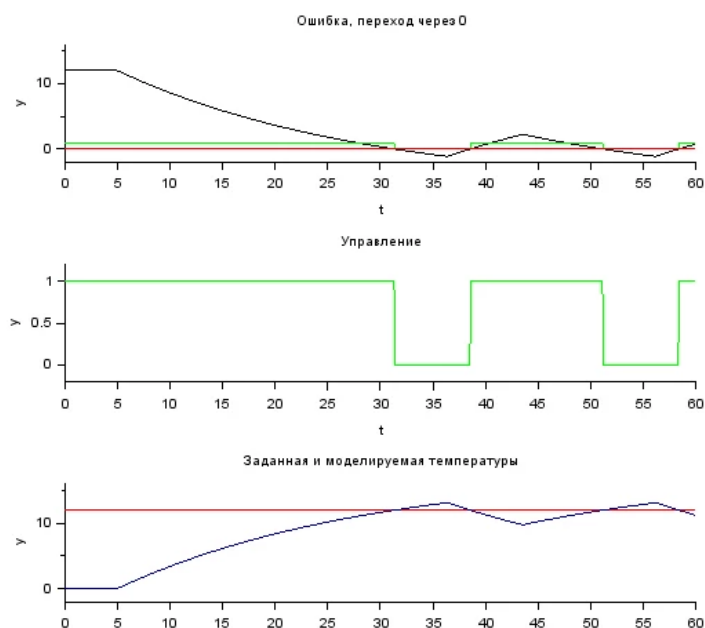


Рисунок 2. - Результаты моделирования

Объектно-визуальный способ моделирования замкнутой системы управления температурой с двухступенчатым контроллером в программе Scilab Xcos является удобным и эффективным подходом для исследователей и инженеров 4]. Использование этого метода позволяет значительно упростить процесс разработки, настройки и оптимизации систем управления, обеспечивая наглядное представление сложных процессов и возможность быстрой корректировки параметров.

В будущем данная методология может быть расширена для моделирования более сложных систем управления с учетом нелинейностей и внешних возмущений [5].

Список литературы

1. Гайнуллин, Р. Н. Основы контроля давления и температуры в технологических процессах: Учебно-методическое пособие / Р. Н. Гайнуллин, А. Р. Герке, А. В. Лира. – Казань: Казанский национальный исследовательский технологический университет, 2018. – 80 с.
2. Алексеев, Е. Р. Scilab Решение инженерных и математических задач / Е. Р. Алексеев, О. В. Чеснокова, Е. А. Рудченко. – Москва: Библиотека ALT Linux, 2008. – 260 с.
3. Имитационное моделирование: учеб. пособие / М. С. Эльберг, Н. С. Цыганков. – Красноярск: Сиб. федер. ун-т, 2017 –128 с.
4. <https://www.skf-mtusi.ru/umo/090301vmt/48.1/lr%20i%20pz%20Scilab.pdf>.
5. <https://technology.snauka.ru/2017/05/13530>.

References

1. Gainullin R. N., Gerke A. R., Lira A. V. Osnovy kontrolya napravleniya i temperatura v tekhnologicheskikh protsessakh: Uchebno-metodicheskoe posobie [Fundamentals of pressure and temperature control in technological processes: Textbook]. – Kazan: Kazan National Research Technological University, 2018. – p. 80
 2. Alekseev, E. R. Scilab Solution of Engineering and Mathematical Problems / E. R. Alekseev, O. V. Chesnokova, E. A. Rudchenko. – Moscow: ALT Linux Library, 2008. – p.260.
 3. Simulation Modeling: Textbook. posobiye / M. S. Elberg, N. S. Tsygankov. – Krasnoyarsk: Sib. federal. University, 2017 – p. 128
 4. <https://www.skf-mtusi.ru/umo/090301vmt/48.1/lr%20i%20pz%20Scilab.pdf>.
 5. <https://technology.snauka.ru/2017/05/13530>.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

КЕЙС-СТАДИИ: ПЕРВОПРОХОДЦЫ ВНЕДРЕНИЯ ИИ

Колода Е.

*Колода Консалтинг, Торонто, Канада (7142 Брениганские ворота, Миссиссога, НА L5N 7L5),
e-mail: ekoloda@kolodaconsulting.com*

Эволюция искусственного интеллекта (ИИ) вызвала технологическую революцию, трансформирующую отрасли благодаря инновационным приложениям и продвинутой аналитике. От предиктивного обслуживания до персонализированного клиентского опыта, первопроходцы ИИ успешно продемонстрировали преобразующую силу этой технологии. В данной статье рассматриваются кейс-стадии ведущих организаций, внедривших ИИ, с акцентом на стратегии, обеспечившие их успех, вызовы, с которыми они столкнулись, и уроки, извлеченные из их опыта.

Ключевые слова: Первопроходцы ИИ, цифровая трансформация, предиктивная аналитика, эффективность бизнеса, инновации в отрасли.

CASE STUDIES: PIONEERS IN AI IMPLEMENTATION

Koloda E.

*Koloda Consulting, Toronto, Canada. (7142 Branigan Gate, Mississauga, ON L5N 7L5), e-mail:
ekoloda@kolodaconsulting.com*

The evolution of Artificial Intelligence (AI) has sparked a technological revolution, transforming industries through innovative applications and advanced analytics. From predictive maintenance to personalized customer experiences, AI pioneers have successfully demonstrated the transformative power of this technology. This article not only explores case studies of leading organizations that have embraced AI, but also critically analyzes their strategies, outcomes, and the specific challenges they faced. It goes beyond a descriptive overview, offering key lessons that can be applied by other businesses seeking to adopt AI.

Keywords: AI pioneers, digital transformation, predictive analytics, business efficiency, industry innovation.

Introduction

Artificial Intelligence (AI) is at the forefront of a transformative shift across numerous industries. No longer a futuristic concept, AI has become an integral part of modern business, embedded in tools and systems that manage complex operations, enhance decision-making, and drive innovation. Despite the widespread advancements, the journey towards effective AI adoption is not without its challenges. Many businesses face issues such as high implementation costs, data privacy concerns, and workforce adaptation hurdles.

This article delves into the journeys of several pioneering companies that have successfully implemented AI solutions. By providing a detailed analysis of these case studies, we aim to demonstrate not only the transformative potential of AI but also the complexities involved in achieving effective AI integration. This deeper exploration includes the specific context in which AI was adopted, the unique challenges faced by each company, and a comparative analysis of how different strategies yielded varied outcomes. We also offer insights into future AI trends and practical lessons that can guide businesses on their own AI adoption journey.

AI Implementation Pioneers: Case Studies

1. Rolls-Royce: AI-Driven Predictive Maintenance

Rolls-Royce, a name synonymous with engineering excellence, has integrated AI into its maintenance services for aircraft engines. Utilizing a combination of AI and IoT sensors, Rolls-Royce's engines are now equipped to send real-time data to centralized systems. The AI algorithms analyze this data to predict maintenance needs before a failure occurs, ensuring aircraft stay operational with minimal downtime.

Data-driven insights reveal that this AI-based predictive maintenance approach has resulted in a 30% reduction in unscheduled engine maintenance and a 15% decrease in overall operational costs. The predictive models not only reduce downtime but also extend engine lifespan, translating to millions in cost savings annually [1].

A key aspect of Rolls-Royce's success has been collaboration. By partnering with Microsoft Azure, Rolls-Royce leveraged cloud AI capabilities to enhance data analytics and create predictive models. This partnership not only reduced costs associated with engine maintenance but also set a new industry standard for proactive equipment management.

A critical element of Rolls-Royce's AI journey was its ability to gain organizational buy-in. Leadership emphasized the importance of AI literacy, ensuring that key stakeholders understood both the potential benefits and the limitations of AI. This cultural shift was pivotal in overcoming initial resistance and fostering a company-wide embrace of AI technologies.

2. Starbucks: AI for Customer Experience Personalization

Starbucks has long been known for its customer-centric business model. Leveraging AI, the coffee giant has redefined personalization in customer service. Using the "Deep Brew" initiative, Starbucks harnesses AI to analyze customer preferences and tailor recommendations accordingly, whether in-store or via the mobile app.

According to internal data, AI-driven personalization efforts have increased customer engagement by 20% and resulted in a 15% boost in average transaction values [2]. Deep Brew utilizes AI for everything from inventory management to predicting customer orders, thereby reducing waste and optimizing supply chains. This seamless integration has contributed to improved customer satisfaction and an enhanced overall experience, demonstrating the power of AI in elevating brand loyalty.

Starbucks' approach stands out for its combination of data analytics and human intuition. The company's AI-driven personalization is effective because it does not replace human customer service but rather enhances it, allowing employees to focus on meaningful interactions with customers. This hybrid approach has been instrumental in strengthening the bond between Starbucks and its clientele, highlighting the importance of balancing AI capabilities with human elements.

3. Siemens: AI in Manufacturing and Industrial Automation

Siemens has been a leading figure in leveraging AI to advance Industry 4.0. By deploying AI-driven automation solutions, Siemens has optimized manufacturing processes across various production plants. Predictive analytics allow the detection of anomalies before they escalate into problems, significantly minimizing the risks of costly downtimes.

Data from Siemens suggests that their AI implementation has led to a 40% improvement in production efficiency and a 20% reduction in defect rates [3]. AI-powered robots work alongside

human operators, improving productivity without replacing the human workforce. Siemens' approach highlights the role of AI as a collaborator rather than a competitor in the industrial sector.

A notable challenge Siemens faced was the integration of AI into existing legacy systems. To address this, Siemens adopted a phased implementation strategy, which included pilot projects and proof of concept (PoC) testing. This method allowed them to fine-tune AI models and demonstrate value before scaling up. Siemens' success underscores the importance of phased rollouts in mitigating risk and ensuring smooth AI integration.

4. Alibaba: AI for Smart Retail

Alibaba, one of the largest e-commerce platforms in the world, uses AI to enhance both online and offline shopping experiences. The "AI Customer Brain" leverages deep learning algorithms to provide personalized product recommendations, boosting user engagement and increasing sales conversion rates.

According to a report by Alibaba, their AI-driven recommendation engine has led to a 35% increase in conversion rates, significantly boosting revenue [4]. Additionally, Alibaba has pioneered the concept of "New Retail," which integrates online and offline data to create seamless shopping experiences. In physical stores, AI technologies such as facial recognition enable personalized promotions, while smart supply chain management ensures products are restocked efficiently.

Alibaba's success in AI implementation is attributed to its focus on seamless integration of online and offline data, which has transformed the shopping experience. A key takeaway from Alibaba's journey is the importance of breaking down data silos. By centralizing data from multiple sources, Alibaba has created a more holistic view of its customers, allowing for highly personalized experiences that drive both customer satisfaction and loyalty.

5. Pfizer: AI in Drug Discovery

The pharmaceutical industry has traditionally faced lengthy and costly drug discovery processes. Pfizer has adopted AI to expedite these timelines, focusing on faster identification of promising compounds. By collaborating with IBM's Watson, Pfizer applies machine learning models to vast datasets, helping researchers identify potential drug candidates far more quickly than conventional methods.

Data-driven analysis shows that Pfizer's use of AI has reduced drug discovery times by 30%, while cutting associated research costs by up to 20% [5]. This AI integration has significantly reduced both time and costs involved in bringing new drugs to market. Pfizer's pioneering use of AI highlights the transformative potential of AI in healthcare, emphasizing innovation through collaboration with technology partners.

Pfizer's experience reveals the crucial role of partnerships in successful AI adoption. Collaborating with IBM provided access to AI expertise and computing power that would have been costly to develop in-house. This highlights the strategic value of partnerships, particularly for organizations venturing into new technological domains where they lack internal expertise.

6. Tesla: AI in Autonomous Driving

Tesla is a widely recognized leader in the development of autonomous driving technology. The company employs AI to train its self-driving software, using vast amounts of real-world driving data collected from its vehicles. Tesla's approach involves neural networks that continuously learn from

new data, allowing for rapid improvements in the vehicle's ability to navigate complex driving scenarios.

According to Tesla, their AI-powered Autopilot system has improved driving safety by reducing accident rates by approximately 40% when engaged [6]. Tesla's AI models analyze billions of miles of driving data to make split-second decisions that enhance both safety and user experience. This data-driven approach has established Tesla as a pioneer in autonomous driving and serves as a benchmark for the future of automotive technology.

A key element of Tesla's strategy is its data-centric approach. By collecting massive amounts of driving data, Tesla has been able to improve the accuracy and reliability of its AI models. The company's ability to iteratively update its models based on real-world feedback has been instrumental in accelerating the development of autonomous features. Tesla's journey illustrates the power of leveraging vast datasets to refine AI capabilities continuously.

7. Google: AI for Data Center Optimization

Google has leveraged AI to optimize the energy efficiency of its massive data centers. By employing DeepMind's AI algorithms, Google has been able to reduce energy usage for cooling by 40%. The AI system uses real-time data to make adjustments to cooling systems, predicting temperature changes and optimizing fan speeds to minimize energy consumption.

A report by Google highlighted that this AI-driven optimization has resulted in a 15% overall reduction in power usage effectiveness (PUE) across its data centers [7]. This case study showcases how AI can be applied not only for consumer-facing applications but also for significant operational efficiencies, reducing environmental impact and operational costs.

Google's approach demonstrates the application of AI in operational efficiency beyond customer engagement. A key insight from Google's experience is the value of using AI to address environmental sustainability issues. By optimizing data center operations, Google has not only reduced costs but also minimized its carbon footprint, showing that AI can be a powerful tool in supporting corporate sustainability goals.

Conclusion and Call to Action

The adoption of AI is inevitable, and businesses need to align with this trend to stay competitive. The debate over AI adoption isn't just about technology; it's about preparing for a future where AI is integral to business success. The examples provided illustrate how AI can transform business operations, enhance efficiency, and create new value.

To succeed, businesses must invest in strategic partnerships, workforce reskilling, and AI-driven innovation. For companies looking to start their AI journey, the experiences of these pioneers offer a valuable roadmap for navigating both the opportunities and challenges of AI adoption.

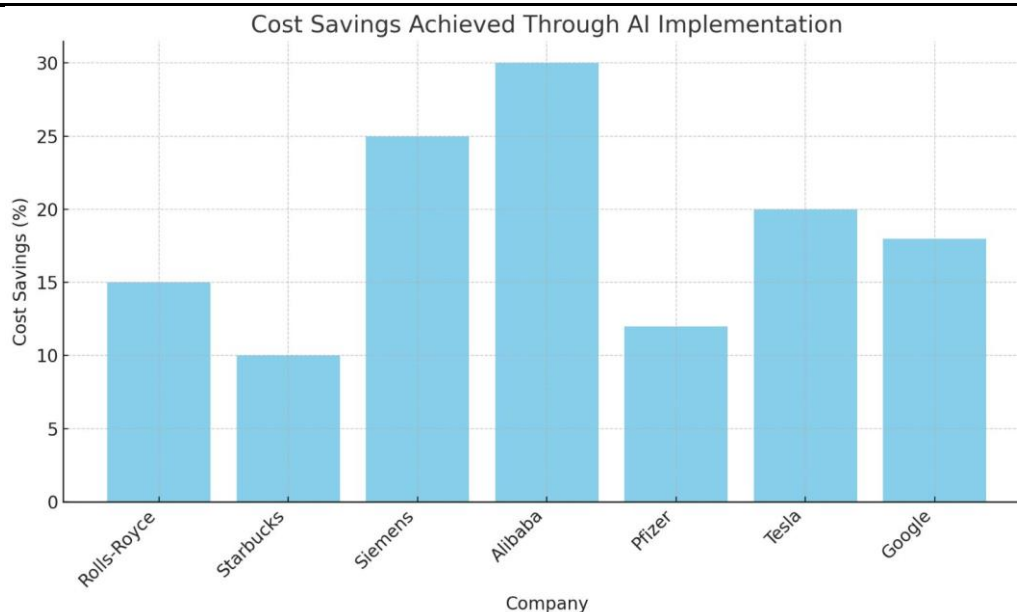


Figure 1. - Cost savings achieved trough AI implementation

Let's shape the future together.

Список литературы

1. Партнерство Rolls-Royce и Microsoft Azure в области профилактического обслуживания. Доступно по адресу: <https://www.microsoft.com/rolls-royce-predictive-maintenance>
2. Инициатива Starbucks Deep Brew и показатели персонализации. Доступно по адресу: <https://www.starbucks.com/deep-brew-ai-impact>
3. Отчет Siemens Industry 4.0 и автоматизация на основе искусственного интеллекта. Доступен по адресу: <https://www.siemens.com/ai-manufacturing-impact>
4. Отчет Alibaba "Мозг клиента с искусственным интеллектом" и коэффициент конверсии. Доступен по адресу: <https://www.alibaba.com/ai-customer-brain>
5. Совместная работа Pfizer и IBM Watson по разработке лекарств. Доступно по адресу: <https://www.ibm.com/pfizer-watson-drug-discovery>
6. Отчет о безопасности автопилота Tesla. Доступно по адресу: <https://www.tesla.com/autopilot-safety>
7. Искусственный интеллект Google DeepMind для оптимизации центров обработки данных. Доступно по адресу: <https://www.google.com/deepmind-data-center-efficiency>

References

1. Rolls-Royce and Microsoft Azure Partnership for Predictive Maintenance. Available at: <https://www.microsoft.com/rolls-royce-predictive-maintenance>
2. Starbucks Deep Brew Initiative and Personalization Metrics. Available at: <https://www.starbucks.com/deep-brew-ai-impact>
3. Siemens Industry 4.0 and AI-Driven Automation Report. Available at: <https://www.siemens.com/ai-manufacturing-impact>
4. Alibaba's AI Customer Brain and Conversion Rate Report. Available at: <https://www.alibaba.com/ai-customer-brain>

5. Pfizer and IBM Watson Collaboration for Drug Discovery. Available at: <https://www.ibm.com/pfizer-watson-drug-discovery>
 6. Tesla Autopilot Safety Report. Available at: <https://www.tesla.com/autopilot-safety>
 7. Google DeepMind AI for Data Center Optimization. Available at: <https://www.google.com/deepmind-data-center-efficiency>
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 629.11

ИНТЕГРАЦИЯ ВЕТРОГЕНЕРАТОРОВ В ТРАНСПОРТНЫЕ СРЕДСТВА И ПЕРСПЕКТИВЫ ИХ ИСПОЛЬЗОВАНИЯ В АРКТИЧЕСКОМ РЕГИОНЕ

Родионов Д. Р., Литвин Р. А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ", Санкт-Петербург, Россия (190005, город Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: deniro07032003@gmail.com

В статье рассматриваются перспективы интеграции ветрогенераторов в транспортные средства с целью повышения автономности и экологичности транспорта, а также возможность их применения в условиях Арктического региона. Описывается принцип работы ветрогенераторов на основе регенерации энергии во время движения и торможения транспортных средств, что позволяет уменьшить расход топлива и повысить энергоэффективность. Обсуждаются оптимальные условия для функционирования ветрогенераторов на различных типах транспортных средств, включая седельные грузовики, а также специфика их эксплуатации в суровых климатических условиях Арктики. Представленные результаты исследований подтверждают, что использование ветрогенераторов в транспорте способствует снижению зависимости от традиционных источников энергии и является перспективным направлением устойчивого развития.

Ключевые слова: Ветрогенератор, транспортные средства, Арктика, регенерация энергии, автономность, экологичность, возобновляемые источники энергии, лобовое сопротивление, энергоэффективность, устойчивое развитие.

INTEGRATION OF WIND TURBINES INTO VEHICLES AND PROSPECTS FOR THEIR USE IN THE ARCTIC REGION

Rodionov D. R., Litvin R. A.

ST. PETERSBURG STATE UNIVERSITY OF ARCHITECTURE AND CIVIL ENGINEERING, St. Petersburg, Russia (4 2nd Krasnoarmeyskaya st., St. Petersburg 190005, Russian Federation), e-mail: deniro07032003@gmail.com

The article discusses the prospects for integrating wind turbines into vehicles in order to increase the autonomy and environmental friendliness of transport, as well as the possibility of their use in the Arctic region. The principle of operation of wind turbines based on energy regeneration during movement and braking of vehicles is described, which reduces fuel consumption and increases energy efficiency. The optimal conditions for the operation of wind turbines on various types of vehicles, including saddle trucks, as well as the specifics of their operation in the harsh climatic conditions of the Arctic are discussed. The presented research results confirm that the use of wind turbines in transport helps to reduce dependence on traditional energy sources and is a promising direction for sustainable development.

Keywords: Wind turbine, vehicles, Arctic, energy regeneration, autonomy, environmental friendliness, renewable energy sources, drag, energy efficiency, sustainable development.

Регенерация энергии в транспортных средствах

Регенерация энергии, известная из автоспорта, используется в гражданских автомобилях для накопления энергии, выделяемой при торможении. Например, после одного торможения Bentley Continental GT может снабдить электричеством загородный дом на неделю.

Предложение вырабатывать энергию и во время движения является логичным продолжением этой темы.

Эффективная скорость ветра для работы ветрогенератора обычно составляет от 3 м/с до 25 м/с. Оптимальная скорость ветра для производства максимального количества энергии обычно находится в диапазоне от 11 м/с до 16 м/с. В переводе на километры в час нижний порог составляет 40 км/ч, а верхний порог — 90 км/ч. В то же время наиболее экономичная скорость для большинства седельных грузовиков обычно находится в диапазоне от 90 км/ч до 105 км/ч (Рисунок 1). Этот тип транспортного средства был выбран потому, что он находится практически всегда в непрерывном движении.

График наглядно демонстрирует, что скорость ветра для эффективной выработки электроэнергии совпадает с оптимальной скоростью движения грузовика. Поэтому такая система сможет сделать работу грузовика более эффективной.

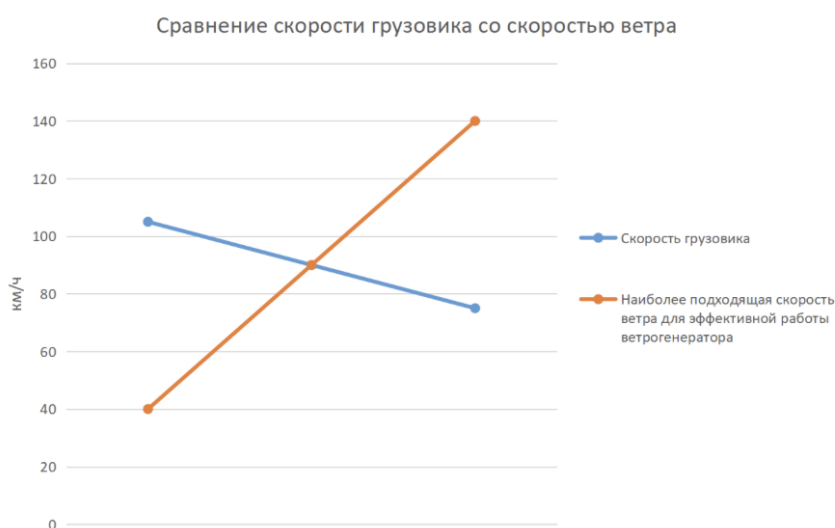


Рисунок 1. - График сравнения скорости седельного грузовика со скоростью ветра

Влияние угла атаки лопастей ветрогенератора

Также установка ветряного электрогенерирующего устройства на транспортное средство повлияет на его лобовое сопротивление. Для грузовиков коэффициент лобового сопротивления находится в диапазоне от 0.5 до 0.7. Коэффициент лобового сопротивления транспортного средства будет зависеть от угла атаки лопастей ветрогенератора. Выбрав среднюю скорость встречного ветра (97.5 км/ч), были изучены значения угла атаки лопастей для нахождения оптимального значения (Рисунок 2).



Рисунок 2. - Влияние угла атаки лопастей ветрогенератора на коэффициент лобового сопротивления грузовика

Угол атаки = 10 градусов:

Преимущества: Низкое сопротивление ветру.

Недостатки: Менее эффективен при более высоких скоростях.

Угол атаки = 12 градусов:

Преимущества: Обеспечивает увеличенную производительность, чем угол атаки в 10 градусов. Эффективен в широком диапазоне скоростей.

Недостатки: Может немного увеличить сопротивление ветру.

Угол атаки = 15 градусов:

Преимущества: Обеспечивает максимальную производительность ветрогенератора.

Недостатки: Высокое сопротивление ветру. Это приведёт к повышенному расходу топлива.

Из этих вариантов, при скорости в 97.5 км/ч, более оптимальным будет угол атаки в 12 градусов. Он обеспечит хорошую производительность ветряного электрогенерирующего устройства, не слишком увеличивая сопротивление ветру (0.55) и сохраняя достаточную эффективность движения грузовика.

Применение ветрогенераторов в Арктическом регионе

В Арктическом регионе, где высока автономность и необходимость в устойчивом энергоснабжении [2], ветрогенераторы находят своё применение. Проекты компании «РусГидро» в Мурманской области и внедрение ветрогенераторов в отдалённых районах Аляски (например, в деревне Коцебу) показывают положительные результаты [1].

Технологические аспекты интеграции ветрогенераторов в транспортные средства и условия их эксплуатации в Арктике [4] представляют собой вызовы для инженеров и экологов. Необходимость разработки специализированных решений для работы в экстремальных условиях становится актуальной задачей [3].

Эффективная работа ветрогенераторов в условиях Арктики также связана с особенностями местных ветровых условий и суровыми климатическими факторами. Например, исследования показывают, что ветрогенераторы могут эффективно работать при низких температурах и в условиях сильного ветра, что делает их идеальным и для арктических регионов [5]. Применение таких технологий в Арктике способствует развитию устойчивой

энергетики и уменьшению зависимости от традиционных источников энергии, что важно для экологического благополучия региона [6].

Заключение

Использование ветрогенераторов в транспортных средствах и в Арктическом регионе показывает положительные результаты. Дальнейшее развитие этой технологии может существенно улучшить энергоснабжение и экологическую устойчивость в данных областях. Привлечение внимания к возобновляемым источникам энергии, таким как ветрогенераторы, является важной задачей для устойчивого развития [7].

Статья публикуется по результатам проведения научно-исследовательской работы, проводимой в рамках конкурса грантов на выполнение научно-исследовательских работ обучающимися СПбГАСУ (ФГБОУ ВО «Санкт-Петербургский государственный архитектурно-строительный университет») в 2024 году.

Список литературы

1. Беляев, Л. С., Беляев, С. Л., Кустова, Е. А. Перспективы использования ветроэнергетических установок в Арктическом регионе // Энергетическая политика. 2019. №6. С. 44-49.
2. Гусев, С. Н., Иванов, А. А., Миронов, В. В. Ветроэнергетика в России: проблемы и пути решения // Электричество. 2020. №5. С. 34-41.
3. Петров, М. В., Смирнов, П. П. Возобновляемые источники энергии в Арктике: текущие достижения и перспективы развития // Арктика и Север. 2021. №41. С. 56-67.
4. Федоров, А. В., Лебедев, И. И. Технологические аспекты интеграции ветроэнергетических установок в транспортные средства // Вестник машиностроения. 2018. №9. С. 12-18.
5. Климов, Д. В., Тюрин, С. С. Опыт эксплуатации ветроэнергетических установок в условиях крайнего севера // Наука и техника в дорожной отрасли. 2021. №4. С. 98-105.
6. Павлов, Н. И., Соколов, Е. М. Возобновляемые источники энергии и их применение в транспортных системах // Энергетика. 2017. №3. С. 23-29.
7. Козлов, А. В., Михайлов, Ю. Н. Энергетическая эффективность ветрогенераторов в арктических условиях // Российский энергетический журнал. 2020.

References

1. Belyaev, L. S., Belyaev, S. L., Kustova, E. A. Prospects for the use of wind power plants in the Arctic region // Energy policy. 2019. No.6. pp. 44-49.
2. Gusev, S. N., Ivanov, A. A., Mironov, V. V. Wind energy in Russia: problems and solutions // Electricity. 2020. No.5. pp. 34-41.
3. Petrov, M. V., Smirnov, P. P. Renewable energy sources in the Arctic: current achievements and development prospects // Arctic and North. 2021. No. 41. pp. 56-67.
4. Fedorov, A.V., Lebedev, I. I. Technological aspects of the integration of wind power plants into vehicles // Bulletin of Mechanical Engineering. 2018. No.9. pp. 12-18.
5. Klimov, D. V., Tyurin, S. S. Experience of operation of wind power plants in the conditions of the Far North // Science and technology in the road industry. 2021. No.4. pp. 98-105.

6. Pavlov, N. I., Sokolov, E. M. Renewable energy sources and their application in transport systems // Energetika. 2017. No.3. pp. 23-29.
 7. Kozlov, A.V., Mikhailov, Yu. N. Energy efficiency of wind turbines in Arctic conditions // Russian Energy Journal. 2020.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 666.97

ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ ТЕРМООБРАБОТКИ БЕТОННЫХ И ЖЕЛЕЗОБЕТОННЫХ ИЗДЕЛИЙ

¹Кудабаев Р.Б., ²Сулейменов У.С.

ГУ ЮЖНО-КАЗАХСТАНСКИЙ УНИВЕРСИТЕТ ИМ. М. АУЕЗОВА, Шымкент, Казахстан (160012, Шымкент, Проспект Тауке хана, 5 к Д), e-mail: ¹kudabaev_81@mail.ru, ²ulanbator@inbox.ru

В статье приведены данные о применении комбинированного метода гелиотермообработки бетонных и железобетонных изделий, применением гелиоформ, гелиокамер со светопрозрачными, теплоизолирующими или пленкообразующими покрытиями и подвода дополнительно-дублирующих источников тепла. Проведены сравнительные эксперименты по оценке температуры в традиционной конструкций гелиокамеры (без теплоаккумулирующего материала) и конструкций гелиокамеры с теплоаккумулирующим материалом на основе парафинов. Установлено, что применение теплоаккумулирующих материалов в гелиокамере для термообработки бетонных изделий и конструкций дает возможность создать оптимальный (мягкий) режим термообработки при одновременной экономии энергоресурсов.

Ключевые слова: Бетон, гелиотермообработка, аккумулярование энергии, теплоаккумулярующий материал.

IMPROVING THE ENERGY EFFICIENCY OF HEAT TREATMENT OF CONCRETE AND REINFORCED CONCRETE PRODUCTS

Kudabaev R.B., Suleimenov U.S.

SU SOUTH KAZAKHSTAN UNIVERSITY. M. AUEZOVA, Shymkent, Kazakhstan (160012, Shymkent, Tauke Khan Avenue, 5 k D), e-mail: ¹kudabaev_81@mail.ru, ²ulanbator@inbox.ru

The article presents data on the use of a combined method of solar thermal treatment of concrete and reinforced concrete products, the use of solar molds, solar cells with translucent, heat-insulating or film-forming coatings and the supply of additional duplicating heat sources. Comparative experiments have been carried out to assess the temperature in traditional solar cell structures (without heat storage material) and solar cell structures with heat storage material based on paraffins. It has been established that the use of heat-accumulating materials in a solar cell for heat treatment of concrete products and structures makes it possible to create an optimal (mild) heat treatment regime while saving energy resources.

Keywords: Concrete, solar thermal treatment, energy storage, heat storage material.

Введение.

Одним из актуальных вопросов производства бетонных и железобетонных изделий является проблема повышения энергоэффективности. Анализ научной литературы показывает что в настоящее время при термообработке строительных изделия применяются такие методы как прямой нагрев, преобразование солнечной энергии в тепловую в низкопотенциальных энергетических установках, аккумулярование солнечной энергии в энергоемких материалах, концентрация плотности потока солнечной радиации, комбинированные методы, сочетающие применение традиционных теплоносителей с солнечной энергией [1-9]. Сравнительный

анализ уравнений теплового баланса и характера тепло- и массообмена на поверхности твердеющего бетона свидетельствует, что при всех методах ухода тепловое воздействие на бетон солнечной радиацией неизбежно. Применение для защиты и укрытия поверхности свежееуложенного бетона разнообразных материалов и жидкостей, имеющих различные оптические и теплотехнические свойства, позволяет в зависимости от требований по температуре нагрева создавать в условиях интенсивного притока солнечной радиации и высокой температуры окружающей среды оптимальные режимы его выдерживании. Однако количественно бетон получает больше лучистой энергии при укрытии светопрозрачными пленками, чем при уходе за ним с применением других материалов. Только под покрытием из полимерных пленок с образованием замкнутого пространства вокруг бетона проявляется принцип «парникового эффекта». Основная часть солнечной радиации, определяющая энергетический режим в гелиотехнических устройствах, находится в видимой и инфракрасных областях.

Наиболее интересным методом с точки зрения настоящего исследования является комбинированные методы гелиотермообработки бетонных и железобетонных изделий, которая предусматривает применение гелиоформ, гелиокамер со светопрозрачными, теплоизолирующими или пленкообразующими покрытиями и подвод дополнительно-дублирующих источников тепла [10,11].

Материалы и методы исследования.

В основу комбинированной гелиотермообработки положен принцип оптимального сочетания воздействия непосредственно на твердеющий бетон изделий солнечной радиации различной плотности потока с регулируемым подводом тепловой энергии от дополнительно-дублирующих источников при условии обеспечения суточного технологического цикла.

В гелиокамерах, работающих по принципу «горячего ящика», солнечная радиация преобразовывается в тепловую и аккумулируется в объеме камеры в пределах температур изотермического выдерживания бетона. В подобных гелиокамерах можно осуществлять пакетную технологию выдерживания изделий, а также заполнять их объем бетонными конструкциями различных геометрических размеров.

Температурный режим в камере определяется главным образом наличием в его объеме камеры тепловоспринимающего материала, его ориентацией по отношению к лучам солнца. Поглощая солнечную радиацию, тепловоспринимающий материал нагревается и становится генератором тепловой энергии: в камере солнечная энергия преобразуется в тепловую. При наличии тепловоспринимающего материала температура воздуха в камере повышается по сравнению с температурой наружного воздуха и может достигать до 80°C. Превышение температуры в камере в сравнении с температурой окружающей среды при адекватных условиях проведения эксперимента может составить более 50°C. Отсутствие тепловоспринимающего материала в объеме гелиокамер позволяет получить температуру в камере до 60°C. Поэтому, одним из условий получения в гелиокамере температур, близких к температуре изотермического выдерживания бетона, является наличие в объеме камеры тепловоспринимающего материала. Использование в качестве тепловоспринимающего материала теплоаккумулирующих материалов заметно изменяет тепло влажностной режим в камере.

Результаты и обсуждения.

На температурный режим в гелиокамере оказывают влияние также условия солнечной радиации на тепловоспринимающую поверхность, которая связана с ориентацией гелиокамеры на местности. По литературным данным [1] максимального значения температура воздуха в гелиокамере достигает при ориентации ее длинной осью юго-восточнее на 30° . Время достижения максимальной температуры приходится на 15-16 ч. Увеличение угла разворота длинной оси до 45° юго-восточной и юго-западной ориентации для раннего или более позднего падения солнечной радиации несколько снижают температуру воздуха в гелиокамере. Превышение температуры воздуха в гелиокамере в сравнении с температурой среды окружающего пространства при юго-западной, южной и юго-восточной ориентации на 30° составило $55-60^\circ\text{C}$, при увеличении угла поворота до 45° составило $40-45^\circ\text{C}$.

Таким образом, время максимального притока солнечной радиации при ориентации гелиокамер на 30° юго-восточнее и юго-западнее соответствовала большая температура в объеме гелиокамеры. Поэтому оптимальное значение угла разворота гелиокамеры юго-западной или юго-восточной ориентации принято 30° . Изделия в камере размещены наклонно для того, чтобы угол падения солнечных лучей, прошедших через светопрозрачное ограждение, на бетонную поверхность, должен был быть близким к 90° . При температуре наружного воздуха 35°C температура воздуха в установке достигала $70-80^\circ\text{C}$.

Для обоснования эффективности применения теплоаккумулирующих материалов в гелиокамерах для термообработки изделий и конструкций были проведены сравнительные эксперименты по оценке температуры в традиционной конструкции гелиокамеры (без теплоаккумулирующего материала) и конструкций гелиокамеры с теплоаккумулирующим материалом на основе парафинов. В качестве сравнения было оценено изменение влажности и температуры в камерах в течение суток.

Измерение температуры в гелиокамере производилось на уровне полок с бетонными изделиями (в середине камеры на высоте 0,9 м от дна камеры).

Результаты сравнения приведены в соответствии с Рисунком 1.

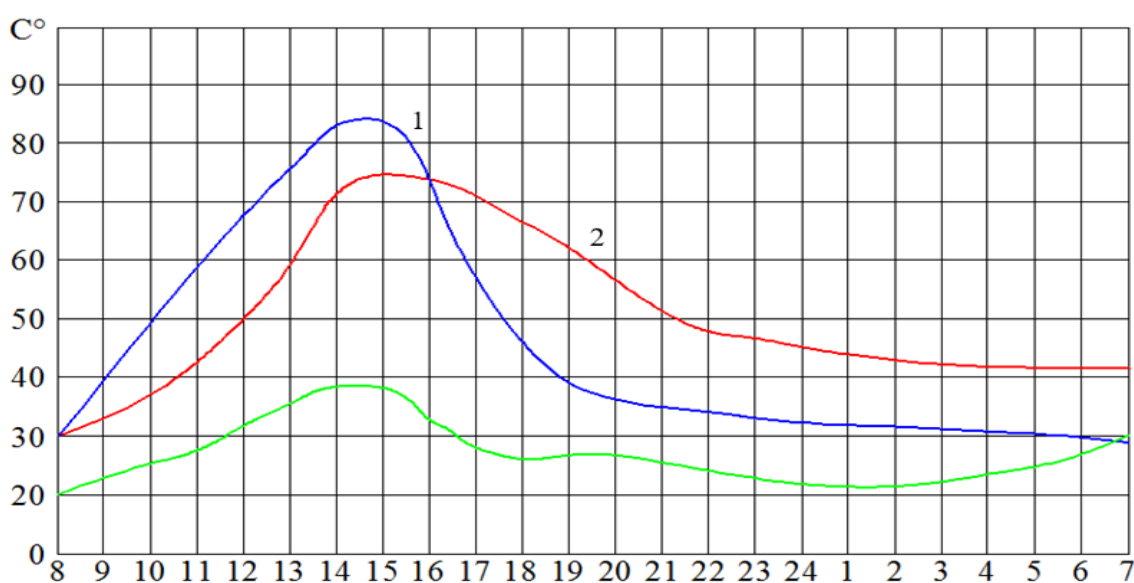


Рисунок 1 – Изменение температуры в гелиокамере в течение суток традиционным способом 2) с теплоаккумулирующим материалом

В соответствии с Рисунком 1 в камере с теплоаккумулирующим материалом из товарного парафина пик температуры дольше сохраняется в течение суток, а также в вечернее и ночное время температура в камере выше на 10-12°C по сравнению с камерой без теплоаккумулирующего материала.

Было установлено, что максимальное давление в традиционной гелиокамере составила примерно 0,9 атм., в камере с теплоаккумулирующим материалом она составила 1,2 атм., что на 30% выше.

Выводы. Результаты проведенных исследований показали, что применением теплоаккумулирующих материалов в гелиокамере для термообработки бетонных изделий и конструкций дает возможность создать оптимальный (мягкий) режим термообработки при одновременной экономии энергоресурсов.

Работа выполнена в соответствии с договором на выполнение научно-исследовательских работ в рамках государственного заказа от «20» октября 2022 года № 291/ЖГ-2-22-24 АР14972832 «Разработка энергосберегающей технологии термообработки бетонных изделий и конструкций использованием альтернативной солнечной энергии».

The work was carried out in accordance with the contract for the implementation of research work within the framework of the state order dated October 20, 2022 No 291/ZHG-2-22-24 AR14972832 "Development of an energy-saving technology for heat treatment of concrete products and structures using alternative solar energy".

Список литературы

1. Подгорнов, Н.И. Методы термообработки сборного и монолитного железобетона с использованием солнечной энергии [Текст]: дис. ... док. техн. наук: 05.02.22, 05.23.08 / Н.И. Подгорнов. – Москва, 2005. – 487 с.
2. Заседателев, И.Б. Гелиотермообработка сборного железобетона [Текст] / И.Б. Заседателев, Е.Н. Малинский, Е.С. Темкин. – Москва, Стройиздат, 1990.
3. Хашиев, О.А. Гибкая гелиотермообработка бетона на основе использования теплоаккумуляторов и дублирующих источников тепла [Текст]: дис. ... канд. техн. наук: 05.23.05 / О.А. Хашиев. – Ростов-на-Дону, 1995. – 168 с.
4. Орозбеков, М.О. Комбинированная гелиотермообработка сборного железобетона в условиях жаркого климата [Текст]: дис. ... док. техн. наук: 05.23.08 / М.О. Орозбеков. – ОШ, 1994. – 270 с.
5. Борбоев, А.М. Тепловая обработка изделий из тяжелого бетона в теплоаккумулирующих гелиокамерах [Текст]: дис. ... канд. техн. наук: 05.23.05 / А.М. Борбоев. – Москва, 1993.
6. Мирзаев, Ш.Р. Гелиотермообработка изделий из конструкционного теплоизоляционного керамзитобетона: дис. ... канд. техн. наук: 05.23.05 / Ш.Р. Мирзаев. – Москва, 1990.
7. Колчаров, А.К. Круглогодичная гелиотермообработка железобетонных изделий с применением предварительно разогретых смесей [Текст]: дис. ... канд. техн. наук: 05.23.05 / А.К. Колчаров. – Москва, 1994.
8. Заседателев И.Б., Малинский Е.Н., Темкин Е.С. Гелиообработка сборного железобетона, -М., Стройиздат, 1990, 171 с.

9. Земляков, Г.В. Исследование путей снижения затрат энергоресурсов в строительстве / Г.В. Земляков, С.П. Баранов, Е.И. Морозов // Вклад вузовской науки в развитие приоритетных направлений производственно-хозяйственной деятельности, разработку экономичных и экологически чистых технологий и прогрессивных методов обучения: материалы 54-й Междунар. науч.-техн. конф. в 10 ч. - Минск: БГПА, 2000. - Ч. 7. - С. 56.
10. Крылов Б.А., Аруова Л.Б. Комбинированный метод использования гелиотехнологии на полигонах // «Бетон и железобетон» - №12 - Москва, 1996 г.
11. Аруова Л.Б., Абдибаттаева М.М. Комбинированная гелиотермообработка в зимних условиях. В сб. 1 Всероссийской конференции, посвященной 100-летию Михайлова, НИИЖБ, Москва, 2001 г.

References

1. Podgornov, N.I. Metody termoobrabotki sbornogo i monolitnogo zhelezobetona s ispol'zovaniem solnechnoj energii [Tekst]: dis. ... dok. tekhn. nauk: 05.02.22, 05.23.08 / N.I. Podgornov. – Moskva, 2005. – 487 s.
2. Zasedatelev, I.B. Geliotermoobrabotka sbornogo zhelezobetona [Tekst] / I.B. Zasedatelev, E.N. Malinskij, E.S. Temkin. – Moskva, Strojizdat, 1990.
3. Hashiev, O.A. Gibkaya geliotermoobrabotka betona na osnove ispol'zovaniya teploakkumulyatorov i dubliruyushchih istochnikov tepla [Tekst]: dis. ... kand. tekhn. nauk: 05.23.05 / O.A. Hashiev. – Rostov-na-Donu, 1995. – 168 s.
4. Orozbekov, M.O. Kombinirovannaya geliotermoobrabotka sbornogo zhelezobetona v usloviyah zharkogo klimata [Tekst]: dis. ... dok. tekhn. nauk: 05.23.08 / M.O. Orozbekov. – OSh, 1994. – 270 s.
5. Borboev, A.M. Teplovaya obrabotka izdelij iz tyazhelogo betona v teploakkumuliruyushchih geliokamerah [Tekst]: dis. ... kand. tekhn. nauk: 05.23.05 / A.M. Borboev. – Moskva, 1993.
6. Mirzaev, Sh.R. Geliotermoobrabotka izdelij iz konstrukcionnogo teploizolyacionnogo keramzitobetona: dis. ... kand. tekhn. nauk: 05.23.05 / Sh.R. Mirzaev. – Moskva, 1990.
7. Kolcharoev, A.K. Kruglogodichnaya geliotermoobrabotka zhelezobetonnyh izdelij s primeneniem predvaritel'no razogretyh smesey [Tekst]: dis. ... kand. tekhn. nauk: 05.23.05 / A.K. Kolcharoev. – Moskva, 1994.
8. Zasedatelev I.B., Malinskij E.H., Temkin E.S. Geliotermoobrabotka sbornogo zhelezobetona, -M., Strojizdat, 1990, 171 s.
9. Zemlyakov, G.V. Issledovanie putej snizheniya zatrat energoresursov v stroitel'stve / G.V. Zemlyakov, S.P. Baranov, E.I. Morozov // Vklad vuzovskoj nauki v razvitie prioritetnyh napravlenij proizvodstvenno-hozyajstvennoj deyatel'nosti, razrabotku ekonomichnyh i ekologicheski chistyh tekhnologij i progressivnyh metodov obucheniya: materialy 54-j Mezhdunar. nauch.-tekhn. konf. v 10 ch. - Minsk: BGPA, 2000. - Ch. 7. - S. 56.
10. Krylov B.A., Aruova L.B. Kombinirovannyj metod ispol'zovaniya geliotekhnologii na poligonah // «Бетон и железобетон» - №12 - Москва, 1996 г.
11. Aruova L.B., Abdibattaeva M.M. Kombinirovannaya geliotermoobrabotka v zimnih usloviyah. V sb. 1 Vserossijskoj konferencii, posvyashchen noj 100-letiyu Mihajlova, NIIZhB, Moskva, 2001 g.



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 528.81

ВЫБОР ДАТЧИКОВ ДЛЯ ГИПЕРСПЕКТРАЛЬНЫХ СИСТЕМ

Ткачева Е.Г., ¹Калашников В.С.

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:
¹akm543@mail.ru

В статье рассматриваются ключевые компоненты и принципы работы гиперспектральных систем, включая блок оптики, дисперсионный элемент и детекторы. Описаны различные типы сенсоров, такие как PMT, CCD и CMOS, с акцентом на их особенности и области применения. Особое внимание уделено выбору подходящего сенсора в зависимости от требований к чувствительности, скорости и эффективности системы. В статье также анализируются преимущества и ограничения каждого типа сенсора в зависимости от условий эксплуатации и специфики измерений. Подчеркнута важность баланса между производительностью и экономической эффективностью при выборе сенсора для гиперспектральных систем.

Ключевые слова: Гиперспектральные системы, оптические сенсоры, дисперсионные элементы, фотоумножители, приборы с зарядовой связью, комплементарные металл-оксид-полупроводниковые структуры.

SENSOR SELECTION FOR HYPERSPECTRAL SYSTEMS

Tkacheva E.G., ¹Kalashnikov V.S.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY),
Moscow, Russia, (105005, Moscow, 2nd Baumannskaya ul, 5 bld. 1), e-mail: ¹akm543@mail.ru

The article discusses the key components and principles of hyperspectral systems, including the optics module, dispersive element, and detectors. Various sensor types, such as PMT, CCD, and CMOS, are described with a focus on their characteristics and applications. Special attention is given to selecting the appropriate sensor based on the system's requirements for sensitivity, speed, and efficiency. The article also analyzes the advantages and limitations of each sensor type based on operating conditions and measurement specifics. The importance of balancing performance and cost-effectiveness when selecting a sensor for hyperspectral systems is emphasized.

Keywords: Hyperspectral systems, optical sensors, dispersive elements, photomultiplier tubes, charge-coupled device, complementary metal-oxide-semiconductor.

Гиперспектральный датчик (hyperspectral sensor, HSS) представляет собой оптико-электронную многоканальную систему, предназначенную для сбора информации в виде набора изображений, представляющих разные диапазоны электромагнитного спектра. Эти изображения затем объединяются в куб гиперспектральных данных, при этом каждый пиксель такого изображения содержит информацию о спектре (Рисунок 1).

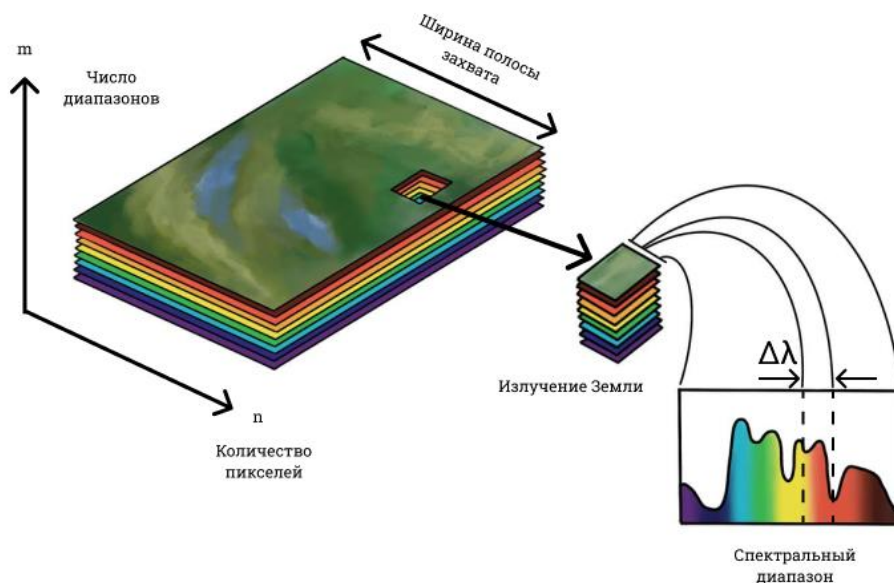


Рисунок 1. - Концепция гиперкуба, состоящего из отдельных изображений, записанных в «m» спектральных диапазонах

Работа гиперспектральной системы может быть понята лучше, если разделить ее на основные блоки, такие как блок оптики, дисперсионный элемент, детекторы, а также системы управления и обработки данных. Рассмотрим подробнее, что происходит в каждом из этих блоков (Рисунок 2.).

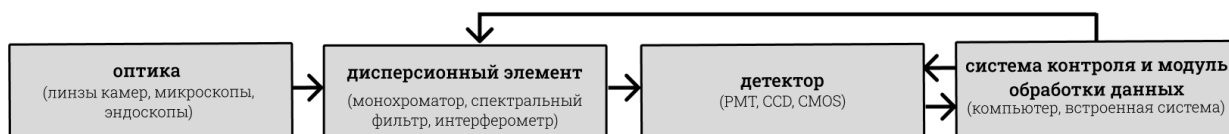


Рисунок 2. Блок-схема гиперспектральной системы отображения

Блок оптики в гиперспектральных системах отвечает за сбор входного светового сигнала от наблюдаемого объекта. [1] Это начальный этап, где свет, отраженный или излученный объектом, фокусируется и направляется на дисперсионный элемент. Используются различные типы оптических систем, включая линзы и зеркала, чтобы эффективно собрать и передать свет с минимальными потерями качества и искажениями.

Дисперсионный элемент является ключевой частью гиперспектральной системы, его задача – разделить входящий световой поток на отдельные спектральные компоненты (полосы). Такое разделение возможно благодаря использованию дифракционных решеток, призм или других оптических устройств, которые по-разному преломляют свет различных длин волн. [2]

Детекторный блок предназначен для преобразования разделенного спектрального сигнала в электронные данные. Детекторы захватывают световые сигналы в различных спектральных диапазонах и преобразуют их в цифровую форму для дальнейшей обработки. Ключевым моментом является высокая чувствительность и точность детекторов,

позволяющая эффективно регистрировать информацию даже при низком уровне светового сигнала.

Последний этап работы гиперспектральной системы включает в себя управление процессом сбора данных и их последующую обработку. Системы управления координируют работу всех элементов устройства, обеспечивая оптимальные условия для получения качественных данных. [3] Мощное программное обеспечение позволяет эффективно обрабатывать большие объемы информации, выделять интересующие признаки и проводить комплексный анализ с целью получения ценных сведений о наблюдаемом объекте.

Существуют различные типы гиперспектральных сенсоров, среди которых основными являются: фотоэлектронные умножители или фотоумножители (photomultiplier tube, PMT), приборы с зарядовой связью или ПЗС-матрицы, (charge-coupled device, CCD), и комплементарные металл-оксид-полупроводниковые структуры (complementary metal-oxide-semiconductor, CMOS). Рассмотрим, как каждый из этих сенсоров обрабатывает поступающую на них энергию.

Фотоумножители

PMT – это высокочувствительные детекторы, которые могут обнаруживать слабые световые сигналы, даже отдельные фотоны. [4] Они работают путем преобразования светового сигнала в электронный сигнал через серию фотокатодов и динодов, что позволяет усиливать сигнал в миллионы раз. PMT особенно полезны в приложениях, где требуется высокая чувствительность и быстрая временная реакция, однако их использование ограничено низкой эффективностью квантового выхода в некоторых спектральных диапазонах и высокой стоимостью.

ПЗС – матрицы

CCD – это тип фоточувствительных микросхем, который преобразует и накапливает поступающий световой сигнал в видимом, ближнем инфракрасном и ультрафиолетовом диапазонах в электрический заряд в каждом из своих пикселей. Затем эти заряды последовательно перемещаются через схему сенсора и преобразуются в электрический сигнал, который может быть усилен и обработан. CCD обеспечивают высокое качество изображения с низким уровнем шума, но требуют значительных энергозатрат и более сложных систем охлаждения для поддержания оптимальной работы.

Комплементарные металл-оксид-полупроводниковые структуры

CMOS работают по принципу, схожему с CCD, но используют другую технологию обработки сигнала. В CMOS каждый пиксель обрабатывает свои заряды независимо, что позволяет проводить аналого-цифровое преобразование непосредственно на чипе. Это приводит к более высокой скорости считывания и меньшему энергопотреблению по сравнению с CCD. CMOS сенсоры стали более популярными из-за их стоимости, универсальности и эффективности, хотя они могут уступать CCD в качестве изображения и чувствительности при некоторых условиях. Однако CMOS сенсоры более восприимчивы к шуму и темновому току по сравнению с CCD, что связано с использованием встроенной микросхемы для передачи и усиления сигналов. Это приводит к снижению динамического диапазона и чувствительности. Темновой ток, который зависит от температуры, является

распространенным источником шума в показаниях сенсора и требует учета при калибровке для выполнения корректных измерений.[5]

Выбор между PMT, CCD и CMOS сенсорами зависит от специфических требований, включая чувствительность, скорость, диапазон детектирования, стоимость и физические размеры. Для гиперспектральных систем выбирают тип датчика в зависимости от целей измерения и условий эксплуатации, стремясь достичь наилучшего баланса между высокой производительностью и экономической эффективностью.

Список литературы

1. Сутырина Е. Н. Дистанционное зондирование земли: учеб. пособие – Иркутск : Изд-во ИГУ, 2013. – 165 с.
2. Гиперспектральная визуализация. Что это и где применяется? // lenlasers.ru URL: <https://lenlasers.ru/novosti-i-stati/giperspektralnaya-vizualizatsiya-cto-eto-i-gde-primenyaetsya/> (дата обращения: 24.09.2024).
3. Гиперспектральная съемка // ИННОТЕР URL: <https://innoter.com/articles/giperspektralnaya-semka/> (дата обращения: 30.09.2024).
4. Hyperspectral Imaging for Clinical Applications // SpringerLink URL: <https://link.springer.com/article/10.1007/s13206-021-00041-0#Sec15> (дата обращения: 01.10.2024).
5. Требования к датчикам и камерам для гиперспектральной съемки // gisproxima.ru URL: https://gisproxima.ru/trebovaniya_k_datchikam (дата обращения: 04.10.2024).

References

1. Sutyryna E. N. Remote sensing of the Earth: studies. the manual – Irkutsk : Publishing House of the ISU, 2013. – 165 p.
 2. Hyperspectral visualization. What is it and where is it applied? // lenlasers.ru URL: [https://lenlasers.ru/novosti-i-stati/giperspektralnaya-vizualizatsiya-cto-eto-i-gde-primenyaetsya /](https://lenlasers.ru/novosti-i-stati/giperspektralnaya-vizualizatsiya-cto-eto-i-gde-primenyaetsya/) (date of access: 09/24/2024).
 3. Hyperspectral photography // INNOTHER URL: [https://innoter.com/articles/giperspektralnaya-semka /](https://innoter.com/articles/giperspektralnaya-semka/) (date of access: 30.09.2024).
 4. Hyperspectral Imaging for Clinical Applications // SpringerLink URL: <https://link.springer.com/article/10.1007/s13206-021-00041-0#Sec15> (date of reference: 01.10.2024).
 5. Requirements for sensors and cameras for hyperspectral photography // gisproxima.ru URL: https://gisproxima.ru/trebovaniya_k_datchikam (date of application: 04.10.2024).
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 519.252

МНОГОКРИТЕРИАЛЬНАЯ ОПТИМИЗАЦИЯ ПАРАМЕТРОВ МОСТИКА ДЛЯ ПРЫЖКОВ В БАССЕЙН

¹Калашников В.С., Ткачева Е.Г.

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:
¹akm543@mail.ru

В статье рассматривается как найти оптимальные длину и толщину доски, которая будет выполнять функцию мостика для прыжков в бассейн, за счет многокритериальной оптимизации размерных параметров. В качестве условия имеем общедоступный городской бассейн, в котором планируется установить мостик (деревянную доску) в форме параллелепипеда, длина которого колеблется от 225 до 275 сантиметров. Материал доски – дуб. В зависимости от характера действующего усилия максимальное допустимое напряжение для данного типа древесины колеблется от 4 до 12 МПа. Максимальная нагрузка на доску равняется 1500 Н.

Ключевые слова: Многокритериальная оптимизация, ANSYS Workbench, ANSYS DesignXplorer, Метод DOE, поверхность отклика, алгоритм оптимизации MOGA.

MULTICRITERIA OPTIMIZATION OF PARAMETERS OF A POOL DIVING BRIDGE

¹Kalashnikov V.S., Tkacheva E.G.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY),
Moscow, Russia, (105005, Moscow, 2nd Baumanskaya ul, 5 bld. 1), e-mail: ¹akm543@mail.ru

The article discusses how to find the optimal length and thickness of a board that will serve as a diving bridge into a pool, using multi-criteria optimization of dimensional parameters. The condition is a public city pool, in which it is planned to install a bridge (wooden board) in the form of a parallelepiped, the length of which varies from 225 to 275 centimeters. The board material is oak. Depending on the nature of the acting force, the maximum allowable stress for this type of wood varies from 4 to 12 MPa. The maximum load on the board is 1500 N.

Keywords: Multicriteria optimization, ANSYS Workbench, ANSYS DesignX-plorer, DOE method, response surface, MOGA optimization algorithm.

Допущения компьютерной модели

Для создания модели, необходимо учесть следующие допущения:

- в расчетах не будем учитывать влажность, которая должна влиять на максимальное допустимое напряжение;
- дополнительные силовые нагрузки, действующие на доску при многократных прыжках перед главным прыжком в воду и прыжок с разбега;
- деструктивно действующие на деталь параметры при длительной эксплуатации, тоже не будем учитывать с целью упрощения задачи;
- будем считать, что небольшая стойка у бассейна точно выдержит конструкцию.

При помощи модуля *ANSYS DesignXplorer* планируется подобрать оптимальные длину и толщину доски с учетом требований к мере деформации при максимальной нагрузке, максимальным допустимым напряжениям и массе доски. В приоритет поставим легкость конструкции и уменьшение деформаций. В ходе работы необходимо построить модель деревянной доски, приложить к ней силу, провести расчёт модели, использовать алгоритмы оптимизации.

Теоретическая часть

Мостики для прыжков в бассейн бывают различных типов, но в данной работе мостик будет рассматриваться, как трамплин или доска для прыжков в воду. Данная конструкция имеет гибкую площадь для ныряния и соответственно пружинит под собственным весом спортсмена, тем самым давая ему наибольшую амплитуду для задуманного прыжка.[1]

При проектировании сложных конструкций одной из актуальных задач является оптимизация ее элементов. В расчетной среде *ANSYS Workbench* начиная с версии 7.0 присутствует специализированный модуль для решения задач оптимизации — *ANSYS DesignXplorer*.

Важно собрать достаточно информации о текущем варианте конструкции, чтобы ответить на вопросы «что-если» и оценить влияние переменных на характеристики изделия. При этом, основываясь на точной информации, можно принять правильные решения, даже в случае неожиданного изменения конструктивных ограничений. [2] Модуль *ANSYS DesignXplorer* описывает взаимосвязи между параметрами конструкции и характеристиками изделия при помощи метода планирования эксперимента (DOE), объединенного с поверхностями отклика. Метод DOE и поверхности отклика предоставляют всю информацию, которая позволяет в полной мере реализовать преимущества концепции «Проектирование изделий на основе инженерных расчетов». Когда известна зависимость производительности от конструкционных переменных, то легко понять и определить все требуемые изменения, которые нужно внести, чтобы конструкция соответствовала предъявляемым требованиям. После создания поверхностей отклика можно легко обмениваться информацией в удобном для понимания виде: кривые, поверхности, чувствительности и т.д.[3]

ANSYS DesignXplorer содержит ведущие в отрасли алгоритмы, которые анализируют таблицу проектных режимов для создания поверхности отклика. Поверхность отклика может быть использована для мгновенного предсказания производительности устройства без проведения дополнительных вычислений. Эта мета-модель пониженного порядка применяется для исследований чувствительности, оптимизации и 6-сигма расчетов.

Практическая часть

Toolbox → Analysis Systems → Static Structural → зажав правой кнопкой мыши, перетаскиваем в область Project Schematic.

Static Structural → Geometry.

Создание геометрической модели

Открываем в Geometry редактор моделей Design Modeler и начинаем строить 3D-модель. Масштаб для создания модели поставим в сантиметрах.

Создаём скетч в плоскости XY.

Sketching → Draw → Rectangle, нарисуем прямоугольное сечение доски.

Sketching → Dimensions → General, зададим ширину (80 см) и толщину (8 см).

При помощи инструмента Extrude зададим длину доски (250 см). Получаем простейшую геометрическую деталь (Рисунок 1).

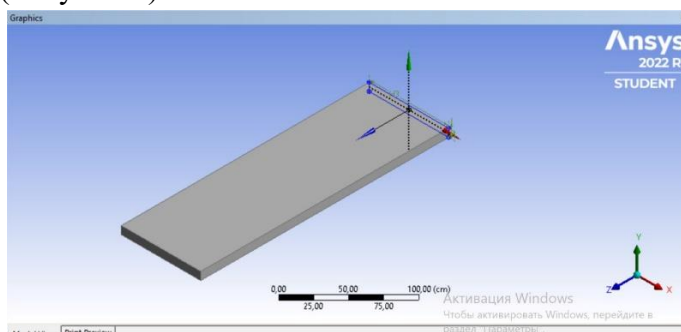


Рисунок 1 – Построение геометрической детали

Добавим длину и толщину в перечень регулируемых параметров, нажав на пустую область слева от наименования переменной, тем самым иницируя появление объекта Parameter Set в Project Schematic.[4]

| Parameter Editor | | | | |
|--|-----------|--------|--------|---------|
| | Name | Value | Type | Comment |
| ✓ | length | 250 cm | Length | |
| ✓ | thickness | 8 cm | Length | |
| | | | | |
| | | | | |
| | | | | |
| Design Parameters Parameter/Dimension Assignments | | | | |

Рисунок 2 – Параметры

Расчет в Mechanical

Возвращаемся в Project Schematic: Project Schematic → Static Structural → Model.
В качестве материала была выбрана древесина Wood, Oak (Рисунок 3).

| | |
|---|-------------------------------------|
| Wood, Oak | |
| Oak (quercus spp.) (quercus spp.), longitudinal direction (L) | |
| Data compiled by the Granta Design team at ANSYS, incorporating various sources including JAHM and MagWeb. ANSYS Inc. provides no warranty for this data. | |
| Density | 935,70 kg/m ³ |
| Structural | |
| Isotropic Elasticity | |
| Derive from | Young's Modulus and Poisson's Ratio |
| Young's Modulus | 2,278e+10 Pa |
| Poisson's Ratio | 0,37420 |
| Bulk Modulus | 3,018e+10 Pa |
| Shear Modulus | 8,2885e+09 Pa |
| Isotropic Secant Coefficient of Thermal Expansion | 4,69e-06 1/°C |
| Tensile Ultimate Strength | 1,467e+08 Pa |
| Tensile Yield Strength | 4,776e+07 Pa |
| Thermal | |
| Isotropic Thermal Conductivity | 0,45280 W/m·°C |

Рисунок 3 – Материал Wood, Oak

Outline → Mesh → Generate Mesh, генерируем разбиения.

Outline → Static Structural → Insert → Fixed Support, закрепим торец доски.

Outline → Static Structural → Insert → Force, приложим силу 1500 Н относительно оси Y
ко всей перекладине (значение силы взято из постановки задачи) (Рисунок 4).

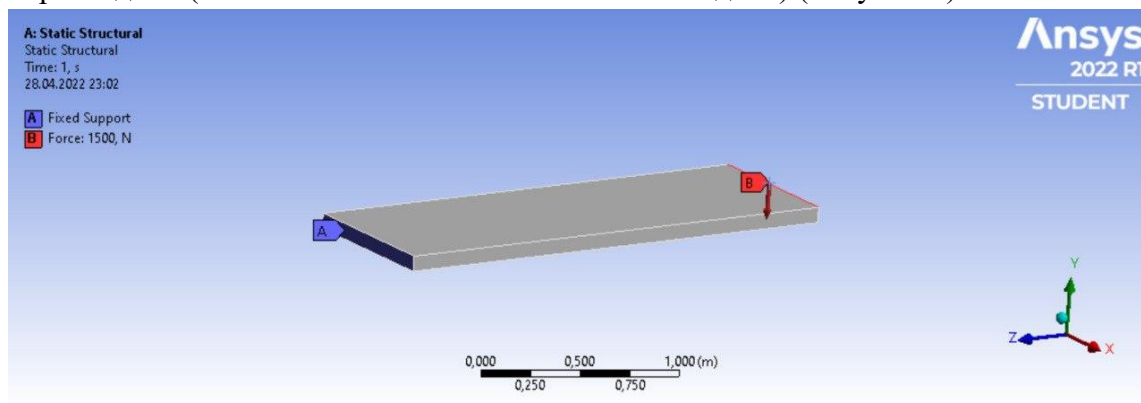


Рисунок 4 – Закреплённый торец и приложенная сила

Outline → Static Structural → Solution → Insert → Total Deformation, добавим измерение на деформацию.

Outline → Static Structural → Solution → Insert → Equivalent Stress, добавим измерение на эквивалентные напряжение, использующиеся для определения предела прочности материала (Рисунок 5-6).

Произведем анализ модели:

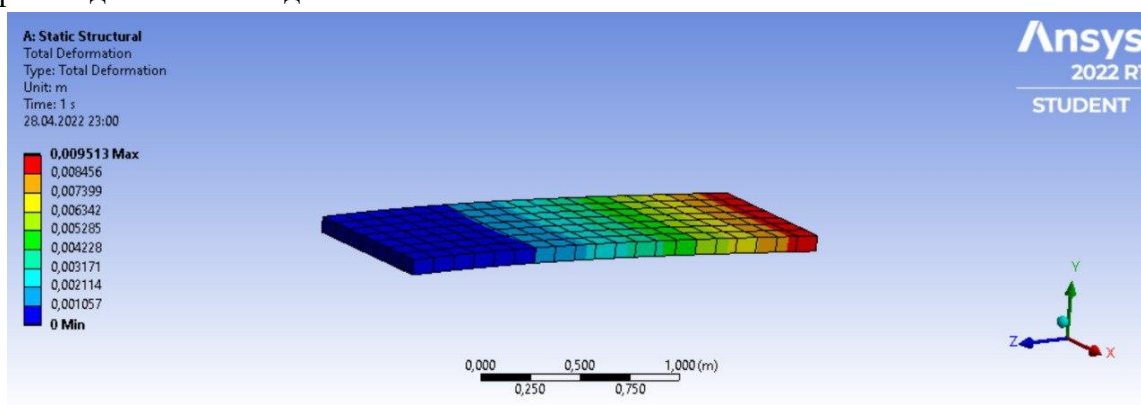


Рисунок 5 – Расчёт измерений на *Total Deformation*

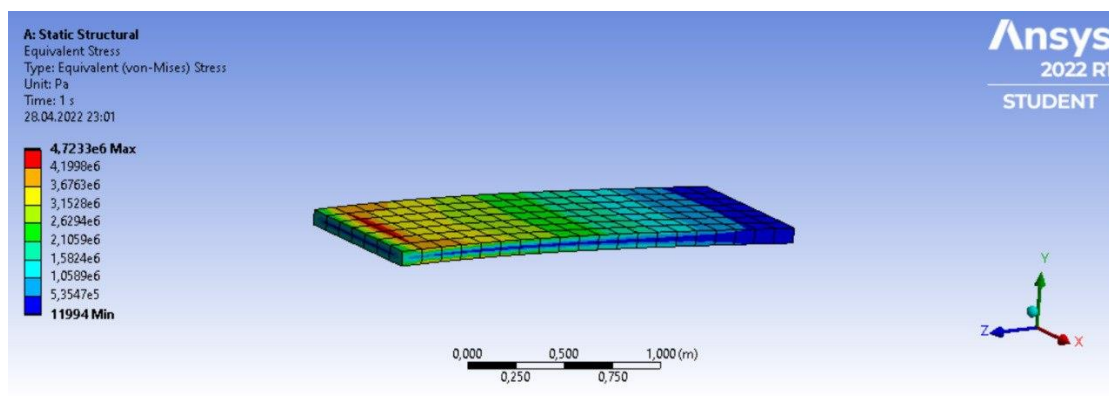


Рисунок 6 – Расчёт измерений на *Equivalent Stress*

Получили максимальную деформацию около 10 мм и максимальное напряжение на нагрузку около 4,72 МПа.

Массу модели, максимальную деформацию и максимальное напряжение обозначим как выходные параметры для будущей многокритериальной оптимизации.[5]

Многокритериальная оптимизация с модулем *DesignXplorer*

Toolbox → Design Exploration → Response Surface Optimization, зажав правой кнопкой мыши, перетаскиваем в область Project Schematic, соединяя с Parameter Set (Рисунок 7).

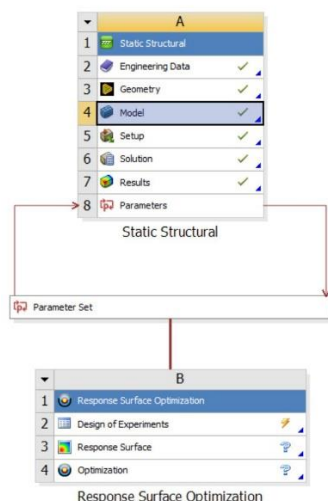


Рисунок 7 – Project Schematic после добавления модуля *DesignXplorer*

Project Schematic → Response Surface Optimization → Design of Experiments.

Зададим область определения входных параметров: пусть, согласно постановке задачи, длина доски колеблется от 225 до 275 см, а толщина сечения соответственно может лежать в диапазоне от 7,2 до 8,8 см.

По области определения при помощи стандартного алгоритма Design of Experiments → Central Composite Design составим набор опорных точек, при этом автоматически произведется расчёт выходных параметров (Рисунок 8).

| Table of Schematic B2: Design of Experiments (Central Composite Design : Auto Defined) | | | | | | |
|--|--------|------------------|---------------------|------------------------------------|-------------------------------------|-------------------------|
| | A | B | C | D | E | F |
| 1 | Name | P1 - length (cm) | P2 - thickness (cm) | P3 - Total Deformation Maximum (m) | P4 - Equivalent Stress Maximum (Pa) | P5 - Geometry Mass (kg) |
| 2 | 1 DP | 250 | 8 | 0,009513 | 4,723E+06 | 149,71 |
| 3 | 2 | 225 | 8 | 0,0069067 | 4,2528E+06 | 134,74 |
| 4 | 3 | 275 | 8 | 0,012698 | 5,1951E+06 | 164,68 |
| 5 | 4 | 250 | 7,2 | 0,013037 | 5,8327E+06 | 134,74 |
| 6 | 5 | 250 | 8,8 | 0,0071541 | 3,9019E+06 | 164,68 |
| 7 | 6 | 225 | 7,2 | 0,0094643 | 5,2517E+06 | 121,27 |
| 8 | 7 | 275 | 7,2 | 0,017404 | 6,4155E+06 | 148,21 |
| 9 | 8 | 225 | 8,8 | 0,0051946 | 3,5133E+06 | 148,21 |
| 10 | 9 | 275 | 8,8 | 0,0095488 | 4,2916E+06 | 181,15 |

Рисунок 8 – Таблица с опорными точками

Можно заметить, что среди опорных точек встречаются крайние случаи, в которых напряжения превышают допустимые пределы, поэтому для поиска оптимального решения

необходимо использовать поверхность отклика Response Surface, построенную на основе данных опорных точек.

Project Schematic → Response Surface Optimization → Response Surface

Выбираем алгоритм построения поверхности отклика – Standard Response Surface.

Также осуществим генерацию 3-х верификационных точек – точек, максимально удаленных от опорных.

Сгенерированная поверхность отклика позволяет проанализировать зависимость любого выходного параметра от входных значений длины и толщины (Рисунки 9-11).

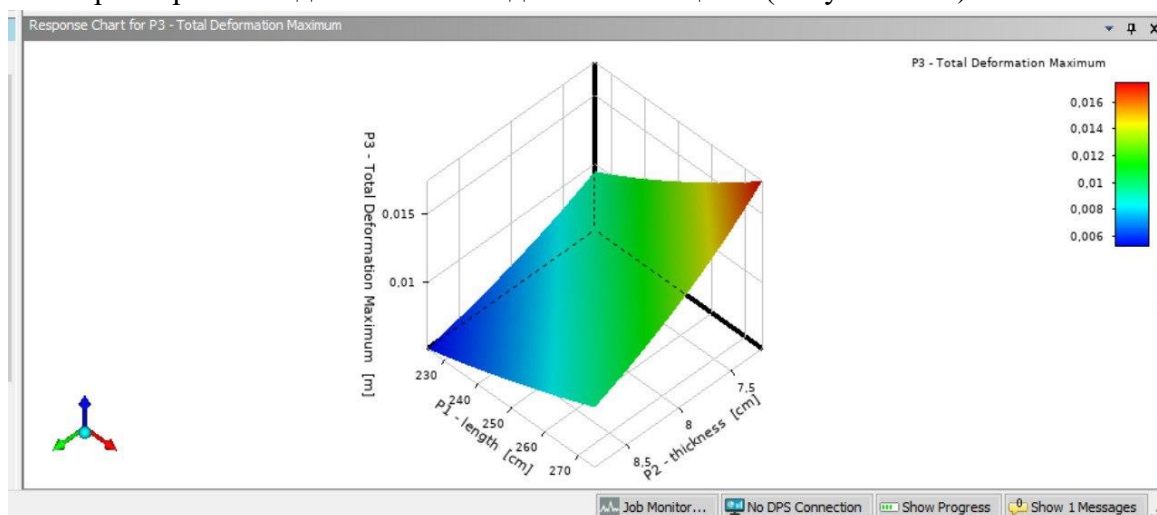


Рисунок 9 – Зависимость максимальной деформации от входных параметров

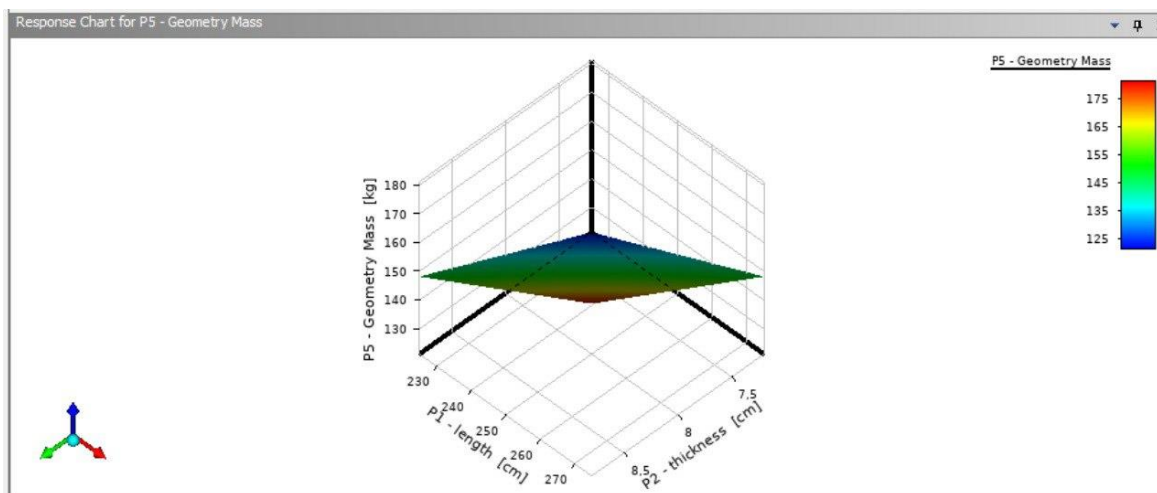


Рисунок 10 – Зависимость массы конструкции от входных параметров

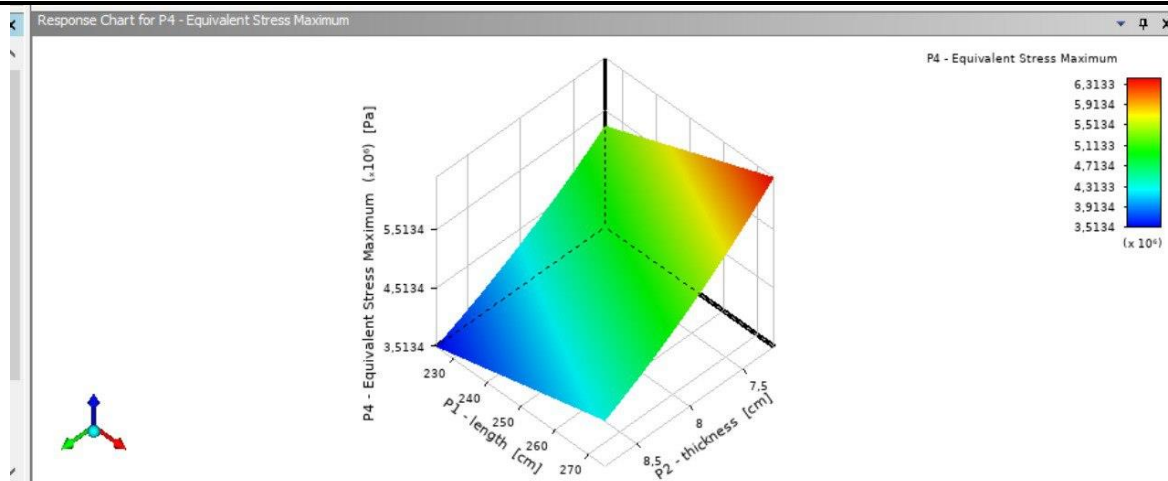


Рисунок 11 – Зависимость максимального напряжения от входных параметров

Также можно проанализировать, в какой степени влияет каждый отдельный входной параметр на величину выходного в разделе Local Sensitivity (Рисунок 12). Можно убедиться, что толщина сечения (– 61,655%) сильнее влияет на максимальное напряжение, чем длина перекладины (33,781%), а относительно максимальной деформации толщина сечения (– 49,753%) и длина (47,925%) уже более соразмерны по влиянию на конечный результат.

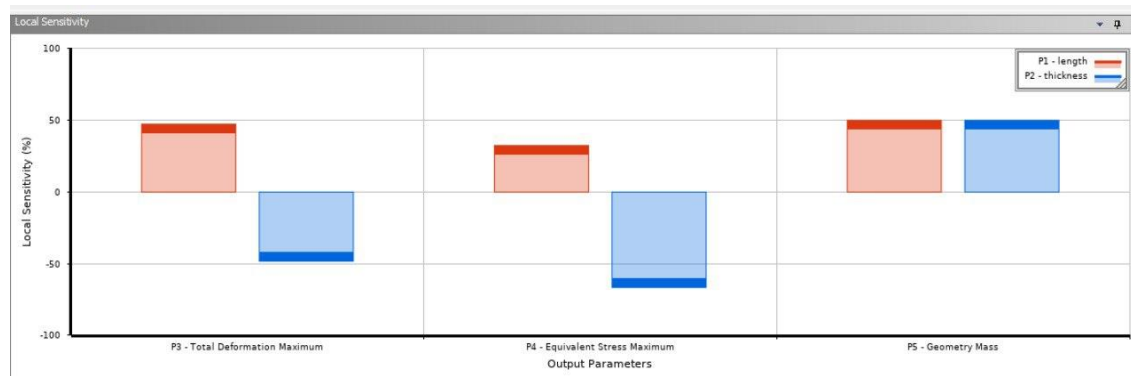


Рисунок 12 – Результат *Local Sensitivity*

Полученные данные уже позволяют вычислить оптимальные размеры конструкции, однако, встроенные в ANSYS DesignXplorer алгоритмы оптимизации дают возможность автоматически подобрать наиболее выгодные параметры с учетом того, какие из них являются для нас более приоритетными.

Project Schematic → Response Surface Optimization → Optimization

В разделе Objectives and Constraints у нас есть возможность выбрать, к чему должен стремиться каждый из параметров (Рисунок 13).

Согласно поставленной задаче, задаём следующие направления оптимизации и их приоритеты (Рисунок 14):

- Минимизация деформаций, приоритет высокий
- Минимизация массы, приоритет стандартный
- Максимальное допустимое напряжение: 5 МПа

| Table of Schematic B4: Optimization | | | | | | | | | |
|-------------------------------------|----------------|--------------------------------|--------------|--------|-----------|-----------------------|-------------|-------------|-----------|
| | A | B | C | D | E | F | G | H | I |
| 1 | Name | Parameter | Objective | | | Constraint | | | |
| 2 | | | Type | Target | Tolerance | Type | Lower Bound | Upper Bound | Tolerance |
| 3 | P1 | P1 - length | No Objective | | | No Constraint | | | |
| 4 | P2 | P2 - thickness | No Objective | | | No Constraint | | | |
| 5 | Minimize P3 | P3 - Total Deformation Maximum | Minimize | 0 | | No Constraint | | | |
| 6 | P4 <= 5E+06 Pa | P4 - Equivalent Stress Maximum | No Objective | | | Values <= Upper Bound | | 5E+06 | 0,001 |
| 7 | Minimize P5 | P5 - Geometry Mass | Minimize | 0 | | No Constraint | | | |
| * | | | | | | | | | |

Рисунок 13 – Таблица *Objectives and Constraints*

| Table of Schematic B4: Optimization | | | | | | | | | |
|-------------------------------------|---------------------|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G | H | I |
| 1 | Optimization Study | | | | | | | | |
| 2 | Minimize P3 | Goal, Minimize P3 (Default importance) | | | | | | | |
| 3 | Minimize P5 | Goal, Minimize P5 (Default importance) | | | | | | | |
| 4 | P4 <= 5E+06 Pa | Strict Constraint, P4 values less than or equals to 5E+06 Pa (Default importance) | | | | | | | |
| 5 | Optimization Method | | | | | | | | |
| 6 | MOGA | The MOGA method (Multi-Objective Genetic Algorithm) is a variant of the popular NSGA-II (Non-dominated Sorted Genetic Algorithm-II) based on controlled elitism concepts. It supports multiple objectives and constraints and aims at finding the global optimum. | | | | | | | |
| 7 | Configuration | Generate 100 samples initially, 100 samples per iteration and find 3 candidates in a maximum of 20 iterations. | | | | | | | |
| 8 | Status | | | | | | | | |

Рисунок 14 – Направление оптимизации и приоритеты

Автоматически был выбран алгоритм оптимизации MOGA – многоцелевой генетический алгоритм (Рисунок 15).

Запускаем алгоритм оптимизации:

| 9 | Candidate Points | | | |
|----|-------------------------------------|-------------------|-------------------|-------------------|
| 10 | | Candidate Point 1 | Candidate Point 2 | Candidate Point 3 |
| 11 | P1 - length (cm) | 225,7 | 225,67 | 225,71 |
| 12 | P2 - thickness (cm) | 8,2867 | 8,2814 | 8,2789 |
| 13 | P3 - Total Deformation Maximum (m) | ★ 0,0062748 | ★ 0,0062848 | ★ 0,0062933 |
| 14 | P4 - Equivalent Stress Maximum (Pa) | ★★ 3,9731E+06 | ★★ 3,9778E+06 | ★★ 3,9808E+06 |
| 15 | P5 - Geometry Mass (kg) | ✖ 140 | ✖ 139,9 | ✖ 139,88 |

Рисунок 15 – Результат оптимизации

Таким образом, были подобраны оптимальные характеристики доски:

- Длина доски – 225,7 см
- Толщина доски – 8,2867 см

Минимизация массы позволила сократить значение до 140 кг.

ANSYS предоставляет трехзвездочную систему для оценки соответствия поверхности отклика контрольным точкам. По результатам оптимизации видно, что значение массы отклоняется от поверхности отклика. Это можно объяснить небольшим размером выборки, использованной для построения поверхности.

Модуль оптимизации также дает возможность детальное изучение результатов оптимизации при помощи диаграммы Парето. Из полученной диаграммы можно оценить, потенциал конструкции.

Также можно получить графическое отображение всех сгенерированных samples, изучить глобальную чувствительность выходных параметров к входным.

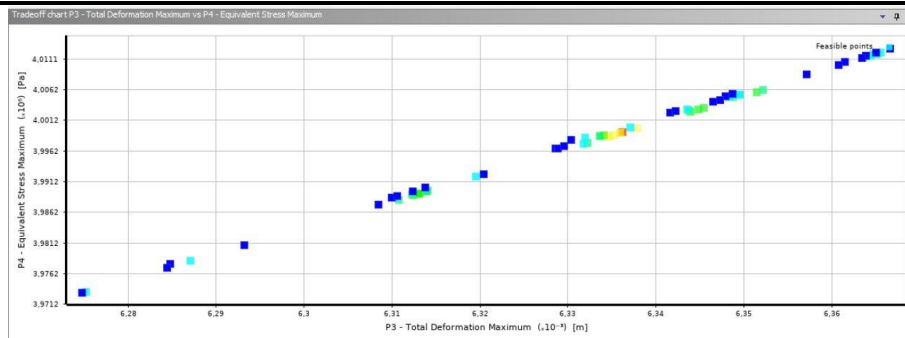


Рисунок 16 – Диаграмма Парето

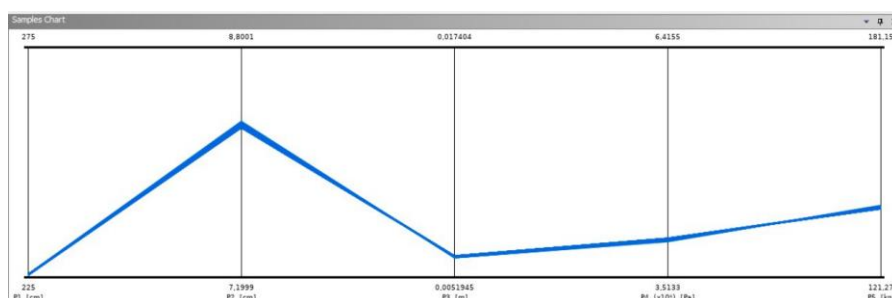


Рисунок 17 – *Samples Chart*

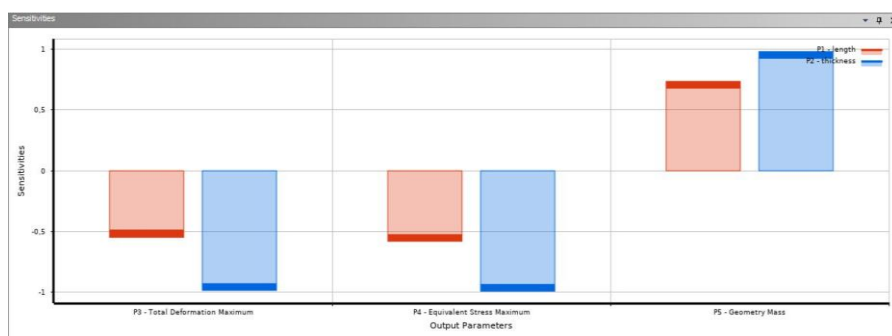


Рисунок 18 – Итоговая чувствительность

Выводы

Были найдены оптимальные решения поставленной задачи с учетом уровней приоритетности отдельных характеристик. Несмотря на то, что минимизация массы и деформаций для одного и того же материала – конкурирующие требования, оптимизирующий модуль позволил найти наиболее подходящее решение, а также избежать ручных вычислений и сэкономить достаточное количество времени при решении поставленной задачи.

Список литературы

1. Решение задач механики сплошной среды в программном комплексе ANSYS: метод. указания / М.В. Мурашов. С.Д. Панин. — М.: Издательство: г. Москва, МГТУ им. Н.Э. Баумана, 2009. — 40 с.: ил.
2. Оптимизация конструкций ANSYS DesignXplorer – Текст: электронный // ansysadvantage.ru: [сайт]. [URL: <https://www.ansysadvantage.ru/design-optimization-ansys-designxplorer>] (дата обращения: 13.10.2024)

3. ANSYS Parametric Design Language Guide – Текст: электронный // www.mm.bme.hu: [сайт]. URL: https://www.mm.bme.hu/~gyebro/files/fea/ansys/ans_apdl.pdf (дата обращения: 10.10.2024)
4. Мостик для бассейна – Текст: электронный // [URL: <http://www.bolshoyvopros.ru/questions/3757677-kak-nazyvaetsja-shtuka-s-kotoroj-prygajut-v-bassejn.html>] (дата обращения: 11.10.2024)
5. Основные сведения о программном комплексе ANSYS. Геометрическое моделирование / Е.А. Солдусова – Издательство: г. Самара, Самарский государственный технический университет, 2010. — 54 с.: ил.

References

1. Solving problems of continuum mechanics in the ANSYS software package: method. instructions / M.V., Murashov. S.D. Panin. — M.: Publisher: Moscow, Bauman Moscow State Technical University, 2009. — p.40: ill.
 2. Optimization of structures ANSYS DesignXplorer – Text: electronic // ansysadvantage.ru : [website]. [URL: <https://www.ansysadvantage.ru/design-optimization-ansys-designxplorer>] (accessed: 10/13/2024)
 3. ANSYS Parametric Design Language Guide – Text: electronic // www.mm.bme.hu : [website]. URL: https://www.mm.bme.hu/~gyebro/files/fea/ansys/ans_apdl.pdf (accessed date: 10.10.2024).
 4. Pool bridge – Text: electronic // [URL: <http://www.bolshoyvopros.ru/questions/3757677-kak-nazyvaetsja-shtuka-s-kotoroj-prygajut-v-bassejn.html>] (date of request: 11.10.2024)
 5. Basic information about the ANSYS software package. Geometric modeling / E.A. Soldusova – Publishing house: Samara, Samara State Technical University, 2010. — p.54 ill.
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 536.2

ТЕПЛОПРОВОДНОСТЬ КОМПОЗИЦИОННОГО МАТЕРИАЛА СО СТАЛЬНОЙ РЕШЕТКОЙ НА ОСНОВЕ TPMS ТИПА SCHOEN'S GW И МАТРИЦЕЙ ИЗ КЕРАМИЧЕСКОГО МАТЕРИАЛА

Брагин Д.М., ¹Зинина С.А., Попов А.И., Мустафин Р.М., Кечин Н.Н.

ФГБОУ ВО «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»,
Самара, Россия, (443100, Самарская область, город Самара, Молодогвардейская ул., д.244),
e-mail: ¹sofazinina4@gmail.com

В работе рассмотрен композиционный материал с стальной решеткой на основе TPMS типа Schoen's GW и матрицей из керамического материала. Результаты моделирования переноса тепла подтверждают анизотропность свойств рассмотренного композиционного материала. Определена зависимость эффективной теплопроводности от относительного объема стальной решетки TPMS при распространении тепла в направлении декартовых координат. Термическое сопротивление композиционного материала при переносе тепла в направлении OY и OX выше, что увеличивает плотность теплового потока по сравнению с переносом тепла в направлении OZ на 11-15%. Уравнение Максвелла демонстрирует усредненное значение теплопроводности без учета направления переноса тепла в композиционных материалах на основе TPMS. Результаты работы демонстрируют необходимость учета геометрических особенностей композита при проектировании тепловой защиты и изоляционных систем.

Ключевые слова: Теплоперенос, анизотропность, композиционный материал, Schoen's GW, Triply Periodic Minimal Surface.

THERMAL CONDUCTIVITY OF A COMPOSITE MATERIAL WITH A STEEL LATTICE BASED ON TPMS OF SCHOEN'S GW TYPE AND A MATRIX MADE OF CERAMIC MATERIAL

Bragin D.M., ¹Zinina S.A., Popov A.I., Mustafin R.M., Kuchin N.N.

SAMARA STATE TECHNICAL UNIVERSITY, Samara, Russia, (443100, Samara region, Samara, Molodogvardeyskaya str., 244), e-mail: ¹sofazinina4@gmail.com

The paper considers a composite material with a steel lattice based on TPMS of Schoen's GW type and a matrix made of ceramic material. The results of heat transfer modeling confirm the anisotropy of the properties of the considered composite material. The dependence of the effective thermal conductivity on the relative volume of the TPMS steel grating during heat propagation in the direction of the Cartesian coordinates is determined. The thermal resistance of the composite material during heat transfer in the OY and OX directions is higher, which increases the heat flux density compared to heat transfer in the OZ direction by 11-15%. The Maxwell equation demonstrates the average value of thermal conductivity without taking into account the direction of heat transfer in TPMS-based composite materials. The results of the work demonstrate the need to take into account the geometric features of the composite when designing thermal protection and insulation systems.

Keywords: Heat transfer, anotropy, composite material, schoen's gw, triply periodic minimal surface.

Многокомпонентные материалы, известные как композиционные материалы, применяются при изготовлении кузовных деталей автомобиля, строительных конструкциях, ветряных турбинах, корпусах электроники и т.д. [1]. Очевидно, применение сфер не

ограничивается автомобилестроением, строительством и энергетикой. Композиционные материалы продолжают находить все новые сферы применения благодаря возможности точного подбора их свойств под конкретные задачи и условия эксплуатации [2].

В ряде задач, связанных с переносом тепла, а в частности при проектировании тепловой защиты и изоляции систем, необходим точный подбор теплопроводности конструкции [3]. На данный момент существуют экспериментальные методы определения теплопроводности материалов, среди которых метод стационарного теплового потока, метод горячей нити, тепловизионный метод и другие [4,5]. Каждый из методов имеет свои особенности и ограничения, поэтому выбор конкретного метода зависит от типа материала, его структуры, толщины, а также от требуемой точности. Однако в случае, когда необходимо определить теплопроводность материала на стадии проектирования до изготовления композита применяются аналитические методы. На данный момент прогнозирование свойств теплопроводности конструкций доступно при помощи параллельной модели (1) и уравнения Максвелла (2).

$$\lambda_{||} = \lambda_1 \varepsilon_1 + \lambda_2 \varepsilon_2 \quad (1)$$

$$\lambda = \lambda_1 \frac{(2\lambda_1 + \lambda_2 - 2\varepsilon_1(\lambda_1 - \lambda_2))}{(2\lambda_1 + \lambda_2 + \varepsilon_1(\lambda_1 - \lambda_2))} \quad (2)$$

где λ – теплопроводность композиционного материала, Вт м⁻¹ °C⁻¹; λ_i – теплопроводность компонента композита, Вт м⁻¹ °C⁻¹; ε – объемная доля компонента композита.

Использование параллельной модели демонстрирует максимальные значения теплопроводности при параллельном расположении элементов композита. При более сложной структуре используются уравнения Максвелла. Однако уравнения Максвелла могут быть использованы для композитов с изотропными свойствами. В композиционных материалах с сотовым сердечником свойства чаще всего анизотропны, а теплопроводность описывается тензором теплопроводности (3). В этом случае термическое сопротивление материала зависит от направления распространения тепла, что не учитывается в параллельной модели и уравнениях Максвелла.

$$\lambda = \begin{bmatrix} \lambda_{xx} & \lambda_{xy} & \lambda_{xz} \\ \lambda_{yx} & \lambda_{yy} & \lambda_{yz} \\ \lambda_{zx} & \lambda_{zy} & \lambda_{zz} \end{bmatrix} \quad (3)$$

В текущем исследовании представлен метод численного эксперимента, реализованного в программном комплексе Ansys, который позволяет определять теплопроводность анизотропного композиционного материала.

На рис. 1 представлена геометрическая модель сердечника композиционного материала. Комбинирование сердечников и последующее заполнения межпорового пространства (матрицы) позволяет получить композиционный материал требуемого масштаба. В качестве стального сердечника используется структура, основанная на TPMS (от англ. Triply Periodic Minimal Surface) типа Schoen's GW [6], а матрица композиционного материала заполнена керамикой.

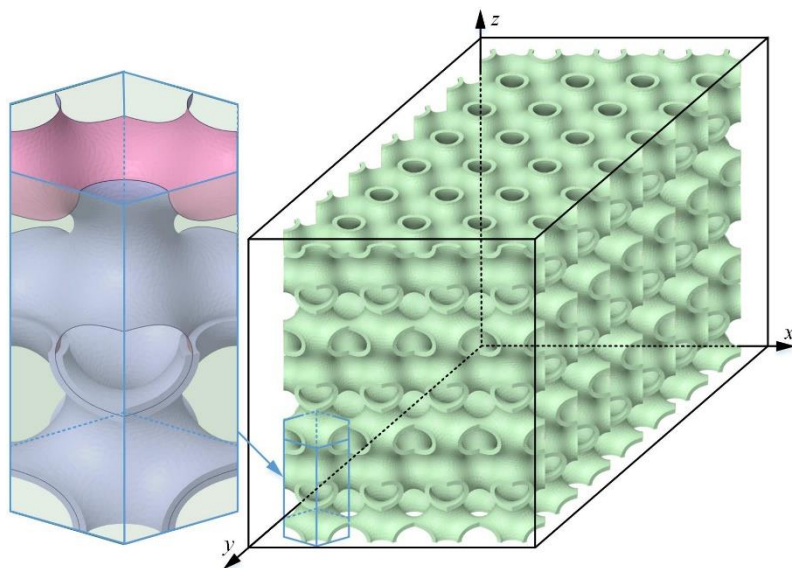


Рисунок 1. - Стальной сердечник композиционного материала, основанный на TPMS типа Schoen's GW

Таблица 1.- Геометрические размеры RVE объема

| № | Длина x, мм | Ширина z, мм | Высота y, мм | Относительный объем | |
|---|-------------|--------------|--------------|---------------------|--------|
| | | | | Керамика | Металл |
| 1 | 13,1 | 10,1 | 11,7 | 89% | 11% |
| 2 | 13,1 | 10,1 | 11,7 | 93% | 7% |
| 3 | 13,1 | 10,1 | 11,7 | 98% | 2% |

Для исследования теплофизических свойств неоднородных материалов с упорядоченной структурой применяется метод репрезентативного элементарного объема (REV-метод – от англ. representative elementary volume) [7]. Согласно REV-методу, выбирается минимальный объем, воспроизводящий свойства исследуемой системы. В рамках исследования был определен объем RVE, свойства которого могут быть обобщены на весь объем композиционного материала. Размеры расчетных моделей RVE представлены на рисунке 2 и в таблице 1. Теплопроводящие свойства конструкции приняты постоянными и независимыми от температуры. Объемная доля решетки TPMS (сердечника композиционного материала) варьировалась от 2% до 11%.

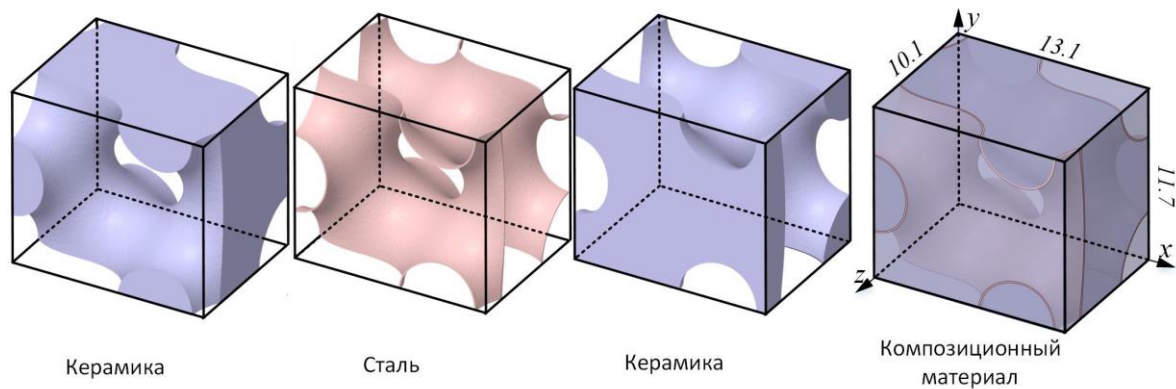


Рисунок 2. - Объем RVE композиционного материала с стальным сердечником и матрицей из керамики

Введем систему координат так, как показано на Рисунке 1 и Рисунке 2. Теплопроводящие свойства конструкции в направлении оси OX, OY, OZ могут отличаться из-за геометрических особенностей. Таким образом в работе рассматривается три модели переноса тепла в направлении оси OX, OY, OZ. Для исследования используется численный эксперимент методом стационарного теплового потока. На противоположных границах ячеек задаются температуры T1 (20°C) и T2 (50°C). После определения теплового потока, проходящего через структуру в установившемся режиме, определяется эффективная теплопроводность конструкции исходя из закона Фурье (4).

$$\begin{pmatrix} q_x \\ q_y \\ q_z \end{pmatrix} = - \begin{pmatrix} \lambda_{xx} & \lambda_{xy} & \lambda_{xz} \\ \lambda_{yx} & \lambda_{yy} & \lambda_{yz} \\ \lambda_{zx} & \lambda_{zy} & \lambda_{zz} \end{pmatrix} \begin{pmatrix} \partial T / \partial x \\ \partial T / \partial y \\ \partial T / \partial z \end{pmatrix} \quad (4)$$

Результаты моделирования переноса тепла подтверждают анизотропность свойств рассмотренного композиционного материала. Основные результаты представлены на Рисунке 3.

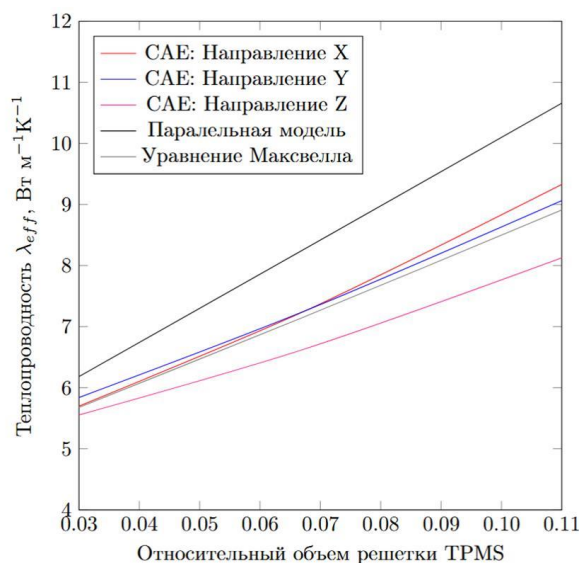


Рисунок 3. - Зависимость теплопроводности композиционного материала от относительного объема стального сердечника полученная в ходе CAE моделирования, Параллельной модели и уравнения Максвелла.

При увеличении относительного объема стальной решетки эффективная теплопроводность композиционного материала возрастает почти линейно во всех направлениях. Это связано с тем, что добавление стали с высокой теплопроводностью в композиционный материал улучшает общие теплофизические свойства системы.

Теплопроводность в направлении осей OX, OY и OZ имеет различные значения, что подтверждает наличие анизотропии в структуре. Исходя из зависимости эффективной теплопроводности от относительного объема решетки TPMS в направлении оси OZ наблюдается минимумы теплопроводности. Термическое сопротивление композиционного материала при переносе тепла в направлении OX и OY значительно ниже, что увеличивает плотность теплового потока в этих направлениях на 11-15%. Параллельная модель ожидаемо демонстрирует верхнюю границу для теплопроводности, поскольку она предполагает идеальный случай, при котором теплопроводность компонента распределяется параллельно по всему объему материала. Эта модель дает наибольшие значения теплопроводности, так как игнорирует сопротивление на границах между компонентами. Модель Максвелла для изотропных материалов демонстрирует усредненное значение теплопроводности без учета направления переноса тепла. Модель Максвелла может использоваться для определения осредненной теплопроводности по различным направлениям, однако при необходимости более точного понимания свойств могут применяться численные или натурные эксперименты.

Для использования композитов, основанных на сердечнике Schoen's GW, важно учитывать направление теплового потока и структурную анизотропию материала. Выбор ориентации композита существенно влияет на эффективность теплопередачи, что может быть использовано при оптимизации термических характеристик конструкции.

Исследование выполнено за счет гранта Российского научного фонда № 23-79-10044, <https://rscf.ru/project/23-79-10044/>

The study was funded by a grant from the Russian Science Foundation No 23-79-10044, <https://rscf.ru/project/23-79-10044/>

Список литературы

1. Khan F. et al. Advances of composite materials in automobile applications—A review //Journal of Engineering Research. – 2024.
2. Ozturk F., Cobanoglu M., Ece R. E. Recent advancements in thermoplastic composite materials in aerospace industry //Journal of Thermoplastic Composite Materials. – 2024. – Т. 37. – №. 9. – С. 3084-3116.
3. Huang C. et al. Enhanced tough recyclable hemiaminal dynamic covalent network with boron nitride composites material with high thermal conductivity at low filler content //Journal of Cleaner Production. – 2024. – Т. 448. – С. 141657.
4. Федоров А. А., Кораблев В. А., Федоров А. В., Ковальский И. С., Волков С. М., Андреева А. Метод нагреваемой нити для измерения теплопроводности вязких жидкостей // Вестник Международной академии холода. 2022. № 3. С. 66–73.
5. Корнилов Т. А., Эверстова В. Н. Оценка теплозащитных свойств наружных стен из полистиролбетонных блоков каркасно-монолитного здания //Academia. Архитектура и строительство. – 2024. – №. 3. – С. 137-144.
6. Chen D. et al. Interface structure of the dark conglomerate liquid crystal phase //Soft Matter. – 2011. – Т. 7. – №. 5. – С. 1879-1883.
7. Kanit T. et al. Determination of the size of the representative volume element for random composites: statistical and numerical approach //International Journal of solids and structures. – 2003. – Т. 40. – №. 13-14. – С. 3647-3679.

References

1. . Khan F. et al. Advances of composite materials in automobile applications—A review //Journal of Engineering Research. – 2024.
2. Ozturk F., Cobanoglu M., Ece R. E. Recent advancements in thermoplastic composite materials in aerospace industry //Journal of Thermoplastic Composite Materials. – 2024. – Т. 37. – №. 9. – pp. 3084-3116.
3. Huang C. et al. Enhanced tough recyclable hemiaminal dynamic covalent network with boron nitride composites material with high thermal conductivity at low filler content //Journal of Cleaner Production. – 2024. – Т. 448. – pp.141657.
4. Fedorov A. A., Korablev V. A., Fedorov A. V., Koval'skiy I. S., Volkov S. M., Andre-eva A. Metod nagrevaemoj niti dlya izmereniya teploprovodnosti vyazkix zhidkostej // Vestnik Mezhdunarodnoj akademii xoloda. 2022. № 3. pp. 66–73.
5. Kornilov T. A., E`verstova V. N. Ocenka teplozashhitny`x svojstv naruzhny`x sten iz polistirolbetonny`x blokov karkasno-monolitnogo zdaniya //Academia. Arxitektura i stroitel`stvo. – 2024. – №. 3. – pp. 137-144.
6. Chen D. et al. Interface structure of the dark conglomerate liquid crystal phase //Soft Matter. – 2011. – Т. 7. – №. 5. – pp. 1879-1883.

Теплопроводность композиционного материала со стальной решеткой на основе TPMS типа SCHOEN'S GW и матрицей из керамического материала / Брагин Д.М., Зинина С.А., Попов А.И. и др. // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 12(50) с. 144–150

7. Kanit T. et al. Determination of the size of the representative volume element for random composites: statistical and numerical approach //International Journal of solids and structures. – 2003. – Т. 40. – №. 13-14. – pp. 3647-3679.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 614.841.2.001.5

ИССЛЕДОВАНИЯ С ПРИМЕНЕНИЕМ СКАНИРУЮЩЕЙ ЭЛЕКТРОННОЙ МИКРОСКОПИИ В ЦЕЛЯХ УСТАНОВЛЕНИЯ ПРИЧИН ВОЗНИКНОВЕНИЯ ПОЖАРОВ НА АЛЮМИНИЕВЫХ ПРОВОДНИКАХ

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

В статье рассматриваются ключевые аспекты применения алюминиевых проводов и кабелей в электротехническом и энергетическом оборудовании, а также их уязвимость к различным негативным воздействиям, способным привести к серьезным аварийным ситуациям.

С помощью сканирующей электронной микроскопии (СЭМ) проведено детальное изучение микроструктуры проводников, выявлены признаки коррозии и образования оксидных пленок, что существенно ухудшает их проводимость. Результаты показывают, что электродуговые процессы до и после пожара имеют схожие механизмы, но различия в условиях окружающей среды приводят к формированию различных морфологических характеристик.

Ключевые слова: Сканирующая электронная микроскопия, электрический пожара, пожарно-техническая экспертиза, алюминиевые проводники.

SCANNING ELECTRON MICROSCOPY STUDIES TO DETERMINE THE CAUSES OF FIRES ON ALUMINUM CONDUCTORS

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

The article deals with the key aspects of aluminum wires and cables application in electrical and power engineering equipment, as well as their vulnerability to various negative effects that can lead to serious accidents.

Using scanning electron microscopy (SEM) a detailed study of conductor microstructure has been carried out, signs of corrosion and formation of oxide films have been revealed, which significantly deteriorates their conductivity. The results show that electric arc processes before and after the fire have similar mechanisms, but differences in environmental conditions lead to the formation of different morphological characteristics.

Keywords: Scanning electron microscopy, electrical fire, fire technical examination, aluminum conductors.

Алюминиевые провода и кабели играют ключевую роль в современном электротехническом и энергетическом оборудовании благодаря своим уникальным

свойствам, таким как легкость, высокая проводимость и устойчивость к коррозии. Они находят широкое применение в различных областях, начиная от передачи электроэнергии и заканчивая бытовой электроникой. Однако, несмотря на эти преимущества, алюминиевые проводники подвержены множеству негативных факторов, которые могут существенно повлиять на их эксплуатационные характеристики и безопасность [1-3, 5].

Статистические данные свидетельствуют о том, что от 60% до 80% всех электрических пожаров происходят из-за проблем с проводкой, перегрева электроприборов и короткого замыкания. В таких случаях алюминиевые проводники становятся важным объектом для расследования причин возникновения пожаров, так как они часто служат вещественными доказательствами. Оплавление алюминиевых проводников может происходить по нескольким причинам:

- непосредственным коротким замыканием цепи или перегрузкой, вызванной первичным коротким замыканием, которое подразделяется на внезапное мгновенное короткое замыкание и длительную перегрузку, вызванную нагревом.
- вторичным коротким замыканием, не связанным с электрическим пожаром, вызванным повреждением изоляции. Это вторичное короткое замыкание, в свою очередь, может быть вызвано первичным источником зажигания, температурой, временем и продолжительностью воздействия.
- пожаром, не связанным с электрическим пожаром [4, 6-7].

В данной статье рассматриваются результаты исследований, проведенных с использованием сканирующей электронной микроскопии (СЭМ), для детального изучения микроструктуры алюминиевых проводников. Исследования показывают, что внешние тепловые воздействия приводят к значительным изменениям на поверхности проводников, включая коррозию и образование оксидных пленок. Эти изменения, в свою очередь, ухудшают проводимость материала и могут стать причиной серьезных аварийных ситуаций [8-9].

Применение сканирующей электронной микроскопии (СЭМ) проводится для детального изучения микроструктуры проводников, выявления трещин, коррозии и других аномалий.

Результаты исследования показали, что на поверхности алюминиевых проводников, в результате внешне-теплого воздействия, наблюдались значительные признаки коррозии и образования оксидных пленок (Рисунок 1). Эти изменения ассоциированы с многократными термическими циклами и воздействием влаги, что существенно ухудшает проводимость материала.

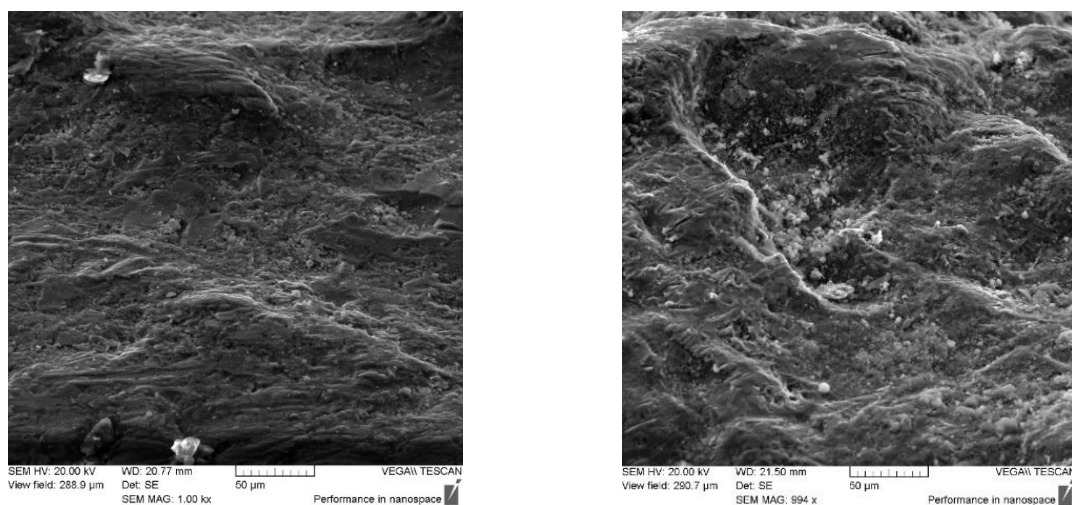


Рисунок 1 - Морфология поверхности алюминиевых проводников при тепловом воздействии, не связанном в электрическими аварийными режимами

На Рисунке 2 показана поверхность оплавленных алюминиевых проводников при электродуговом процессе в условиях до пожара: обнаружены лунки и кратеры, имеются микропоры и большое количество микрокристаллов, которые разбросаны по поверхности.

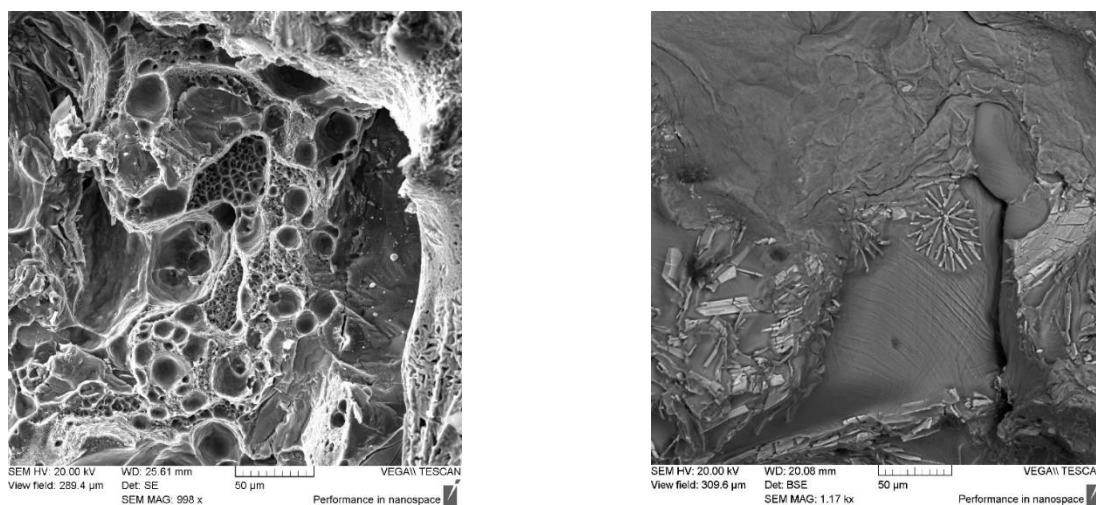


Рисунок 2 - Морфологические признаки на алюминиевых проводниках при электродуговом процессе в условиях до пожара

В результате исследования образцов полученных при моделировании электродугового процессе в условиях пожара было обнаружено, что присутствуют примесные элементы, есть несколько микрокристаллов, но их количество невелико (Рисунок 3).

- Чешко, Ю.Н. Бельшина; под общ. ред. Э.Н. Чижикова. – СПб: ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России», 2016. – 160 с.
4. Колмаков А.И., Степанов Б.В., Зернов С.И., Россинская Е.Р., Соколов Н.Г. Диагностика причин разрушения металлических проводников, изъятых с мест пожаров: Метод. рекомендации. - М.: ЭКЦ МВД РФ, 1992. – 32 с.
 5. Колмаков А.И., Граненков Н.М., Зернов С.И., Пеньков В.В., Соколов Н.Г., Степанов Б.В., Таубкин И.С., Чешко И.Д.. Экспертное исследование металлических изделий (по делам о пожарах) / Учебное пособие /М. ЭКЦ МВД России, 1993. – 104 с.
 6. Zhao Chang Zheng, Wang Xin Ming, Yu Li Li. Analysis on ground fault and propagation characteristic of electrical fire[C]//The Proceedings of the China Association for Science and Technology. Beijing: Science Press, 2009:144-148.
 7. Xin-ming Wang, Ying Wu, Chang-zheng Zhao, Qing-shan Meng, Ao Gao, Analysis on Fire Risk of Aluminium Conductors under Electrical Faults in Low Voltage Circuit, Procedia Engineering, Volume 52, 2013, Pages 408-412, ISSN 1877-7058, <https://doi.org/10.1016/j.proeng.2013.05.001>
 8. Lapovok R. Y. Qi, Kosinova A. Architected hybrid conductors: Aluminium with embedded copper helix / R. Lapovok, Y. Qi, A. Kosinova [et al.] // MATERIALS & DESIGN. – 2020. – Vol. 187. – P. 108398. – DOI 10.1016/j.matdes.2019.108398.
 9. 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.

References

1. . Smelkov G.I. Fire safety of electrical wiring. – М.: LLC "CABLE", 2009. – p.328.
2. Mitrichev L.S., Kolmakov A.I., Stepanov B.V. and others. Investigation of copper and aluminum conductors in areas of short circuit and thermal exposure. Methodological recommendations. - М., 1986. – p.43.
3. Metallographic and morphological studies of metal objects of forensic fire-technical expertise: textbook / A.Y. Mokryak, I.D. Cheshko, Yu.N. Belshina; under the general editorship of E.N. Chizhikov. – St. Petersburg: St. Petersburg State Budgetary Educational Institution "St. Petersburg University of GPS of the Ministry of Emergency Situations of Russia", 2016. – p.160
4. Kolmakov A.I., Stepanov B.V., Zernov S.I., Rossinskaya E.R., Sokolov N.G. Diagnostics of the causes of destruction of metal conductors removed from fire sites: Method. recommendations. - М.: ECC of the Ministry of Internal Affairs of the Russian Federation, 1992. – p.32
5. Kolmakov A.I., Granenkov N.M., Zernov S.I., Penkov V.V., Sokolov N.G., Stepanov B.V., Taubkin I.S., Cheshko I.D.. Expert study of metal products (in cases of fires) / Textbook /М. ECC of the Ministry of Internal Affairs of Russia, 1993. – p.104
6. Zhao Chang Zheng, Wang Xin Ming, Yu Li Li. Analysis on ground fault and propagation characteristic of electrical fire[C]//The Proceedings of the China Association for Science and Technology. Beijing: Science Press, 2009: pp.144-148.

7. Xin-ming Wang, Ying Wu, Chang-zheng Zhao, Qing-shan Meng, Ao Gao, Analysis on Fire Risk of Aluminium Conductors under Electrical Faults in Low Voltage Circuit, Procedia Engineering, Volume 52, 2013, Pages 408-412, ISSN 1877-7058, <https://doi.org/10.1016/j.proeng.2013.09.001>
 8. Lapovok R. Y. Qi, Kosinova A. Architectural hybrid conductors: Aluminum with embedded copper helix / R. Lapovok, Y. Qi, A. Kosinova [et al.] // MATERIALS & DESIGN. – 2020. – Vol. 187. – P. 108398. – DOI 10.1016/j.matdes.2019.108398.
 9. Mokryak A.Yu., Mokryak A.V. Research of metal and electrotechnical objects of forensic fire and technical expertise: monograph / edited by B.V. Gavkalyuk – St. Petersburg: St. Petersburg University of GPS of the Ministry of Emergency Situations of Russia, 2022. – p. 212
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 614.841.2.001.5

ПРИЧИНЫ ВОЗНИКНОВЕНИЯ ПОЖАРОВ В ЭЛЕКТРОМОБИЛЕ

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

В данной статье рассматриваются причины возникновения пожаров в электромобилях. Этот вид транспорта становится всё более популярным благодаря своей экологичности и экономичности, но, как и любой другой, он не лишён потенциальных опасностей. В частности, пожары представляют серьёзную угрозу для безопасности пассажиров и окружающей среды. В работе анализируются такие факторы, как короткое замыкание, перегрев аккумуляторов, повреждение проводки, неправильная зарядка, внешние факторы и конструктивные недостатки. Уделяется внимание важности соблюдения правил эксплуатации и обслуживания электротранспорта для снижения риска возникновения пожаров. Статья подчёркивает необходимость повышения осведомлённости пользователей и производителей о возможных угрозах, а также разработки более безопасных технологий в области электротранспорта.

Ключевые слова: Электротранспорт, экспертиза пожаров, пожарная безопасность, зарядка, короткое замыкание.

CAUSES OF FIRES IN ELECTRIC VEHICLES

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

This article discusses the causes of fires in electric vehicles. This mode of transportation is becoming increasingly popular due to its environmental friendliness and cost-effectiveness, but like any other mode of transportation, it is not without potential hazards. In particular, fires pose a serious threat to the safety of passengers and the environment. The paper analyzes such factors as short circuits, battery overheating, damaged wiring, improper charging, external factors and design flaws. Attention is paid to the importance of following the rules of operation and maintenance of electric vehicles to reduce the risk of fires. The article emphasizes the need to raise awareness among users and manufacturers of possible hazards and to develop safer technologies in the field of electric vehicles.

Keywords: Electric transport, fire expertise, fire safety, charging, short circuit.

Введение

В последние годы электромобили становятся всё более популярными, предлагая экологически чистый и эффективный способ передвижения. В настоящее время в России наблюдается стремительный рост числа пользователей электромобилей. Благодаря

государственной поддержке по субсидированию производства и покупки электромобилей парк электрокаров, по данным Минэкономразвития, с 2021 года увеличился в 3,2 раза. Производство электромобилей за 2,5 года составило более 12 тыс. единиц.

Спрос на новые электромобили в России по сравнению с аналогичным периодом прошлого года вырос на 98,6%. Однако, несмотря на их преимущества, безопасность остаётся важной темой обсуждения. Одним из наиболее тревожных аспектов является риск возникновения пожаров в электромобилях [1-3, 5].

Целью данного исследования является выявление и анализ основных причин возникновения пожаров в электромобилях, а также оценка их влияния на безопасность пользователей и окружающей среды. Статья стремится повысить осведомлённость как пользователей, так и производителей о потенциальных угрозах, связанных с эксплуатацией электротранспорта. Понимание причин пожаров и факторов, способствующих их возникновению, является ключевым для разработки эффективных мер по предотвращению подобных инцидентов.

Рассмотрим основные факторы, способствующие возникновению пожаров в электротранспорте [4, 6-8]:

Короткое замыкание.

Одной из самых распространенных причин пожаров в электротранспорте является короткое замыкание. Оно может произойти из-за повреждения изоляции проводов, неправильного подключения аккумуляторов или неисправностей в электрооборудовании. Короткие замыкания могут вызывать перегрев и воспламенение материалов, находящихся рядом.

Перегрев аккумуляторов.

Аккумуляторы, особенно литий-ионные, могут перегреваться при неправильной эксплуатации или производственных дефектах. Перегрев может привести к тепловому разгону, что в свою очередь может вызвать возгорание. Важно следить за состоянием аккумуляторов и соблюдать рекомендации по их зарядке и эксплуатации.

Повреждение проводки

Механические повреждения проводки, например, в результате аварий или неосторожной эксплуатации, могут стать причиной возникновения пожара. Изоляция проводов может быть повреждена, что приведет к коротким замыканиям и перегреву.

Неправильная зарядка

Неправильная зарядка электромобилей может привести к перегреву аккумуляторов. Использование несертифицированных зарядных устройств или зарядка в условиях высокой температуры могут увеличить риск возникновения пожара.

Внешние факторы

Пожары могут возникать и по причинам, не связанным непосредственно с самим электротранспортом. Это могут быть внешние источники огня, такие как пожары в окружающей среде, или столкновения с другими транспортными средствами.

Конструктивные недостатки

Некоторые модели электротранспорта могут иметь конструктивные недостатки, которые делают их более уязвимыми к возникновению пожаров. Это может включать неадекватную систему охлаждения, недостаточную защиту от механических повреждений или слабые места в конструкции.

Анализируя причины пожаров в электромобилях, можно сказать что большинство из них происходят во время зарядки.

Согласно данным, 80% пожаров в электромобилях происходят в процессе зарядки, при этом перезарядка, отказ батареи или короткое замыкание линии являются наиболее распространёнными причинами [9-13]. Поэтому понимание проблем, связанных с зарядкой электромобилей, имеет большое значение для решения этой проблемы (Рисунок 1) [14].



Рисунок 1 - Пожар на электромобиле во время зарядки

Многие люди имеют привычку перезаряжать свои электромобили, но не намеренно, а из-за того, что они используют их днём и заряжают ночью. Для полной зарядки аккумулятора электромобиля требуется около 6-8 часов, и к тому моменту, когда аккумулятор полностью заряжен, люди часто уже спят и не отключают его на следующее утро. Продолжение зарядки после полной зарядки может привести к нагреву зарядного устройства и аккумулятора, что может легко стать причиной пожара. По некоторым данным, около 85 процентов пожаров в электромобилях происходит в период между 8 часами вечера и 5 часами утра следующего дня.

Кроме того, люди не всегда учитывают влияние окружающей среды на зарядку электромобилей. Оптимальная температура зарядки для электромобилей составляет 25°C, и заряжать их лучше всего в сухом, проветриваемом и прохладном помещении. Зарядка в жаркую погоду под прямыми солнечными лучами может не только повредить батарею, но и повысить риск самовозгорания. А в дождливые дни не рекомендуется подвергать вилку, порт зарядки и другие элементы воздействию дождя, так как попадание дождевой воды внутрь батареи может привести к её утечке и возгоранию.

Чтобы предотвратить большинство пожаров электромобилей, необходимо повысить осведомленность пользователей о безопасности. Некоторые люди, хотя и пользуются электромобилями каждый день, не всегда понимают связанные с ними меры предосторожности. Они могут совершать опасные действия, такие как:

- зарядка электромобиля на открытом воздухе в дождь.
- несвоевременная замена аккумулятора.

- забывание извлечь зарядные устройства.
- парковка электромобилей вблизи пожарных лестниц и лестничных клеток.

Эти действия повышают риски пожарной безопасности электромобилей. Помимо того, что сами пользователи должны быть более осведомлены, местные органы власти и пожарные департаменты также должны усилить пропаганду и разъяснение этих знаний. Они должны объяснить населению причины, по которым электромобили подвержены пожарам, и предложить профилактические меры.

Заключение

Пожары в электромобиле — это серьезная проблема, требующая внимания как со стороны производителей, так и со стороны пользователей. В данной статье были подробно рассмотрены причины возникновения пожаров в электромобилях, которые, несмотря на свои экологические и экономические преимущества, представляют собой потенциальную угрозу для безопасности пользователей и окружающей среды. Основные факторы, способствующие таким инцидентам, включают короткие замыкания, перегрев аккумуляторов, повреждение проводки, неправильную зарядку, внешние факторы и конструктивные недостатки.

Особое внимание уделено тому, что 80% пожаров происходят во время зарядки, что подчеркивает важность соблюдения правил эксплуатации и повышения осведомленности пользователей о потенциальных рисках. Для минимизации угрозы необходимо информировать владельцев электромобилей о безопасных практиках зарядки, регулярном обслуживании и правильном использовании оборудования.

Таким образом, для обеспечения безопасности электротранспорта требуется комплексный подход, включающий как действия со стороны пользователей, так и инициативы производителей и местных властей. Повышение уровня знаний о мерах предосторожности и разработка более безопасных технологий помогут снизить риск возникновения пожаров и сделают использование электромобилей более безопасным и комфортным.

Список литературы

1. Плотников В. Г., Чешко И. Д., Кондратьев С. А. Пожарная опасность литий-ионных аккумуляторов и низковольтных источников питания на их основе // Расследования пожаров. 2014. Вып. 4. С. 53–58.
2. Елисеев Ю. Н., Мокряк А. В. Анализ пожарной опасности литий-ионных аккумуляторных батарей // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". – 2020. – № 3. – С. 14-17.
3. Скундин А. М., Ефимов О. Н., Ярмоленко О. В. Современное состояние и перспективы развития исследований литиевых аккумуляторов // Успехи химии. 2012. Т. 71. № 4. С. 378–398.
4. Srinivasan R., Demirev P.A., Carkhuff B.G., Santhanagopalan S., Jeevarajan J.A., Barrera T.P. Review - Thermal safety management in li-ion batteries: Current issues and perspectives J. Electrochem. Soc., 167 (14) (2020).
5. Wu, Feixiang & Chu, Fulu & Xue, Zhichen. (2021). Lithium-Ion Batteries. 10.1016/B978-0-12-819723-3.00102-5.

6. Q. Wang, B. Mao, S.I. Stoliarov, J. Sun A review of lithium ion battery failure mechanisms and fire prevention strategies Prog. Energy. Combust. Sci., 73 (2019), pp. 95-131.
7. Liwei Zhao, Atsushi Inoishi, Shigeto Okada, Thermal risk evaluation of concentrated electrolytes for Li-ion batteries, Journal of Power Sources Advances, Volume 12, 100079, 2021
8. Мокряк А. В., Мокряк А. Ю., Мельник А. А. Анализ остатков литий-ионных аккумуляторов после теплового разгона методом сканирующей электронной микроскопии // Международный научно-исследовательский журнал. – 2023. – № 4(130). – DOI 10.23670/IRJ.2023.130.63.
9. Пожары и пожарная безопасность в 2018 году: статистический сборник / под общ. ред. Д.М. Гордиенко - М.: ВНИИПО. – 2019. – 125 с.
10. Пожары и пожарная безопасность в 2019 году: статистический сборник / под общ. ред. Д.М. Гордиенко - М.: ВНИИПО. – 2020. – 125 с.
11. Пожары и пожарная безопасность в 2020 году: статистический сборник / под общ. ред. Д.М. Гордиенко - М.: ВНИИПО. – 2021. – 112 с.
12. Пожары и пожарная безопасность в 2021 году: статистический сборник / под общ. ред. Д.М. Гордиенко - М.: ВНИИПО. – 2022. – 114 с.
13. Пожары и пожарная безопасность в 2022 году: статистический сборник / под общ. ред. Д.М. Гордиенко - М.: ВНИИПО. – 2023. – 80 с
14. <https://abw.by/news/incidents/2020/05/19/kak-odin-elektromobil-szheg-celuu-parkovku-s-mashinami-v-kitae>

References

1. Plotnikov V. G., Cheshko I. D., Kondratiev S. A. Fire hazard of lithium-ion batteries and low-voltage power sources based on them // Fire investigations. 2014. Issue. 4. pp. 53–58.
2. Eliseev Yu. N., Mokryak A. V. Analysis of the fire hazard of lithium-ion batteries // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergencies of Russia". – 2020. – No. 3. – pp. 14–17.
3. Skundin A. M., Efimov O. N., Yarmoolenko O. V. Current state and prospects for the development of lithium battery research // Uspekhi khimii. 2012. T. 71. No. 4. pp. 378–398.
4. Srinivasan R., Demirev P.A., Carkhuff B.G., Santhanagopalan S., Jeevarajan J.A., Barrera T.P. Review - Thermal safety management in li-ion batteries: Current issues and perspectives J. Electrochem. Soc., 167 (14) (2020).
5. Wu, Feixiang & Chu, Fulu & Xue, Zhichen. (2021). Lithium-Ion Batteries. 10.1016/B978-0-12-819723-3.00102-5.
6. Q.Wang, B. Mao, S.I. Stoliarov, J. Sun A review of lithium ion battery failure mechanisms and fire prevention strategies Prog. Energy. Combust. Sci., 73 (2019), pp. 95-131.
7. Liwei Zhao, Atsushi Inoishi, Shigeto Okada, Thermal risk evaluation of concentrated electrolytes for Li-ion batteries, Journal of Power Sources Advances, Volume 12, 100079, 2021
8. Mokryak A. V., Mokryak A. Yu., Melnik A. A. Analysis of lithium-ion battery residues after thermal runaway by scanning electron microscopy // International Research Journal. - 2023. - No. 4 (130). - DOI 10.23670 / IRJ.2023.130.63.
9. Fires and fire safety in 2018: statistical digest / under the general editorship of D. M. Gordienko - М.: ВНИИПО. – 2019. – p.125

10. Fires and fire safety in 2019: statistical digest / edited by D.M. Gordienko - М.: VNIIPO. – 2020. – p. 125.
 11. Fires and fire safety in 2020: statistical digest / edited by D.M. Gordienko - М.: VNIIPO. – 2021. – p.112
 12. Fires and fire safety in 2021: statistical digest / edited by D.M. Gordienko - М.: VNIIPO. – 2022. – p.114
 13. Fires and fire safety in 2022: statistical digest / edited by D.M. Gordienko - М.: VNIIPO. – 2023. – p.80.
 14. <https://abw.by/news/incidents/2020/05/19/kak-odin-elektromobil-szheg-celuu-parkovku-s-mashinami-v-kitae>
-