

Международный журнал информационных технологий и энергоэффективности |



Том 8 Номер 6 (32)



2023



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	Перевертун Д.Р. Криптография и её роль в обеспечении информационной безопасности	5
	Perevertun D.R. Cryptography and its role in ensuring information security	
2.	Романов Н.А. Прогнозирование сбоев ИОТ-устройств для гибкого планирования их технического обслуживания	10
	Romanov N.A. Predicting failures of IOT devices for flexible planning of their maintenance	
3.	Хамидулин Д.М., Войкин А.О., Муханова Р.Е., Григорьев Д.О. Математическая модель определения координат станции	16
	Khamidulin D.M., Voikin A.O., Mukhanova R.E., Grigoriev D.O. Mathematical model for determining station coordinates	
4.	Евстифеев И.А. Перспективы использования машинного обучения для классификации документов государственных закупок	28
	Evstifeev I.A. Prospects for using machine learning to classify public procurement documents	
5.	Чекановкин А.Е. Архитектура многопоточного приложения в условиях интероперабельности процессов	40
	Chekanovkin A.E. Architecture of a multi-thread application under the conditions of arch process interoperability	
6.	Багазей Д.И. Потенциал VR в гостиничном бизнесе	50
	Bagazey D.I. The potential of vr in the hospitality industry	
7.	Кириллина Ю.В., Олейник А.С. Анализ ИТ-архитектуры департамента управления проектами	56
	Y.V. Kirillina, A.S. Oleynik Analysis of the IT architecture of the project management department	
8.	Яшин С.О., Соловьев Я.А. Анализ применения цифровых технологий в сфере строительного контроля автомобильных дорог	61
	Yashin S.O., ¹Soloviev Ya.A. Analysis of the use of digital technologies in the field of construction control of highways	
9.	Дементьев С.Ю., Воробьев В.В. Роль интеллектуального анализа процессов в четвертой промышленной революции	69

	Dementev S.Y., Vorobyov V.V. The role of process mining in the fourth industrial revolution	
10.	Балановский В.Л., Подъяконов В.М., Алборова М.Б. Вызовы и риски современного мира в цифровой среде	75
	Balanovsky V.L., Podyakonov V.M., Alborova M.B. Challenges and risks of the modern world in the digital environment	
11.	Обливальный Н.Д. Определение практической значимости и экономической эффективности оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них	80
	Oblivalny N.D. Determining the practical significance and economic efficiency of the optimal way of interacting with the client to increase the profitability of marketing campaigns and reduce their costs	
12.	Осипович П.А. Применение методов теории ограничений систем в отделе проектной разработки ИТ компании	91
	Osipovich P.A. The application of the methods of the theory of systems constraints in the design department of an IT company	
13.	Лукашев А.В., Шабуня В.В., Сарафанников В.С., Билан В.В. Квантовая устремленность как угроза информационной безопасности	97
	Lukashev A.V., Shabunya V.V., Sarafannikov V.S., Bilan V.V. Quantum aspiration as a threat information security	
14.	Васильева Д.Е., Сидорова А.А., Макуха Л.В., Сидоров А.Ю. Виртуальный тур по университету для абитуриентов	102
	Vasilyeva D.E., Sidorova A.A., Makukha L.V., Sidorov A.Yu. Virtual tour of the university for applicants	
15.	Ильясов Р.Р., Рахимов А.Р., Сахаутдинов А.А., Хайруллин Р.Д. Исследование значимости признаков переменных при локальном диагностировании полярных сияний	109
	Ilyasov R.R., Rakhimov A.R., Sakhautdinov A.A., Khairullin R.D. Investigation of the significance of variable signs in the local diagnosis of auroras	
16.	Микрюков И.И. Реализация веб-чата с использованием WebSocket на языке Golang	115
	Mikryukov I.I. Web-chat implementation using WebSocket in Golang language	
17.	Микрюков И.И. Реализация прямой трансляции с помощью NGINX-RTMP модуля	120
	Mikryukov I.I. Implementing live streaming using the NGINX-RTMP module	
18.	Антонов Д.А. Современные инструменты для автоматизации разработки программного обеспечения	126
	Antonov D.A. Modern tools for automating software development	
19.	Андреева Я.А., Василевский К.А. Анализ современных систем обнаружения вторжений	134
	Andreeva Ya.A., Vasilevsky K.A. Analysis of modern intrusion detection systems	

20.	Дементьев С.Ю., Роза М.П. Анализ больших данных на промышленном предприятии	142
	Dementev S.Y., Roza M.P. Big data analysis in an industrial enterprise	
21.	Сулейменова Р.Д., Устюжанина С.П. Киберпреступность XXI века и её влияние на современное общество	148
	Suleimenova R.D., Ustyuzhanina S.P. Cybercrime of the XXI century and their impact on modern society	
22.	Сидоров В.А., Алиусманов Г.Э., Антонов Р.Б., Климчук И.В., Медведев М.С. Анализ существующих инструментов конфигурации и верификации файлов SCL ЦПС	152
	Sidorov V.A., Aliusmanov G.E., Antonov R.B., Klimchuk I.V., Medvedev M.S. Analysis of existing tools for configuration and verification of SCL FILES of the CPS	
23.	Антонов Р.Б., Сидоров В.А., Медведев М.С., Алиусманов Г.Э., Климчук И.В. Роль кибербезопасности цифровых подстанций в цифровизации электроэнергетики	157
	Antonov R.B., Sidorov V.A., Medvedev M.S., Aliusmanov G.E., Klimchuk I.V. The role of cyber security of digital substations in the digitalization of the power industry	
ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ		
24.	Канарейкин А.И. Повышение энергоэффективности вакуумных коллекторов за счёт использования естественной циркуляции	164
	Kanareykin A.I. Increasing the energy efficiency of vacuum collectors through the use of natural circulation	
25.	Кузьмин В.В., Гараев Р.Р. Электропитание объектов газовой промышленности при значительном удалении от линий электропередач	170
	Kuzmin V.V., Garaev R.R. Power supply of gas industry facilities at a considerable distance from power lines	
26.	Канарейкин А.И. Накопление солнечной энергии в ионисторе	174
	Kanareykin A.I. Accumulation of solar energy in an ionistor	



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

КРИПТОГРАФИЯ И ЕЁ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перевертун Д.Р.

ФГБОУ ВО Санкт-Петербургский государственный университет Телекоммуникаций им. профессора М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Данная статья рассматривает роль криптографии в обеспечении информационной безопасности. Криптография - наука о защите информации путем шифрования и расшифрования данных. Она играет критическую роль в различных сферах, включая коммерцию, финансы, здравоохранение и правительство. Криптография обеспечивает конфиденциальность, целостность и подлинность данных, а также предотвращает несанкционированный доступ и подделку информации. Статья также освещает важные аспекты криптографии, такие как аутентификация, защита от отказа в обслуживании, защита персональных данных и управление ключами. Также упоминается роль криптографии в облачных вычислениях и технологии блокчейн. В заключение, отмечается необходимость постоянного совершенствования криптографических методов в связи с появлением новых угроз и развитием квантовых вычислений.

Ключевые слова: Криптография, информационная безопасность, шифрование, конфиденциальность, аутентификация, защита персональных данных, блокчейн, квантовые вычисления.

CRYPTOGRAPHY AND ITS ROLE IN ENSURING INFORMATION SECURITY

Perevertun 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: danilaperevertun@gmail.com

This article examines the role of cryptography in ensuring information security. Cryptography is the science of protecting information by encrypting and decrypting data. It plays a critical role in various fields, including commerce, finance, healthcare, and government. Cryptography ensures confidentiality, integrity and authenticity of data, as well as prevents unauthorized access and forgery of information. The article also highlights important aspects of cryptography, such as authentication, denial of service protection, personal data protection and key management. The role of cryptography in cloud computing and blockchain technology is also mentioned. In conclusion, there is a need for continuous improvement of cryptographic methods in connection with the emergence of new threats and the development of quantum computing.

Keywords: Cryptography, information security, encryption, confidentiality, authentication, personal data protection, blockchain, quantum computing.

В современном цифровом мире, где информация играет важнейшую роль, обеспечение ее безопасности является критическим вопросом. Криптография - наука о защите информации путем применения математических алгоритмов и преобразований. Она играет важную роль в обеспечении конфиденциальности, целостности и подлинности данных.

Одной из основных целей криптографии является обеспечение конфиденциальности. Конфиденциальность означает, что только авторизованные пользователи имеют доступ к защищенной информации, и никто другой не может прочитать или понять содержимое. Криптографические алгоритмы используются для шифрования данных, что делает их непонятными для посторонних лиц. Только тот, кто обладает правильным ключом, может расшифровать данные и получить доступ к оригинальной информации. Это особенно важно при передаче конфиденциальных данных, таких как финансовая информация, медицинские записи, персональные данные и коммерческие секреты [1].

Криптография также обеспечивает целостность данных. Целостность гарантирует, что информация остается неизменной и неподделываемой в процессе передачи и хранения. Криптографические хэш-функции используются для создания уникальной сигнатуры для каждого набора данных. Если даже незначительное изменение происходит в данных, это приведет к изменению хэш-значения. Таким образом, при проверке целостности данных можно обнаружить любые несанкционированные изменения.

Помимо конфиденциальности и целостности, криптография обеспечивает подлинность данных. Подлинность гарантирует, что информация и источник информации подлинны и не были подделаны. Криптографические методы цифровой подписи используются для создания электронной подписи, которая является уникальной для каждого отправителя и не может быть подделана. Получатель может проверить электронную подпись, чтобы убедиться в подлинности источника данных и целостности информации.

Криптография играет важную роль в информационной безопасности в различных сферах, включая коммерцию, финансы, здравоохранение, правительство и многое другое. Она позволяет защитить конфиденциальность клиентов и пользователей, предотвратить несанкционированный доступ к чувствительным данным и обеспечить доверие в электронных коммуникациях.

Однако, как и любая другая технология, криптография не является идеальной. С развитием компьютерных мощностей атакующих и появлением новых методов анализа, криптографические алгоритмы могут стать уязвимыми. Поэтому важно постоянно развивать и совершенствовать криптографические методы и стандарты, чтобы они оставались надежными и устойчивыми к атакам [2].

Кроме основных принципов конфиденциальности, целостности и подлинности, криптография также имеет другие важные аспекты в обеспечении информационной безопасности. Одним из таких аспектов является аутентификация. Аутентификация позволяет проверить подлинность идентификации пользователей или системы. Криптографические методы, такие как цифровые сертификаты и аутентификация на основе открытых ключей (PKI), используются для проверки подлинности идентичности и обеспечения безопасного взаимодействия между участниками.

Криптография также играет роль в обеспечении конфиденциальности при передаче данных по открытым каналам связи, таким как интернет. Протоколы шифрования, такие как SSL/TLS, обеспечивают защищенное соединение между клиентом и сервером, шифруя передаваемую информацию и предотвращая ее перехват и несанкционированный доступ.

Другой важный аспект криптографии - это управление ключами. Криптографические алгоритмы работают на основе ключей, которые используются для шифрования и расшифрования данных. Управление ключами включает в себя безопасное генерирование,

хранение, обмен и уничтожение ключей. Эффективное управление ключами является неотъемлемой частью криптографической системы, поскольку компрометация ключей может привести к нарушению безопасности данных [3-4].

Современные технологии, такие как блокчейн, также полагаются на криптографию для обеспечения безопасности. Блокчейн использует криптографические методы, такие как хэш-функции и цифровые подписи, для обеспечения неподделываемости данных, подтверждения транзакций и создания децентрализованной доверенной среды.

Однако, несмотря на все преимущества криптографии, она не является панацеей и не может полностью исключить угрозы информационной безопасности. Развитие криптоанализа и новых атакующих методов требует постоянного совершенствования криптографических алгоритмов и протоколов. Кроме того, человеческий фактор, такой как ненадлежащая реализация или использование слабых паролей, также может ослабить защиту, даже при использовании сильных криптографических методов.

В целом, криптография играет критическую роль в обеспечении информационной безопасности, обеспечивая конфиденциальность, целостность, подлинность и другие аспекты безопасности данных.

Помимо этого, криптография также является ключевым элементом при обеспечении защиты персональных данных и соблюдении соответствующих законодательных норм и регуляций, таких как Общий регламент по защите данных (GDPR) в Европейском союзе. Криптография позволяет шифровать персональные данные, что делает их непонятными для третьих лиц, и устанавливать контроль над доступом к этим данным. Это особенно важно для организаций, которые собирают, обрабатывают и хранят большие объемы личной информации.

Еще одним важным аспектом криптографии является возможность обеспечить безопасность в облачных вычислениях. Облачные сервисы позволяют организациям хранить и обрабатывать данные удаленно, но одновременно это может повлечь угрозы безопасности. Криптография в облачных вычислениях может быть использована для шифрования данных перед их отправкой в облако, а также для обеспечения конфиденциальности и целостности данных в хранилище облака.

Все более частыми становятся также криптовалюты и технология блокчейн. Криптография является фундаментальным компонентом блокчейна, обеспечивая безопасность транзакций, аутентификацию и защиту от внешних атак. Шифрование используется для создания уникальных цифровых подписей и хэш-функций, которые подтверждают подлинность данных и предотвращают их подделку. Криптография в блокчейне также играет важную роль в обеспечении анонимности и приватности пользователей.

Наконец, следует отметить, что развитие квантовых вычислений представляет новые вызовы и возможности для криптографии. Квантовые компьютеры имеют потенциал взломать некоторые из существующих криптографических алгоритмов, основанных на сложности факторизации и дискретного логарифмирования. В этой связи проводятся исследования по разработке квантоустойчивых криптографических методов, которые будут способны обеспечить безопасность и в эпоху квантовых вычислений [5-7].

В итоге, криптография играет неотъемлемую роль в обеспечении информационной безопасности, обеспечивая конфиденциальность, целостность, подлинность и другие аспекты

защиты данных. Она применяется в различных областях и технологиях, от сетевой безопасности и защиты персональных данных до облачных вычислений и блокчейна. Однако важно постоянно развивать и совершенствовать криптографические методы, учитывая появление новых угроз и технологических прорывов.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. ИНТЕРНЕТ ВЕЩЕЙ (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукофера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. INTERNET OF THINGS (IoT): SECURITY AND PRIVACY THREATS //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N. A., Timofeev R. S. Comparison of training methods for convolutional neural networks //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.

6. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
 7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ПРОГНОЗИРОВАНИЕ СБОЕВ IoT-УСТРОЙСТВ ДЛЯ ГИБКОГО ПЛАНИРОВАНИЯ ИХ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

Романов Н.А.

ФГБОУ ВО Иркутский национальный исследовательский технический университет, Иркутск, Россия (664074, г. Иркутск, ул. Лермонтова, 83), e-mail: itsacool2014@gmail.com

В данной статье рассматриваются методологии прогнозирования сбоев IoT-устройств. В современном мире Интернет вещей (IoT) стал неотъемлемой частью нашей жизни, проникая в различные сферы, начиная от умного дома и заканчивая промышленностью и здравоохранением. В промышленной сфере выход таких устройств из строя несёт за собой дополнительные расходы, повышенные риски, поэтому задача прогнозирования является наиболее актуальной. Методология прогнозирования сбоев IoT-устройств позволяет повысить надежность и эффективность работы IoT-систем, а также оптимизировать планирование и проведение технического обслуживания. Применение данной методологии может способствовать предотвращению сбоев, минимизации простоев и улучшению качества обслуживания IoT-устройств, внося важный вклад в развитие и расширение IoT-технологий.

Ключевые слова: IoT, прогнозирование, выход из строя, промышленность, датчики, анализ, предсказание, предотвращение, обслуживание оборудования.

PREDICTING FAILURES OF IOT DEVICES FOR FLEXIBLE PLANNING OF THEIR MAINTENANCE

Romanov N.A.

Irkutsk national research technical university, Irkutsk, Russia (664074, Irkutsk, Lermontov str., 83), e-mail: itsacool2014@gmail.com

This article discusses the methodology for predicting failures of IoT devices. In the modern world, the Internet of Things (IoT) has become an integral part of our lives, penetrating into various spheres, from the smart home to industry and healthcare. In the industrial sphere, the failure of such devices entails additional costs, increased risks, so the task of forecasting is the most urgent. The methodology for predicting failures of IoT devices allows you to increase the reliability and efficiency of IoT systems, as well as optimize the planning and maintenance. The application of this methodology can contribute to the prevention of failures, minimize downtime and improve the quality of service of IoT devices, making an important contribution to the development and expansion of IoT technologies.

Keywords: IOT, prediction, failure, industry, sensors, analysis, prediction, prevention, equipment maintenance.

Сегодняшний мир стал свидетелем быстрого развития технологий, которое в значительной мере определяет наш образ жизни и способы взаимодействия с окружающим миром. Одной из самых влиятельных и инновационных технологий последнего времени является концепция интернета вещей (IoT). IoT представляет собой сеть физических устройств, взаимодействующих и обменивающихся данными через интернет без необходимости прямого участия человека. Эта технология перешагнула границы

традиционного компьютерного взаимодействия, расширяя сферу применения информационных технологий на различные объекты нашей повседневной жизни.

Роль IoT в современном мире стала неотъемлемой и разносторонней. IoT-устройства включают в себя все, начиная от умных домашних устройств, таких как умные термостаты, освещение и системы безопасности, и заканчивая сложными системами умных городов, медицинского оборудования, автономных автомобилей и промышленных систем управления. С помощью IoT, реальный мир становится неразрывно связанным с цифровым пространством, позволяя собирать, обрабатывать и анализировать огромные объемы данных из различных источников.

Одной из ключевых проблем, с которой сталкиваются пользователи IoT-устройств, является возникновение сбоев и отказов в их работе. Это может привести к серьезным последствиям, таким как нарушение нормального функционирования систем безопасности, снижение производительности и повреждение оборудования. Поэтому важно разработать методы, позволяющие прогнозировать сбои IoT-устройств, чтобы эффективно планировать их техническое обслуживание и предотвратить возможные проблемы.

Целью данной статьи является рассмотрение методов прогнозирования сбоев IoT-устройств с целью обеспечения гибкого планирования их технического обслуживания. Мы проведем обзор существующих исследований в этой области, проанализируем методологии и алгоритмы, применяемые для прогнозирования сбоев, и представим результаты экспериментов, демонстрирующие эффективность предложенного подхода.

Исследования в области прогнозирования сбоев IoT-устройств имеют важное практическое применение, способствуя повышению эффективности технического обслуживания и минимизации простоев. Результаты данного исследования могут быть полезны как для научного сообщества, так и для промышленности, заинтересованной в оптимизации управления IoT-устройствами.

Методы прогнозирования

Определение методов прогнозирования сбоев IoT-устройств является ключевым аспектом разработки эффективной системы обслуживания. Вот некоторые подробности о нескольких методах прогнозирования неисправностей IoT-устройств:

1. Методы временных рядов.

Методы временных рядов широко применяются для прогнозирования сбоев IoT-устройств. Они основаны на анализе исторических данных временных рядов, чтобы выявить временные закономерности и тренды в поведении устройств. Прогнозы строятся на основе статистических моделей, таких как авторегрессионные интегрированные скользящие средние (ARIMA) или авторегрессионные условные гетероскедастичные (ARCH) модели.

ARIMA (Autoregressive Integrated Moving Average) является одной из наиболее распространенных моделей временных рядов, применяемых для прогнозирования сбоев IoT-устройств. ARIMA модель сочетает в себе три компонента: авторегрессию (AR), интегрирование (I) и скользящее среднее (MA). Авторегрессия учитывает зависимость текущего значения ряда от предыдущих значений, интегрирование позволяет учитывать тренды и стационарность данных, а скользящее среднее учитывает зависимость от ошибок предыдущих прогнозов. Модель ARIMA может быть адаптирована к различным временным рядам путем настройки параметров модели [1].

ARCH (Autoregressive Conditional Heteroskedasticity) является моделью, используемой для моделирования и прогнозирования условной гетероскедастичности во временных рядах. В контексте прогнозирования сбоев IoT-устройств, ARCH модель может быть полезна для обнаружения и предсказания всплесков и колебаний в данных. ARCH модель предполагает, что дисперсия ошибок во временных рядах изменяется в зависимости от предыдущих ошибок, что позволяет учитывать и моделировать различные уровни волатильности [2].

Использование моделей ARIMA и ARCH в методологии прогнозирования сбоев IoT-устройств позволяет учитывать временные зависимости, тренды и условную гетероскедастичность в данных. ARIMA модель способна улавливать и моделировать сложные временные паттерны и поведение, а ARCH модель помогает обнаружить и предсказать возможные всплески или изменения в данных, связанные с сбоями устройств.

Комбинация моделей ARIMA и ARCH с другими методами временных рядов и алгоритмами машинного обучения может значительно улучшить точность и надежность прогнозирования сбоев IoT-устройств, особенно при анализе и прогнозировании временных рядов с переменной дисперсией и сложными зависимостями.

2. Методы машинного обучения.

Методы машинного обучения стали популярными в прогнозировании сбоев IoT-устройств благодаря своей способности обнаруживать сложные зависимости в данных. Эти методы могут использовать различные алгоритмы такие как случайный лес, градиентный бустинг, нейронные сети и методы обучения с подкреплением. Модели машинного обучения обучаются на исторических данных сбоев и их причин, чтобы предсказывать возможные неисправности в будущем. Ниже перечислены основные методы машинного обучения.

Регрессия: Методы регрессии используются для предсказания непрерывных числовых значений. Некоторые из наиболее популярных методов регрессии включают линейную регрессию, логистическую регрессию, полиномиальную регрессию и регрессию опорных векторов (SVR).

Классификация: Методы классификации применяются для разделения данных на заданные категории или классы. Некоторые популярные алгоритмы классификации включают метод ближайших соседей (k-Nearest Neighbors), наивный Байесовский классификатор, метод опорных векторов (SVM), решающие деревья и случайный лес [3].

Кластеризация: Методы кластеризации группируют схожие объекты вместе, не требуя заранее определенных категорий. Некоторые из наиболее распространенных алгоритмов кластеризации включают k-средних (k-Means), иерархическую кластеризацию, DBSCAN и алгоритмы гауссовской смеси.

Методы глубокого обучения: Глубокое обучение основано на искусственных нейронных сетях с несколькими слоями. Такие методы, как сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), генеративные состязательные сети (GAN) и рекуррентные сети долгой краткосрочной памяти (LSTM), являются мощными инструментами для обработки изображений, текстовых данных и последовательных данных[5].

Ансамблирование: Методы ансамблирования комбинируют прогнозы нескольких моделей, чтобы получить более точные предсказания. Некоторые популярные методы ансамблирования включают случайный лес, градиентный бустинг (Gradient Boosting) и метод бэггинга (Bagging), случайный лес (Random Forest) [1].

Обучение с подкреплением: Этот метод обучения на основе взаимодействия с окружающей средой. Агент принимает решения и выполняет действия, а затем получает награду или наказание в зависимости от результата. Некоторые алгоритмы обучения с подкреплением включают Q-обучение (Q-Learning) и методы глубокого обучения, такие как Deep Q-Networks (DQN).

Одним из мощных инструментов глубокого обучения, применяемых в этой области, является рекуррентная нейронная сеть, известная как LSTM (Long Short-Term Memory).

LSTM сети представляют собой вид рекуррентных нейронных сетей, способных эффективно обрабатывать последовательные данные с учетом долгосрочных зависимостей. Они особенно полезны при работе с временными рядами, где последовательность событий имеет важное значение. LSTM сети обладают способностью запоминать информацию на протяжении продолжительного временного интервала и выбирать, какую информацию сохранять и какую забывать. Это позволяет им лучше моделировать сложные временные зависимости и предсказывать возможные сбои IoT-устройств.

При применении LSTM в контексте прогнозирования сбоев IoT-устройств, модель может быть обучена на исторических данных о работе устройств и предсказывать возможные сбои в будущем. LSTM сети могут улавливать скрытые паттерны и зависимости, которые не всегда очевидны при использовании традиционных методов прогнозирования. Их способность учитывать долгосрочные зависимости делает их ценным инструментом для прогнозирования сбоев IoT-устройств.

Применение LSTM сетей в методологии прогнозирования сбоев IoT-устройств может существенно улучшить точность и надежность прогнозов, особенно в случаях, когда временные зависимости играют важную роль в процессе. Использование LSTM моделей позволяет более эффективно анализировать и предсказывать события сбоев, способствуя более гибкому и эффективному планированию технического обслуживания IoT-устройств [6].

3. Анализ аномалий.

Анализ аномалий используется для обнаружения и предсказания необычных или отклоняющихся от нормы событий или состояний устройств. Он основан на выявлении аномалий в данных и анализе их связи с возможными сбоями. Алгоритмы анализа аномалий могут использовать методы статистики, машинного обучения или комбинированные подходы для обнаружения неисправностей.

Применение датчиков и диагностических данных:

Использование данных от датчиков и систем диагностики IoT-устройств позволяет отслеживать параметры работы и выявлять изменения, которые могут указывать на возможные сбои. Анализ этих данных может включать мониторинг параметров, распределение данных, изменение показателей производительности и другие характеристики, чтобы предсказывать неисправности и определить оптимальное время для технического обслуживания.

Каждый из этих методов имеет свои преимущества и ограничения, и оптимальный выбор зависит от конкретных требований, доступных данных и особенностей конкретного IoT-устройства или системы. Эффективное прогнозирование сбоев IoT-устройств может быть достигнуто путем комбинации различных методов и использования специализированных моделей, учитывая особенности конкретной проблемы и доступные данные.

Описание методологии прогнозирования сбоев IoT-устройств

Прогнозирование сбоев IoT-устройств является сложной задачей, требующей систематического подхода и использования соответствующих методов. В данной статье предлагается методология прогнозирования сбоев IoT-устройств, основанная на комбинации статистических методов и алгоритмов машинного обучения. Эта методология позволяет эффективно предсказывать возможные неисправности и принимать соответствующие меры по техническому обслуживанию.

Шаг 1: Сбор и предварительная обработка данных

В первом шаге методологии осуществляется сбор и предварительная обработка данных, связанных с работой IoT-устройств. Это может включать в себя сбор и агрегацию данных от датчиков, систем диагностики и журналов событий. Важно провести необходимую предварительную обработку данных, включая очистку от выбросов, заполнение пропущенных значений и приведение данных к подходящему формату.

Шаг 2: Анализ и визуализация данных

После предварительной обработки данных следует провести анализ и визуализацию, чтобы получить представление о характеристиках и паттернах работы IoT-устройств. Это может включать в себя анализ статистических показателей, построение графиков, временных рядов и корреляционного анализа. Цель этого шага - выявить особенности и тренды в данных, которые могут указывать на возможные сбои.

Шаг 3: Выбор и разработка моделей прогнозирования

На основе анализа данных выбираются и разрабатываются подходящие модели прогнозирования сбоев IoT-устройств. Это может включать статистические модели, такие как модели временных рядов (например, ARIMA), или алгоритмы машинного обучения, такие как случайные леса, градиентный бустинг или нейронные сети. Модели обучаются на исторических данных и настраиваются с использованием соответствующих алгоритмов.

Шаг 4: Валидация и тестирование моделей

Для оценки эффективности моделей проводится их валидация и тестирование. Это включает разделение данных на обучающую и тестовую выборки, обучение моделей на обучающих данных и проверку их точности и производительности на тестовых данных. Важно использовать метрики, такие как точность, полнота, F1-меру или среднюю абсолютную ошибку, для оценки качества моделей.

Шаг 5: Реализация и интеграция

После успешной валидации моделей прогнозирования, их необходимо реализовать и интегрировать в систему IoT-устройств. Это может включать разработку программного обеспечения для автоматического мониторинга и прогнозирования сбоев, настройку системы уведомлений или интеграцию с системами управления обслуживанием.

Методология прогнозирования сбоев IoT-устройств позволяет повысить эффективность технического обслуживания и минимизировать простои. Однако, следует отметить, что конкретная реализация методологии может различаться в зависимости от особенностей конкретного проекта и доступных ресурсов.

Список литературы

1. Андрюхин Е.В., Ридли М.К., Правиков Д.И. Прогнозирование сбоев и отказов в распределённых системах управления на основе моделей прогнозирования временных

- рядов // Вопросы кибербезопасности, 2019, №3. С. 24–32. техн. ун-т им. Н.Э. Баумана Москва, 2012. 154 с
2. Шаханов Н.И., Варфоломеев И.А., Ершов Е.В., Юдина О.В. Прогнозирование отказов оборудования в условиях малого количества поломок// Вестник Череповецкого государственного университета, 2016, № 6.С. 36–41.
 3. Имильбаев Р. Р. Методы и алгоритмы прогнозирования значений контролируемых параметров газораспределительной сети по результатам обработки телеметрической информации: дис. канд. техн. наук: Уф. гос. нефт. техн. ун-т Уфа, 2018. 152 с.
 4. Saxena A., Goebel K. Damage propagation modeling for aircraft engine run-to-failure simulation. // 2008 International Conference on Prognostics and Health Management, Denver, CO. 2008. pp. 1–9.
 5. Tibshirani R. J. Regression shrinkage and selection via the lasso // Journal of the Royal Statistical Society. Series B (Methodological), 1996. Vol. 58, No. 1. pp. 267–288.
 6. Hochreiter S. The vanishing gradient problem during learning recurrent neural nets and problem solutions // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 1998. Vol. 6, No 2. pp. 107–116.

References

1. Andriukhin E.V., Ridley M.K., Pravikov D.I. Forecasting failures and failures in distributed control systems based on time series forecasting models // Issues of cybersecurity, 2019, No. 3. pp. 24-32. tech. Bauman Univ., Moscow, 2012. P.154
 2. Shakhonov N.I., Varfolomeev I.A., Ershov E.V., Yudina O.V. Prediction of equipment failures in conditions of a small number of breakdowns// Bulletin of Cherepovets State University, 2016, No. 6.pp. 36-41.
 3. Imelbaev R. R. Methods and algorithms for predicting the values of controlled parameters of the gas distribution network based on the results of processing telemetric information: dis. Candidate of Technical Sciences: Uv. state Oil. tech. Ufa University, 2018. 152 p.
 4. Saxena A., Goebel K. Damage propagation modeling for aircraft engine run-to-failure simulation. // 2008 International Conference on Prognostics and Health Management, Denver, CO. 2008. pp. 1–9.
 5. Tibshirani R. J. Regression shrinkage and selection via the lasso // Journal of the Royal Statistical Society. Series B (Methodological), 1996. Vol. 58, No. 1. pp. 267–288.
 6. Hochreiter S. The vanishing gradient problem during learning recurrent neural nets and problem solutions // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 1998. Vol. 6, No 2. pp. 107–116.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 62

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПРЕДЕЛЕНИЯ КООРДИНАТ СТАНЦИИ

¹Хамидулин Д.М., Войкин А.О., Муханова Р.Е., Григорьев Д.О.

ФГБОУ ВО Новосибирский Государственный архитектурно-строительный университет, Новосибирск, Россия (630008, г.Новосибирск, Ленинградская ул., 113), e-mail:

¹d.khamidulin@sibstrin.ru

В данной статье мы рассмотрели прямую и обратную угловые засечки, где измерение были совершены Теодолитом Theo 010 и Электронным тахеометром Trimble M3 DR5. Также была произведена оценка точности измерений двух приборов для каждой из видов засечек, а также произведено сравнение результатов определения координат станции теодолитом и электронным тахеометром.

Ключевые слова: Прямая угловая засечка, обратная угловая засечка, оценка точности, теодолит Theo 010, электронный тахеометр Trimble M3 DR5.

MATHEMATICAL MODEL FOR DETERMINING STATION COORDINATES

¹Khamidulin D.M., Voikin A.O., Mukhanova R.E., Grigoriev D.O.

Novosibirsk State University of Architecture and Civil Engineering, Novosibirsk, Russia (630008, Novosibirsk, Leningradskaya str., 113), e-mail: ¹d.khamidulin@sibstrin.ru

In this article, we examined the forward and reverse angular serifs, where the measurement was made by The Theo 010 Theodolite and the Trimble M3 DR5 Electronic total station. The accuracy of measurements of two devices for each of the types of serifs was also evaluated, and the results of determining the coordinates of the station with a theodolite and an electronic total station were compared.

Keywords: Forward angular serif, reverse angular serif, accuracy estimation, theodolite Theo 010, Trimble M3 DR5 electronic total station.

Проблема: найти наиболее оптимальный способ измерений и при этом точный для проведения геодезических работ.

Решение проблемы: определить каким способом точность определения координат будет наибольшей, а также способ, который по трудоемкости уступает другому из двух рассматриваемых.

Актуальность: при производстве геодезических работ на строительных площадках важной частью является определение координат станции.

Цель: сравнение способов определения координат станции прямой и обратной угловой засечкой.

Задачи:

1. изучить способы определения координат станции;
2. для прямой угловой засечки измерить горизонтальные углы теодолитом Theo 010 и электронным тахеометром Trimble M3 DR5;

3. построить графики изменения горизонтальных углов;
4. вычислить координаты станции по результатам измерения углов теодолитом и тахеометром;
5. для обратной угловой засечки измерить горизонтальные углы теодолитом Theo 010 и электронным тахеометром Trimble M3 DR5;
6. вычислить координаты станции по результатам измерения углов теодолитом и тахеометром;
7. выполнить оценку точности.

Способы определения координат станции:

- Прямая геодезическая засечка
- Обратная геодезическая засечка
- Комбинированная
- Линейная геодезическая засечка и т.д.

На начальном этапе исследования нас интересовало определить какие существуют способы определения координат станции. В конечном счете на двух интересных из них. Это непосредственно прямая и обратная геодезическая засечки, так как это популярные способы нахождения координат точек, расстояния между ними и дирекционного угла на местности. Остановимся подробнее на каждой из засечек.

Прямая геодезическая засечка — это способ определения координат недоступной точки (рисунок 1). Суть этого метода состоит в том, что сначала выбирают две базовые точки, у которых известны координаты, а затем измеряется угол между прямой, проходящей через эти точки, и наблюдаемой линией визирования, направленной на исследуемую точку [1].

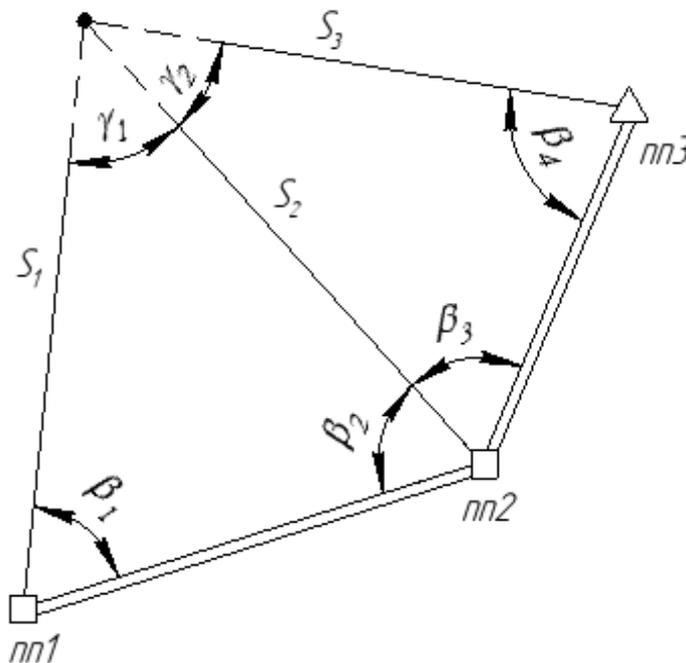


Рисунок 1 – Прямая геодезическая засечка

Для прямой геодезической засечки применяется специальный оптический инструмент – теодолит или электронный тахеометр. С его помощью измеряется угол между базовыми точками и вертикальной плоскостью, проходящей через исследуемую точку. Определение

угла позволяет определить расстояние от базовых точек до исследуемой точки. Затем, используя тригонометрические формулы, можно рассчитать географические координаты исследуемой точки.

Прямая геодезическая засечка - один из наиболее точных методов определения координат точек и используется в различных областях геодезии, например, в строительстве, картографии, геодезии и геоинформатике.

Обратная геодезическая засечка — это способ определения координат недоступной точки (рисунок 2) путем измерения горизонтальных углов между геодезическими пунктами [2].

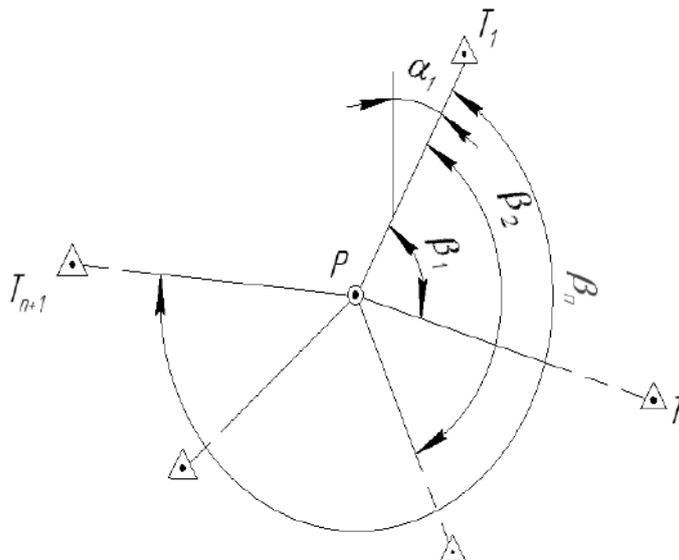


Рисунок 2 – Обратная геодезическая засечка

Суть обратной геодезической засечки заключается в том, что изначально известны координаты одной из точек, а также направления и расстояния до второй точки. Используя эти данные, можно определить координаты второй точки. Это позволяет геодезистам и строителям точно вычислять расстояния и направления для строительства дорог, мостов, зданий и других объектов на земле [3].

Приборы, необходимые при решении засечек:

Далее нас интересовало, а какими именно приборами выполнять измерения, чтобы потом не только рассмотреть способы определения координат, но и в конце определить оценку точности? В конечном итоге остановились на двух: теодолит Theo 010 (рисунок 3) и электронный тахеометр Trimble M3 DR5 (рисунок 4).



Рисунок 3 – Теодолит Theo 010
Погрешность: $m\beta = 10''$



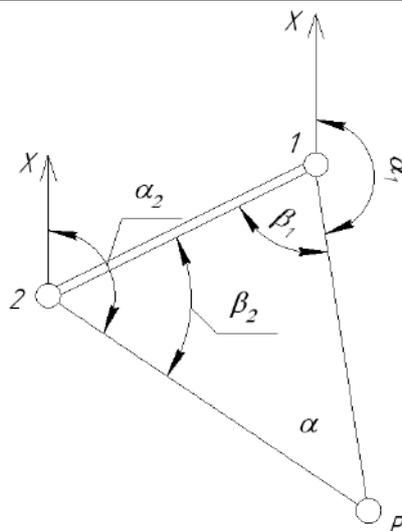
Рисунок 4 – Электронный тахеометр Trimble M3 DR5
Погрешность: $m\beta = 5''$

Исходные данные для решения прямой засечки теодолитом:

В процессе нашей работы мы выполнили по 10 измерений горизонтальных углов для решения прямой засечки теодолитом (рисунок 5). Где за точку Р мы приняли отражатель над дверью, а за точки 1 и 2 мы приняли 8 и 4 столбы в аудитории. Координаты столбов были получены заранее электронным тахеометром в условной системе координат $X_1=115,475$ м, $Y_1=100,000$ м, $X_2=114,588$ м, $Y_2=104,400$ м.

Таблица 1 – Результаты измерений горизонтальных углов теодолитом прямой геодезической засечки

№ п/п	β_1			β_2		
	°	'	''	°	'	''
1	12	56	37	153	50	2
2	12	56	35	153	50	0
3	12	56	43	153	50	21
4	12	56	42	153	50	32
5	12	56	48	153	50	3
6	12	56	42	153	50	2
7	12	56	58	153	50	5
8	12	56	31	153	50	8
9	12	56	58	153	50	9
10	12	56	50	153	50	19
Среднее значение	12	56	44	153	50	8



Риснок 5 – К решению прямой засечки

Графики изменения горизонтальных углов

Как показано на графиках, мы видим, что они детально показывают изменение углов β_1 (рисунок 6) и β_2 (рисунок 7) при 10 измерений. Черная линия показывает среднее значение каждого из углов, которое подписано над графиками.

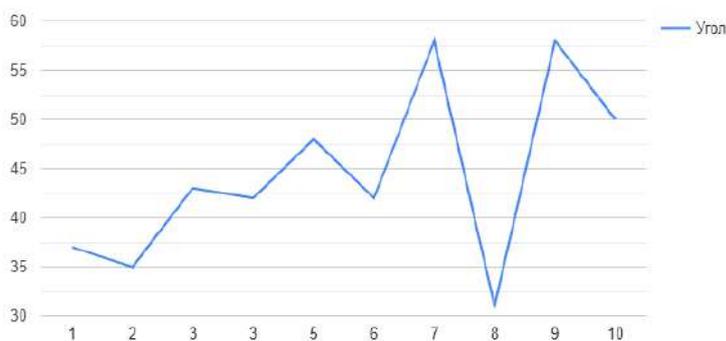


Рисунок 6 – График изменения горизонтального угла β_1

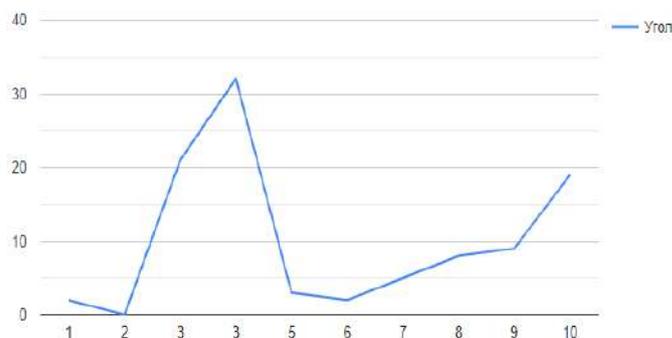


Рисунок 7 – График изменения горизонтального угла β_2

Решение прямой геодезической засечки по формулам Юнга с применением теодолита:

$$X_p = \frac{x_1 * \cot \beta_2 + x_2 * \cot \beta_1 - y_1 - y_2}{\cot \beta_1 + \cot \beta_2} \quad (1)$$

$$Y_p = \frac{y_1 * \cot \beta_2 + y_2 * \cot \beta_1 + x_1 - x_2}{\cot \beta_1 + \cot \beta_2}$$

Таблица 2 – Результаты вычисленных координат точки Р прямой геодезической засечки

№ п/п	Xp	Yp
1	73,430	103,640
2	73,431	103,641
3	73,418	103,641
4	73,415	103,645
5	73,421	103,641
6	73,422	103,640
7	73,401	103,650
8	73,431	103,641
9	73,430	103,642
10	73,420	103,642
Среднее значение	73,422	103,642

Вычисленные нами β_1 и β_2 послужили для нахождения x_p и y_p по формуле Юнга, которая находится выше. Таким образом, мы произвели 10 вычислений координат станции Р и определили среднее значение.

Исходные данные для решения прямой засечки электронным тахеометром:

Такой же идеей решения мы произвели вычисления электронным тахеометром. Построили графики, на которых красной линией отмечено среднее значения углов. Далее вычислили 10 раз каждую из координат и нашли средние значения, также сделали таблицу сравнения координат x_p и y_p для двух приборов (таблица 3).

Решение прямой геодезической засечки по формулам Юнга с применением электронного тахеометра (таблица 4).

Сравнение результатов определения координат станции теодолитом и электронным тахеометром (таблица 5).

Проведя практические измерения, мы получили разницу по $x_p = 0,013\text{м}$ и по $y_p = 0,002\text{м}$.

Оценка точности результатов для прямой засечки: если известна средняя квадратическая ошибка измерения горизонтальных углов m''_β , то тогда погрешность в положении определяемой точки Р вычисляется по формуле:

$$M_p = \frac{b * m''_\beta}{p'' * \sin \gamma} * \sqrt{\sin^2 \beta_1 + \sin^2 \beta_2}, \quad (2)$$

где $b = d_{A-B}$ – базис засечки; $p'' = 206265$ – число радиан в секундах; m''_β – средняя квадратичная погрешность измерения горизонтальных углов; γ – угол при вершине засечки $180^\circ - (\beta_1 + \beta_2)$ (таблица 6).

Таблица 3 – Результаты измерений горизонтальных углов электронным тахеометром прямой геодезической засечки

№ п/п	β1			β2		
	°	'	''	°	'	''
1	12	56	44	153	50	30
2	12	56	36	153	50	35
3	12	56	42	153	50	27
4	12	56	37	153	50	41
5	12	56	40	153	50	29
6	12	56	46	153	50	33
7	12	56	52	153	50	21
8	12	56	39	153	50	28
9	12	56	42	153	50	31
10	12	56	41	153	50	34
Среднее значение	12	56	42	153	50	31

Таблица 4 – Результаты вычисленных координат точки Р прямой геодезической засечки

№ п/п	X _p	Y _p
1	73,408	103,642
2	73,412	103,639
3	73,411	103,641
4	73,409	103,640
5	73,412	103,640
6	73,405	103,642
7	73,405	103,643
8	73,413	103,640
9	73,409	103,631
10	73,409	103,641
Среднее значение	73,409	103,640

Таблица 5 – Разница результатов координат точки Р на двух приборах

Прибор	X _p , м	Y _p , м
Теодолит Theo 010	73,422	103,642
Электронный тахеометр Trimble M3	73,409	103,640
Разница	0,013	0,002

Таблица 6 – Результаты погрешности выдаваемый каждым прибором

Значение средней квадратичной погрешности определяемой M_p , м	
Теодолит	0,03
Электронный тахеометр	0,02

Подводя итоги для прямой засечки, можно уже сказать, что средняя квадратичная погрешность по теодолиту равняется 0,03 и электронному тахеометру 0,02. Разница между приборами составляет 0,01, что является допустимым.

Исходные данные для решения обратной угловой засечки теодолитом:

Теперь выполняем все таким же принципом только обратной угловой засечкой. Для начала мы выполнили по 10 измерений горизонтальных углов. Измерения мы проводили в аудитории, измеряя горизонтальные углы на искомой точке Р между направлениями на три пункта.

Таблица 7 – Результаты измерений горизонтальных углов теодолитом обратной геодезической засечки

№ п/п	β_1			β_2		
	°	'	''	°	'	''
1	16	46	36	198	55	15
2	16	46	39	198	55	25
3	16	46	35	198	55	10
4	16	46	43	198	55	11
5	16	46	44	198	55	18
6	16	46	46	198	55	22
7	16	46	44	198	55	29
8	16	46	40	198	55	40
9	16	46	36	198	55	9
10	16	46	46	198	55	42
Среднее значение	16	46	42	198	55	22

Решение обратной геодезической засечки по формулам Деламбра с применением теодолита:

Таблица 8 – Результаты вычисленных координат точки Р обратной геодезической засечки

№ п/п	X _p	Y _p
1	99,992	99,997
2	99,988	99,998
3	100,023	99,997
4	99,990	99,998
5	99,992	99,998
6	99,999	99,989
7	99,993	99,999
8	99,987	99,999
9	99,990	99,998
10	99,989	99,997
Среднее значение	99,994	99,997

$$\tan \alpha_{1-p} = \frac{(y_2 - y_1) \cot \beta_1 + (y_1 - y_3) \cot \beta_2 - x_2 + x_3}{(x_2 - x_1) \cot \beta_1 + (x_1 - x_3) \cot \beta_2 + y_2 - y_3} = \frac{\Delta y}{\Delta x};$$

$$\alpha_{2-p} = \alpha_{1-p} + \beta_1; \alpha_{3-p} = \alpha_{1-p} + \beta_2; \alpha_{4-p} = \alpha_{1-p} + \beta_3; \quad (3)$$

$$X_p = \frac{x_1 \tan \alpha_{1-p} - x_2 \tan \alpha_{2-p} + y_2 - y_1}{\tan \alpha_{1-p} - \tan \alpha_{2-p}};$$

$$y_p = y_1 + (x_p - x_1) \tan \alpha_{1-p} = y_2 + (x_p - x_2) \tan \alpha_{2-p}$$

Вычисленные нами β_1 и β_2 послужили для нахождения x_p и y_p по формуле Деламбра, которая находится выше. Таким образом, мы произвели 10 вычислений координат станции Р и определили среднее значение.

Исходные данные для решения обратной угловой засечки электронным тахеометром:

Измерения, которые были совершены в обратной угловой засечке теодолитом будут выполнены электронным тахеометром и занесены в соответствующие таблицы.

Таблица 9 – Результаты измерений горизонтальных углов электронным тахеометром обратной геодезической засечки

№ п/п	β_1			β_2		
	°	'	''	°	'	''
1	16	46	53	198	55	47
2	16	46	57	198	55	2
3	16	46	49	198	55	19
4	16	46	49	198	55	23
5	16	46	54	198	55	17
6	16	46	53	198	55	14
7	16	46	57	198	55	15
8	16	46	50	198	55	12
9	16	46	55	198	55	8
10	16	46	39	198	55	6
Среднее значение	16	46	52	198	55	16

Решение обратной геодезической засечки по формулам Деламбра с применением электронного тахеометра:

Таблица 10 – Результаты вычисленных координат точки Р обратной геодезической засечки

№ п/п	Xp	Yp
1	99,994	99,999
2	99,994	99,997
3	99,993	99,995
4	100,003	100,001
5	100,004	100,001
6	100,005	100,001
7	100,002	99,999
8	100,002	100,002
9	100,002	100,001
10	100,008	99,999
Среднее значение	100,001	99,999

По формуле были совершены вычисления с β_1 и β_2 для нахождения x_p и y_p для последующего нахождения средних значений.

Сравнение результатов определения координат станции теодолитом и электронным тахеометром:

Теперь мы сравнили результаты определения координат станции теодолитом и электронным тахеометром для обратной засечки и в результате получили разницу координат станции Р измеренных двумя приборами. Разница составила 7 мм и 2 мм соответственно.

Таблица 11 – Разница результатов координат точки Р на двух приборах

Прибор	Xp, м	Yp, м
Теодолит Theo 010	99,994	99,997
Электронный тахеометр Trimble M3	100,001	99,999
Разница	0,007	0,002

Оценка точности результатов для обратной засечки:

Расчет средней квадратической погрешности определяемой точки Р в обратной угловой засечке осуществляется по указанной формуле, с обозначением всех параметров, входящих в нее на рисунке 8.

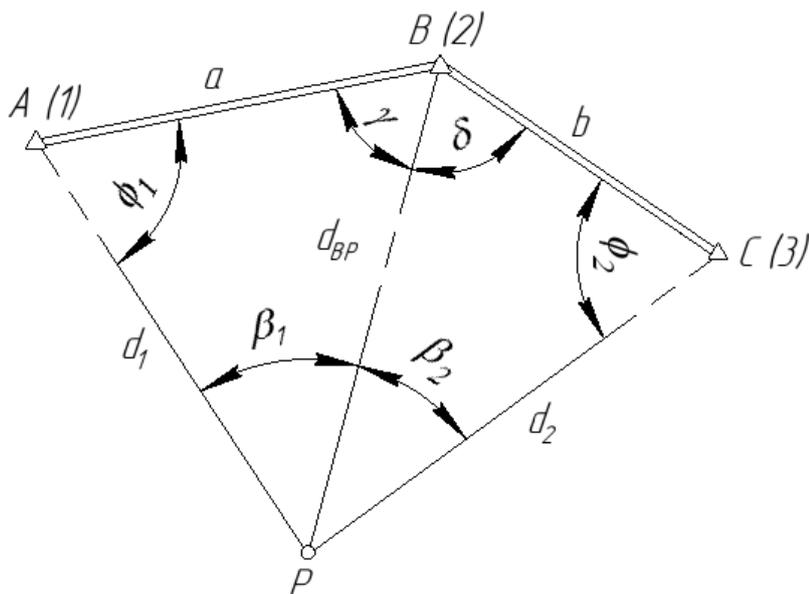


Рисунок 8 – Обратная геодезическая засечка

$$M_p = \frac{d_{BP} * m''_{\beta}}{p'' \sin(\varphi_1 + \varphi_2)} \sqrt{\frac{d_1^2}{a^2} + \frac{d_2^2}{b^2}} \quad (4)$$

Углы φ_1 и φ_2 вычисляются путем геометрических преобразований; d_1, d_2, d_{BP}, a, b – определяются путем решения обратной геодезической задачи

Таблица 12 – Результаты погрешности выдаваемый каждым прибором

Значение средней квадратичной погрешности определяемой M_p , м	
Теодолит	0,04
Электронный тахеометр	0,01

Оценка точности наглядно показала, что погрешность теодолита и электронного тахеометра для задачи обратная угловая засечка равняется 0,04м и 0,01м соответственно.

Заключение: в результате изучения был получен материал, анализ которого позволил заключить, что применение прямой и обратной угловой засечки с использованием теодолита или электронного тахеометра дает практически идентичные результаты при погрешности для прямой засечки: 0,03 и 0,02 и для обратной засечки: 0,04 и 0,01. Применение метода определения координат станции обратной угловой засечкой является более предпочтительным поскольку полевые измерения проводятся в данном случае на одной точке.

Методология прогнозирования сбоев IoT-устройств позволяет повысить эффективность технического обслуживания и минимизировать простои. Однако, следует отметить, что конкретная реализация методологии может различаться в зависимости от особенностей конкретного проекта и доступных ресурсов.

Список литературы

1. Прямая и обратная геодезические задачи [Электронный ресурс]. – URL: <https://mylektsii.ru/1-103759.html> (Дата обращения: 23.04.2023).

2. StudFiles [Электронный ресурс]. – URL: <https://studfile.net/preview/4405175/> (Дата обращения: 20.05.2023).
3. Промтерра [Электронный ресурс]. – URL: <https://www.prom-terra.ru/articles/chto-takoe-obratnaya-i-pryamaya-geodezicheskaya-zadacha-sut-metody-resheniya-naznachenie.html> (Дата обращения: 03.05.2023)
4. «topuch» [Электронный ресурс]. – URL: <https://topuch.com/pryamaya-geodezicheskaya-uglovaya-zasechka/index.html> (Дата обращения: 15.05.23)
5. «2CAD» [Электронный ресурс]. – URL: <https://2cad.ru/blog/geodesy/obratnay-zasechka/> (Дата обращения: 23.05.2023).

References

1. Pryanaya i obratnaya geodezicheskie zadachi [Elektronnyj resurs]. – URL: <https://mylektsii.su/1-103759.html> (Data obrashcheniya: 23.04.2023).
 2. StudFiles [Elektronnyj resurs]. – URL: <https://studfile.net/preview/4405175/> (Data obrashcheniya: 20.05.2023).
 3. Promterra [Elektronnyj resurs]. – URL: <https://www.prom-terra.ru/articles/chto-takoe-obratnaya-i-pryamaya-geodezicheskaya-zadacha-sut-metody-resheniya-naznachenie.html> (Data obrashcheniya: 03.05.2023)
 4. «topuch» [Elektronnyj resurs]. – URL: <https://topuch.com/pryamaya-geodezicheskaya-uglovaya-zasechka/index.html> (Data obrashcheniya: 15.05.23)
 5. «2CAD» [Elektronnyj resurs]. – URL: <https://2cad.ru/blog/geodesy/obratnay-zasechka/> (Data obrashcheniya: 23.05.2023).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ МАШИННОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ДОКУМЕНТОВ ГОСУДАРСТВЕННЫХ ЗАКУПОК

Евстифеев И.А.

ФГБОУ ВО Самарский государственный технический университет, Самара, Россия (443010, г. Самара, Молодогвардейская ул., 244.), e-mail: il.evs@yandex.ru

В данной статье будет произведена попытка разработки алгоритма, который автоматически будет классифицировать документы государственных закупок по ОКПД2 кодам. Это позволит значительно упростить и ускорить процесс анализа закупок, а также повысить эффективность мониторинга государственных закупок. Для достижения этой цели здесь будут использоваться методы машинного обучения, алгоритмы классификации. Так же будет проведен анализ различных методов предобработки данных, чтобы определить наиболее эффективные способы обработки информации. В итоге, результаты этой работы могут быть применены в различных областях, связанных с государственными закупками, включая анализ и оптимизацию бюджетных расходов, мониторинг конкуренции на рынке, а также принятие решений при выборе поставщиков товаров и услуг.

Ключевые слова: алгоритмы классификации, государственные закупки, ОКПД2 код, методы предобработки данных.

PROSPECTS FOR USING MACHINE LEARNING TO CLASSIFY PUBLIC PROCUREMENT DOCUMENTS

Evstifeev I.A.

Samara State Technical University, Samara, Russia (443010, Samara, Molodogvardeyskaya str., 244), e-mail: il.evs@yandex.ru

In this article, an attempt will be made to develop an algorithm that will automatically classify public procurement documents by OKPD2 codes. This will significantly simplify and speed up the procurement analysis process, as well as improve the effectiveness of public procurement monitoring. To achieve this goal, machine learning methods and classification algorithms will be used here. The analysis of various data preprocessing methods will also be carried out to determine the most effective ways of processing information. As a result, the results of this work can be applied in various areas related to public procurement, including analysis and optimization of budget expenditures, monitoring of competition in the market, as well as decision-making when choosing suppliers of goods and services.

Keywords: classification algorithms, public procurement, OKPD2 code, data preprocessing methods.

Цель работы

Цель данной работы заключается в разработке алгоритма классификации документов государственных закупок по видам экономической деятельности с использованием Общероссийского классификатора продукции по видам экономической деятельности (ОКПД2) кодом. Это позволит автоматизировать и упростить процесс анализа закупок, а также повысить эффективность мониторинга государственных закупок. Для достижения этой цели в

работе будут использоваться методы машинного обучения, включая нейронные сети и алгоритмы классификации, а также проводиться анализ различных методов предобработки данных, чтобы определить наиболее эффективные способы обработки информации. Результаты работы могут быть применены в различных областях, связанных с государственными закупками.

Задачи

1. Сбор и анализ данных о государственных закупках, включая информацию о товарах и услугах, их стоимости, дате заключения контрактов, наименовании заказчиков и исполнителей.
2. Предобработка данных, включая очистку, нормализацию, токенизацию и лемматизацию текстовых данных, а также преобразование числовых данных в удобный для анализа формат.
3. Построение модели классификации, включая выбор подходящих алгоритмов и методов машинного обучения, настройку гиперпараметров и оценку качества модели.
4. Анализ результатов классификации, включая оценку точности, полноты, F-меры и других метрик качества, а также исследование влияния различных методов предобработки данных на результаты классификации.
5. Разработка программного обеспечения для автоматической классификации документов государственных закупок по ОКПД2 кодам.
6. Проведение экспериментального исследования, включающего тестирование программного обеспечения на реальных данных о государственных закупках и сравнение результатов классификации с результатами, полученными при использовании других методов классификации.
7. Выводы и рекомендации по дальнейшему развитию и применению разработанного алгоритма классификации в различных областях, связанных с государственными закупками.

Методы

Некоторые методы, которые могут быть применены в рамках данной статьи, были описаны в моем предыдущей главе. Здесь я предоставлю более конкретный список методов и источников, которые могут быть полезны при работе над этой темой:

- Методы машинного обучения для классификации текстовых данных:
- [1] [2] [3]
- Методы предобработки текстовых данных: [4] [5]
- Методы визуализации данных: [6]
- Методы обработки естественного языка: [7]
- Методы оптимизации гиперпараметров: [8] [9]
- Методы метрической оценки: [10] [11]
- Методы при решении задач в области государственных закупок:
- [12] [13] [14]

Описание доменной области

ОКПД2 код – структура, показывающая принадлежность договора к определённому типу товара или услуги. Примеры целевых классов представлены таблице 1:

Таблица 1 – Структура ОКПД2 кода

Глубина кодировки	Тип	Пример кода	Значение кода
XX	Класс	14	одежда
XX.X	Подкласс	14.1	одежда, кроме одежды из меха
XX.XX	Группа	14.13	одежда верхняя прочая
XX.XX.X	Подгруппа	14.13.3	одежда верхняя прочая женская или для девочек
XX.XX.XX	Вид	14.13.34	платья, юбки и юбки-брюки женские или для девочек из текстильных материалов, кроме трикотажных или вязаных
XX.XX.XX.XX	Категория		
XX.XX.XX.XXX	Подкатегория	14.13.34.110	платья женские или для девочек из текстильных материалов, кроме трикотажных или вязаных

Конвейер сервиса

Сбор ссылок на документы

Для сбора сырых данных был определен источник данных - в данном случае это была веб-страница с необходимыми данными, размещенная на портале [15] с собранными в одном месте json со ссылками на документы и ОКПД2 кодами.

Для веб-страницы был создан отдельный запрос, который позволял получить нужные данные из HTML-кода страницы. Для этого была использована библиотека BeautifulSoup, которая позволяет парсить HTML-код и извлекать нужные элементы, в нашем случае это ссылки на архивы с JSON. Также была использована библиотека Requests, которая позволяет отправлять HTTP-запросы на сервер и получать ответы.

После того, как была собрана информация с веб-страницы, ссылки на документы и ОКПД2-коды были преобразованы и сохранены в файл формата CSV. Данный формат был выбран из-за его удобства (есть возможность добавлять записи в параллельном режиме) для дальнейшей обработки и анализа.

Таким образом, метод сбора сырых данных на основе сбора веб-страниц с использованием Python-библиотек позволяет собирать большое количество данных за короткий промежуток времени и обеспечивает удобство для дальнейшей обработки и анализа данных.

Сбор данных документов

Из исходного CSV извлекаются ссылки на документы, затем определяется формат документа "на лету". В данном процессе существует проблема того, что документы могут являться архивами, что затрудняет извлечения текста из этих файлов. Поэтому для упрощения на данном этапе принято использовать только doc, docx, pdf форматы. Файлы выгружаются в отдельную папку.

Сбор данных из документов

После сбора документов в форматах doc, docx, pdf - необходимо получить текст из них. На практике при сборе данных могут возникнуть трудности, когда текст не представлен в виде символов, а изображениями. Для решения данной проблемы достаточно простым, удобным, быстрым в реализации инструментом является textract. В этой библиотеке можно выбрать OCR-библиотека tesseract, она достаточно точно решает эту проблему.

Предобработка данных

Прежде чем приступить к классификации документов, следует выполнить подготовительную работу с данными. Целью предобработки является избавление семплов от выбросов и нормализация текста.

Обучение модели

Для обучения модели используется fasttext. Этот алгоритм достаточно нетребователен к ресурсам и выполняется достаточно быстро, а так же хорошо масштабируется.

Архитектура приложения

Описав выше все программы, присутствующие в данном приложении – построим схему его архитектуры на рисунке 1.

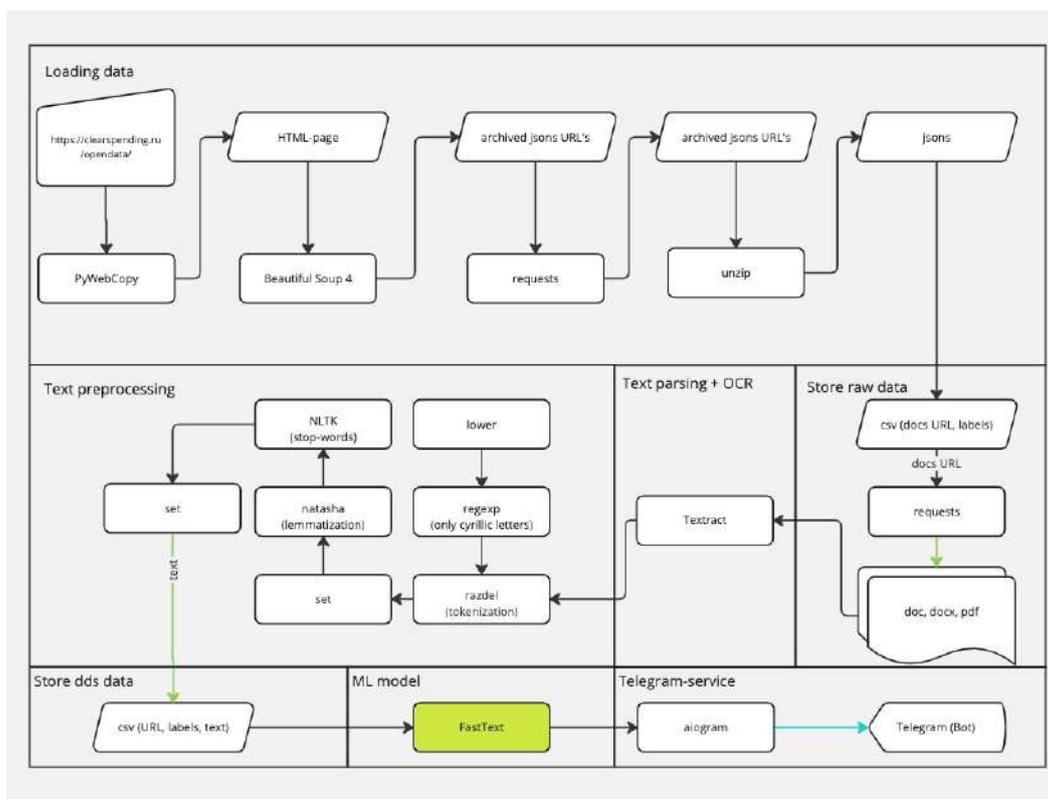


Рисунок 1 – Архитектура приложения

Скриншоты экранных форм

Приведём пример использования чат-бота в Telegram со вводом текста в сообщении на рисунке 2. Так же доступна подача данных документами.

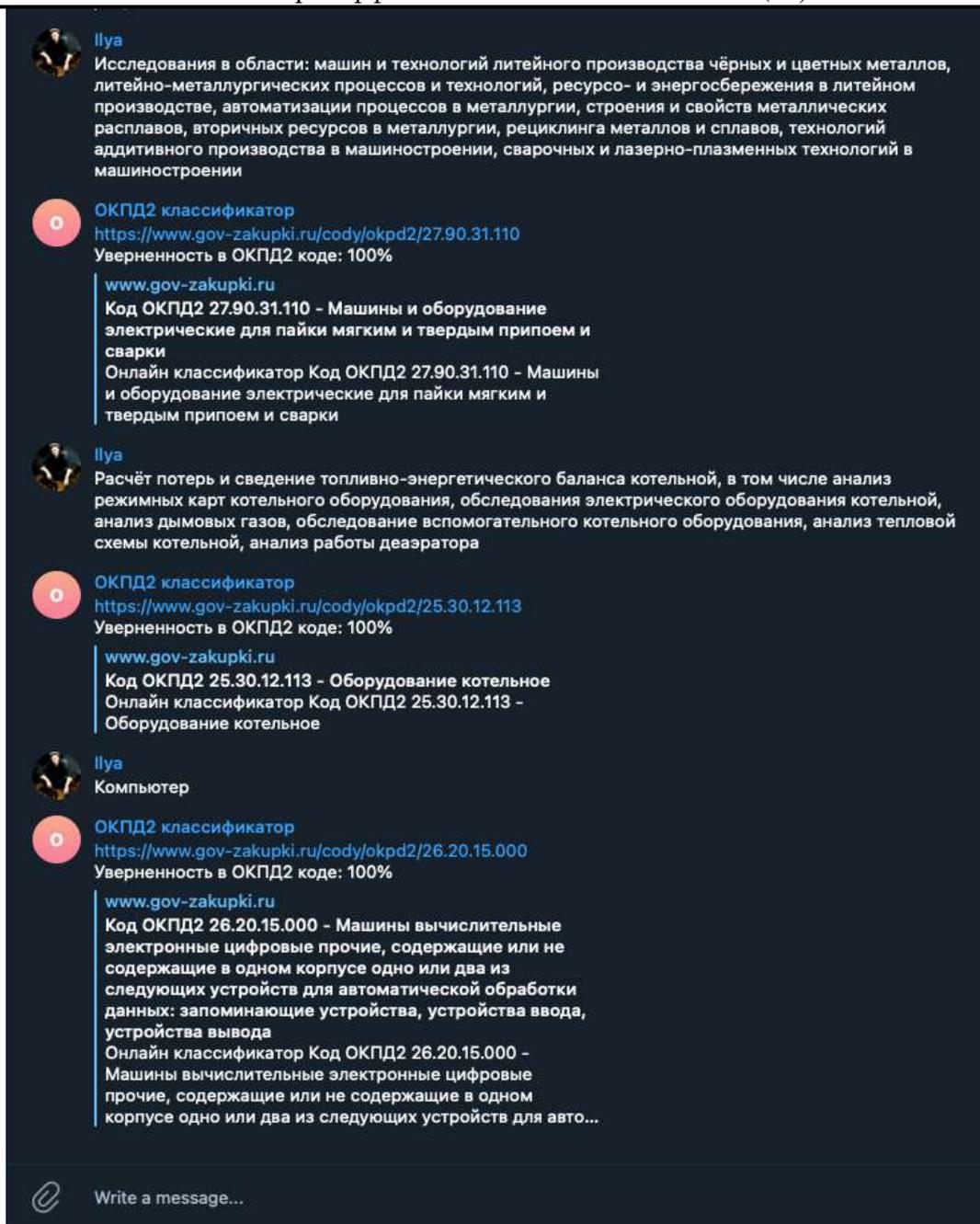


Рисунок 2 – Скриншот экранной формы

Результаты опытных испытаний

При сборе ссылок на документы получено порядка 30гб сырых json файлов. Далее эти файлы были объединены в единый csv файл с целевыми атрибутами (URL документа, ОКПД2 код).

Затем проведен анализ целевых классов, где установлен их сильный дисбаланс. Поэтому порядка из 9000 лейблов с количеством более 500 ссылок на документы случайным образом отобраны семплы до этого количества, остальные остаются как были. Данное число подбиралось для получения порядка 1'000'000 семплов при исходном порядке 10'000'000.

После получения данных для загрузки запущен процесс выгрузки документов. Даже при малом количестве семплов на класс получилось порядка 1 терабайта сырых данных

документов с учетом фильтрации документов по формату. Загрузка производилась в параллельном режиме в 20 поточном режиме порядка 2х недель.

Затем для загруженных файлов запущен процесс по получению текста из файлов и предобработке документов, который длился около недели в четырёхпоточном режиме. Текст добавлялся в csv файл со ссылками на документы и лейблами. В результате получено порядка 6 Гб обработанного csv файла.

Далее проведен анализ csv файла. Сначала исключаются дубликаты семплов, а затем проводится анализ количества токенов. При анализе обнаружилось, что в некоторой доле файлов достаточно мало токенов. Поэтому часть токенов удалено из распределения графическим способом. А т.е. Дано исходное распределение на рисунке 3А. Далее на рисунке 3Б исключены большие документы (более 13000 токенов), а затем на рисунке 3В исключены документы с менее 4800 токенов.

Теперь данные готовы для подготовки к обучению. Для этого разделим выборку в соотношении тренировочной и проверочной выборки в соотношении 95% к 5%. А новую тренировочную в соотношении 90% к 10%.

Предпоследним шагом при подготовке модели является обучение. При обучении на различных линейных, деревянных и прочих простых моделях возникали проблемы с ресурсами. Обучение производилось порядка 12 дней, с помощью FastText. При применении большинства алгоритмов возникали проблемы с ОЗУ, что показывает его экономичность по сравнению с другими алгоритмами.

Результаты практического использования создаваемого продукта

На текущий момент прорабатываются возможные сценарии для применения данной модели. Потенциально данная модель может дополнить или заменить сервисы для поиска ОКПД2 коду, по ключевым словам, и прочему описанию. Так же в архитектуру можно добавить REST API и передавать предсказания пользователям по этому каналу передачи данных.

Таблицы и графики, подтверждающие работоспособность и достижение заданных целей

В конечном итоге получена метрики для полноценных кодов (2492 шт.) F1 - score равная 0.48, precision 0.48, recall 0.48.

В таблице 2 показаны метрики первого элемента кода, а на рисунке 5 матрица согласия.

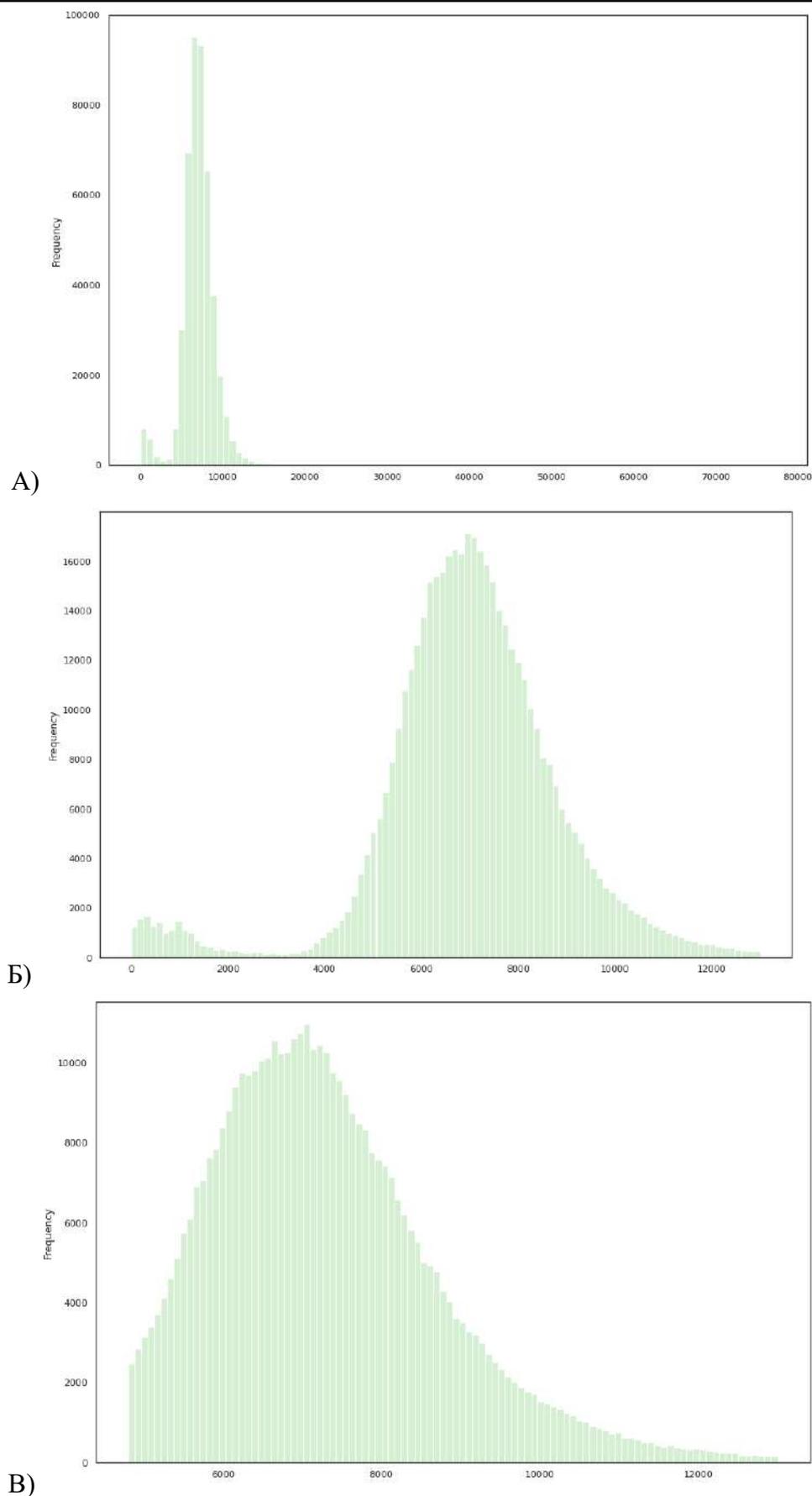


Рисунок 3 – Распределение количества токенов в каждом семпле

Так же построено облако слов для изучения семантического ядра (рисунок 4).

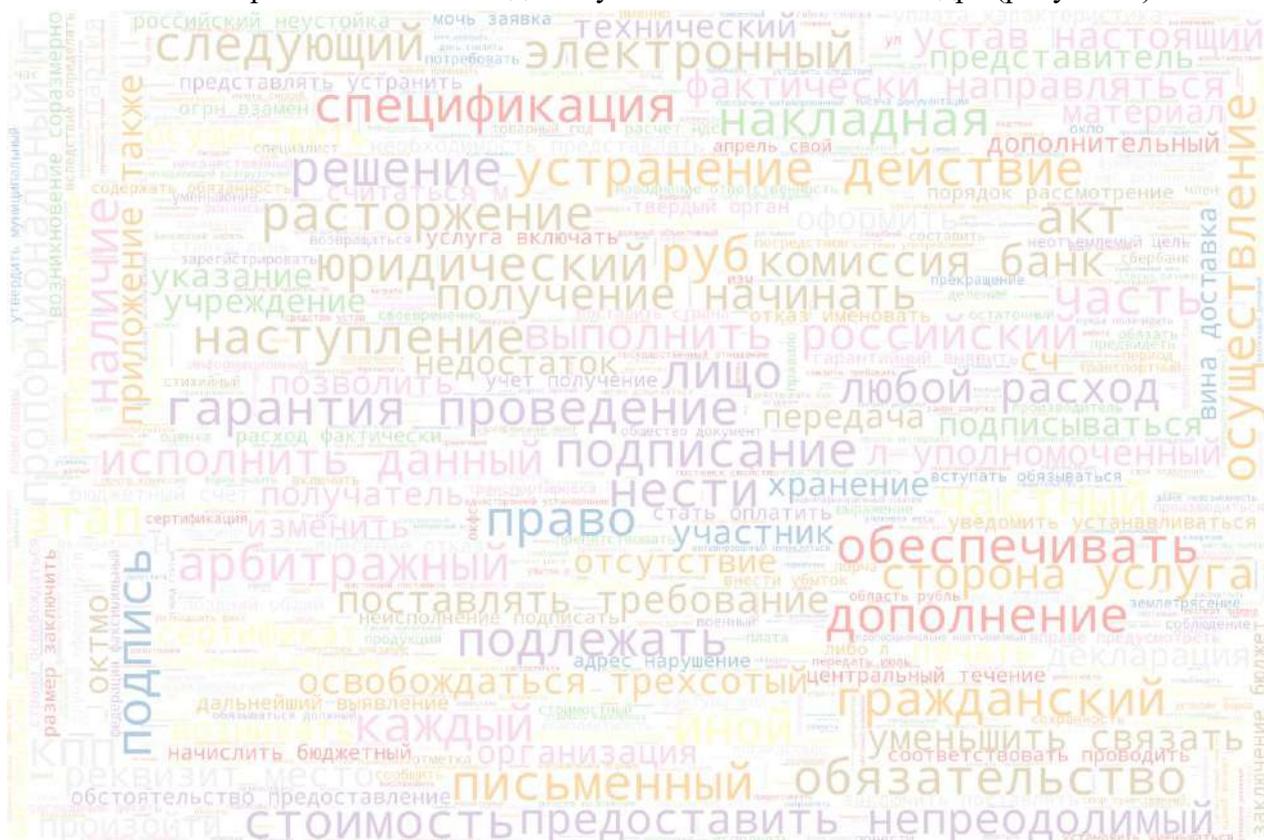


Рисунок 4 – Визуализация семантического ядра данных

Направления дальнейших исследований

- Применение более сложных и точных моделей.
- Погружение в доменную область и декомпозиция кодов.
- Исследование и применение других алгоритмов предобработки документов.
- Запуск периодических процессов загрузки документов в т.ч. подход machine unlearning для исключения устаревших кодов.
- Расширение числа поддерживаемых форматов для распознавания.
- Увеличение скорости загрузки документов.
- Увеличение скорости распознавания документов.
- Добавление REST API или брокера сообщений в архитектуру.

Таблица – 2 Метрики первого элемента кода

labels	precision	recall	f1-score	support
1	0.87	0.87	0.87	733
2	0.96	0.85	0.9	128
3	0.71	0.74	0.73	81
5	0.99	0.95	0.97	83
6	0.67	0.67	0.67	3
8	0.73	0.75	0.74	178
10	0.96	0.96	0.96	3951
11	0.78	0.76	0.77	59
13	0.79	0.8	0.79	730
14	0.84	0.85	0.85	631
15	0.86	0.79	0.82	265
16	0.67	0.66	0.66	175
17	0.83	0.79	0.81	747
18	0.77	0.75	0.76	147
19	0.92	0.91	0.92	503
20	0.77	0.78	0.77	1426
21	0.92	0.94	0.93	2045
22	0.67	0.68	0.67	868
23	0.75	0.69	0.72	519
24	0.71	0.72	0.71	239
25	0.7	0.71	0.71	953
26	0.85	0.86	0.85	1938
27	0.79	0.79	0.79	1380
28	0.81	0.77	0.79	1671
29	0.92	0.91	0.91	86
accuracy				
weighted avg	0.84			19539

Actuals vs Predicted

0	636	3	1	0	0	4	76	0	1	0	0	0	1	0	1	3	0	1	0	1	1	2	0	1	0	
1	6	109	0	0	0	2	0	0	1	0	0	2	0	1	0	2	1	1	0	0	0	0	0	0	3	0
2	0	0	60	0	0	0	19	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
3	0	0	0	79	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	
5	1	0	0	0	0	134	12	0	0	0	0	1	0	0	0	9	6	3	5	0	2	0	1	3	0	
6	81	1	21	0	0	15	3779	8	1	3	0	1	2	0	3	14	9	0	2	1	2	3	1	2	0	
7	1	0	0	0	0	1	5	45	0	0	0	0	0	0	0	2	0	1	0	0	0	1	1	1	0	
8	0	0	2	0	0	0	2	0	583	27	1	3	9	1	1	20	13	33	3	0	12	6	4	6	0	
9	0	1	0	0	0	0	4	0	31	534	21	1	5	0	1	4	2	16	0	0	2	4	3	1	0	
10	0	0	0	0	0	1	2	0	2	22	209	0	3	1	2	3	1	9	0	1	2	2	3	2	0	
11	0	0	0	0	0	1	0	0	5	1	0	116	2	0	0	2	1	13	6	3	17	2	1	3	0	
12	1	0	0	0	0	2	4	0	16	3	2	4	589	16	1	33	7	33	5	0	13	7	2	7	0	
13	1	0	0	0	0	0	0	0	1	1	0	0	11	110	0	5	0	9	0	0	3	2	1	0	0	
14	1	0	0	1	1	1	0	0	2	1	0	1	0	0	459	23	1	2	5	1	0	1	0	2	0	
15	3	0	0	0	0	6	14	4	18	5	0	3	27	5	19	1110	89	28	26	5	16	17	9	17	1	
16	0	0	0	0	0	4	10	0	17	3	0	0	5	1	1	62	1926	3	1	0	0	4	2	1	0	
17	1	0	0	0	0	3	7	0	18	12	3	9	17	5	2	38	12	586	22	12	49	10	22	35	0	
18	0	0	0	0	0	3	1	1	8	1	0	7	2	0	0	44	4	20	359	9	25	7	12	12	0	
19	1	0	0	0	0	2	1	0	1	1	0	4	2	0	0	4	0	17	6	171	17	2	2	7	0	
20	1	0	0	0	0	3	2	0	13	6	2	15	17	0	1	26	4	38	24	23	679	17	30	43	0	
21	0	0	0	0	0	0	1	0	4	2	1	4	11	1	1	22	6	14	7	0	26	1657	82	74	1	
22	0	0	0	0	0	0	3	0	10	6	2	1	3	0	3	7	2	21	2	2	37	95	1093	88	0	
23	0	0	0	0	0	1	3	0	6	3	2	1	4	2	3	13	4	29	6	11	62	99	108	1292	5	
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	2	3	78	
1	2	3	5	6	8	10	11	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29		

Рисунок 5 – Матрица согласия первого элемента кода

Заключение

Прежде всего, на основе анализа документов государственных закупок исследовано применение различных алгоритмов классификации документов. Выявлены программные и аппаратные ограничения большинства алгоритмов. Полученные в предыдущей главе метрики классификации показывают перспективность последующего исследования данной темы.

Список литературы

1. Manning C.D., Raghavan P., Schütze H. An Introduction to Information Retrieval.
2. Jiawei Han, Micheline Kamber, Jian Pei. Data Mining: Concepts and Techniques. 3rd ed. Elsevier Inc., 2012.
3. Domingos P. A Few Useful Things to Know about Machine Learning // Communications of the ACM, Vol. 55(10), Октябрь 2012. pp. 78–87.

4. Jurafsky , Martin H. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. Vol II. Upper Saddle River, (New Jersey). 2008.
5. Manning D., Schutze H. Foundations of Statistical Natural Language Processing. II ed. Лондон: The MIT Press, 2000.
6. Tufte R. THE VISUAL DISPLAY OF QUANTITATIVE INFORMATION. 3rd ed. Graphics Press, 2001. pp. 1-197
7. Eisenstein J. Introduction to Natural Language Processing. Cambridge: MIT Press, 2019. 1-536 pp.
8. Bergstra J., Bengio Y. Random Search for Hyper-Parameter Optimization // Journal of Machine Learning Research. 2012. Vol. 13. pp. 281-305.
9. Howard A., Zhu M., Chen B., Kalenichenko D., Wang W., Weyand T., Andreetto M., Adam H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications // arxiv.org. 2017. URL: <https://arxiv.org/abs/1704.04861> (дата обращения: 1.Февраль.2023).
10. Gelman A., Hill J. Data Analysis Using Regression and Multilevel/Hierarchical Models // Cambridge University Press, 2007. pp. 1-625.
11. Shawe-Taylor J., Cristianini N. Kernel Methods for Pattern Analysis. Кембридж: Cambridge University Press, 2004 г. pp.1-462
12. Межов М.С. Использование машинного обучения для определения континировок, исходя из экономического смысла закупочной документации // International Journal of Open Information Technologies, Vol. 10, 2022. pp. 86-91.
13. Елисеев Д., Романов Д. Машинное обучение: прогнозирование рисков госзакупок // Открытые системы. Апрель 2018. Vol. 2.
14. Классификация данных в системе управления закупками // StecPoint. URL: <https://stecpoint.ru/Practices-Classification/> (дата обращения: 28.Январь.2023).
15. Открытые данные [Электронный ресурс] // ГосЗатраты: [сайт]. [2023]. URL: <https://clearspending.ru/opendata/> (дата обращения: 02.03.2023).

References

1. Manning C.D., Raghavan P., Schütze H. An Introduction to Information Retrieval.
2. Jiawei Han, Micheline Kamber, Jian Pei. Data Mining: Concepts and Techniques. 3rd ed. Elsevier Inc., 2012.
3. Domingos P. A Few Useful Things to Know about Machine Learning // Communications of the ACM, Vol. 55(10), Oktyabr' 2012. pp. 78–87.
4. Jurafsky , Martin H. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. Vol II. Upper Saddle River, (New Jersey). 2008.
5. Manning D., Schutze H. Foundations of Statistical Natural Language Processing. II ed. London: The MIT Press, 2000.
6. Tufte R. THE VISUAL DISPLAY OF QUANTITATIVE INFORMATION. 3rd ed. Graphics Press, 2001. pp 1-197.
7. Eisenstein J. Introduction to Natural Language Processing. Cambridge: MIT Press, 2019. pp.1-536

8. Bergstra J., Bengio Y. Random Search for Hyper-Parameter Optimization // Journal of Machine Learning Research. 2012. Vol. 13. pp. 281-305.
 9. Howard A., Zhu M., Chen B., Kalenichenko D., Wang W., Weyand T., Andreetto M., Adam H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications // arxiv.org. 2017. URL: <https://arxiv.org/abs/1704.04861> (data obrashcheniya: 1.Fevral'.2023).
 10. Gelman A., Hill J. Data Analysis Using Regression and Multilevel/Hierarchical Models // Cambridge University Press, 2007. pp. 1-625.
 11. Shawe-Taylor J., Cristianini N. Kernel Methods for Pattern Analysis. Kembridzh: Cambridge University Press, 2004 g. pp.1-462
 12. Mezhov M.S. Ispol'zovanie mashinnogo obucheniya dlya opredeleniya kontirovok, iskhodya iz ekonomicheskogo smysla zakupchoj dokumentacii // International Journal of Open Information Technologies, Vol. 10, 2022. pp. 86-91.
 13. Eliseev D., Romanov D. Mashinnoe obuchenie: prognozirovanie riskov goszakupok // Otkrytye sistemy. Aprel' 2018. Vol. 2.
 14. Klassifikaciya dannyh v sisteme upravleniya zakupkami // StecPoint. URL: <https://stecpoint.ru/Practices-Classification/> (data obrashcheniya: 28.YAnvar'.2023).
 15. Otkrytye dannye [Elektronnyj resurs] // GosZatraty: [sajt]. [2023]. URL: <https://clearspending.ru/opendata/> (data obrashcheniya: 02.03.2023).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

АРХИТЕКТУРА МНОГОПОТОЧНОГО ПРИЛОЖЕНИЯ В УСЛОВИЯХ ИНТЕРОПЕРАБЕЛЬНОСТИ ПРОЦЕССОВ

Чекановкин А.Е.

ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: 4565855@mail.ru

В современных информационных системах все больше возникает необходимость в многопоточных приложениях, способных эффективно работать в условиях, когда процессы взаимодействуют на разных платформах и в различных средах. В таких сценариях интероперабельность процессов становится ключевым фактором для обеспечения правильной работы приложения. В данной статье будет представлена архитектура многопоточного приложения, которая позволяет решить данную проблему и обеспечить эффективное взаимодействие между процессами.

Ключевые слова: многопоточность; гонка данных; интероперабельность процессов.

ARCHITECTURE OF A MULTI-THREAD APPLICATION UNDER THE CONDITIONS OF ARCH PROCESS INTEROPERABILITY

Chekanovkin A.E.

MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: 4565855@mail.ru

In modern information systems, there is an increasing need for multithreaded applications that can work effectively in conditions when processes interact on different platforms and in different environments. In such scenarios, the interoperability of processes becomes a key factor to ensure the correct operation of the application. This article will present the architecture of a multithreaded application, which allows you to solve this problem and ensure effective interaction between processes.

Keywords: multithreading; data race; process interoperability.

Определение многопоточности

Многопоточность - это концепция в программировании, которая позволяет одновременно выполнять несколько потоков внутри одного процесса. Поток представляет собой независимую единицу выполнения, которая может выполняться параллельно или конкурентно с другими потоками. Каждый поток имеет собственный стек вызовов, указатель команд и состояние выполнения [1].

Основная идея многопоточности заключается в том, чтобы разделить задачу на более мелкие подзадачи и выполнять их параллельно в разных потоках. Это позволяет повысить эффективность и производительность программы, так как различные потоки могут выполнять вычисления, ввод-вывод операции или другие операции одновременно.

В отличие от выполнения в однопоточных приложениях, многопоточные приложения могут более эффективно использовать доступные ресурсы системы, такие как процессорное время и память. Кроме того, многопоточность позволяет реагировать на асинхронные события и организовывать параллельное выполнение различных задач.

Преимущества многопоточных приложений включают улучшенную отзывчивость, более эффективное использование ресурсов, улучшенную масштабируемость и возможность реализации сложных задач, которые требуют параллельного выполнения.

Однако, при разработке многопоточных приложений также возникают ряд сложностей и проблем. Например, необходимо управлять синхронизацией доступа к общим ресурсам, чтобы избежать состояний гонки и других проблем совместного доступа к данным. Кроме того, необходимо тщательно планировать и координировать выполнение потоков, чтобы избежать блокировок и конфликтов. Эти проблемы требуют особого внимания при проектировании и разработке многопоточных приложений.

Преимущества многопоточных приложений

Многопоточные приложения предлагают ряд значительных преимуществ, которые делают их предпочтительным выбором при разработке современных программных систем. Вот некоторые из основных преимуществ многопоточных приложений [2]:

Повышенная производительность: Многопоточные приложения позволяют использовать параллельное выполнение задач на нескольких процессорных ядрах. Это может привести к существенному увеличению производительности и сокращению времени выполнения программы. Разделение работы на небольшие задачи, которые выполняются параллельно, позволяет более эффективно использовать вычислительные ресурсы системы.

Улучшенная отзывчивость: Многопоточность позволяет отделить длительные операции, такие как сетевые запросы или обработка пользовательского ввода, от основного потока выполнения приложения. Это позволяет приложению оставаться отзывчивым на взаимодействие с пользователем, даже если происходят другие вычислительные операции.

Лучшее использование ресурсов: Многопоточные приложения позволяют более эффективно использовать доступные ресурсы системы, такие как процессорное время и память. При наличии нескольких потоков, связанных с различными задачами, можно более равномерно распределить вычислительную нагрузку и избежать простоев, которые могут возникнуть при выполнении операций последовательно.

Возможность параллельной обработки данных: В многопоточных приложениях можно одновременно обрабатывать различные наборы данных или выполнять вычисления на разных частях данных. Это особенно полезно при работе с большими объемами данных, такими как обработка видео, анализ больших наборов данных или распараллеливание сложных вычислений.

Легкость разработки и поддержки: Многопоточные приложения позволяют разделить задачи на более мелкие и независимые единицы, что упрощает их разработку и поддержку. Каждый поток может быть разработан и отлажен отдельно, что упрощает их тестирование и обнаружение ошибок. Кроме того, многопоточные приложения могут быть более гибкими и масштабируемыми, так как дополнительные потоки могут быть добавлены или удалены в зависимости от требований системы.

В целом, многопоточные приложения предоставляют мощный инструмент для эффективной организации и управления выполнением задач. Они способствуют повышению производительности, улучшению отзывчивости и более эффективному использованию ресурсов системы, что делает их незаменимыми во многих современных программных системах.

Проблемы при разработке многопоточных приложений

Разработка многопоточных приложений может столкнуться с рядом сложностей и проблем, связанных с эффективностью, безопасностью и корректностью выполнения [3]. Некоторые из основных проблем, с которыми разработчики могут столкнуться при создании многопоточных приложений, включают:

Состояние гонки (Race conditions): Состояние гонки возникает, когда несколько потоков одновременно обращаются к общему ресурсу и пытаются изменить его состояние. Это может привести к непредсказуемым результатам или ошибкам в программе. Разработчики должны применять механизмы синхронизации, такие как мьютексы или блокировки, для предотвращения состояний гонки и обеспечения правильного доступа к общим ресурсам.

Взаимные блокировки (Deadlocks): Взаимная блокировка возникает, когда два или более потока ожидают освобождения ресурсов, заблокированных другими потоками. Это может привести к застою и невозможности продолжить выполнение программы. Разработчики должны аккуратно планировать использование блокировок и управлять порядком их получения, чтобы избежать взаимных блокировок.

Голодание потоков (Thread starvation): Голодание потоков возникает, когда один или несколько потоков систематически не получают достаточно ресурсов для выполнения своих задач. Это может привести к снижению производительности и отзывчивости приложения. Разработчики должны учитывать приоритеты потоков, правильно управлять ресурсами и предотвращать голодание потоков.

Неправильное использование синхронизации: Неправильное использование механизмов синхронизации, таких как блокировки или семафоры, может привести к непредсказуемому поведению приложения или проблемам с производительностью. Разработчики должны тщательно планировать и применять синхронизацию, чтобы избежать ненужной блокировки и улучшить производительность.

Управление потоками и планирование: Управление потоками и планирование их выполнения может быть сложной задачей, особенно при наличии большого количества потоков. Неправильное планирование или некорректное использование ресурсов процессора может привести к снижению производительности или неравномерному использованию вычислительных ресурсов.

Отладка и тестирование: Отладка многопоточных приложений может быть сложной из-за непредсказуемого поведения и взаимодействия между потоками. Тестирование таких приложений также требует особого внимания, чтобы убедиться в их корректности и надежности при параллельном выполнении.

Все эти проблемы требуют тщательного планирования, проектирования и тестирования многопоточных приложений. Разработчики должны иметь хорошее понимание принципов синхронизации и механизмов управления потоками, чтобы избежать потенциальных проблем и обеспечить корректное функционирование многопоточных приложений.

Определение интероперабельности процессов

Интероперабельность процессов - это способность различных процессов или программных систем взаимодействовать и совместно работать друг с другом, несмотря на различия в их архитектуре, платформе или языке программирования [4]. Интероперабельность процессов является ключевым аспектом в современных информационных системах, где различные компоненты или приложения часто должны обмениваться данными и выполнять совместные операции.

Интероперабельность процессов предполагает, что процессы должны быть в состоянии взаимодействовать, обмениваться информацией и использовать функциональность друг друга без необходимости полной переработки или изменения существующих компонентов. Она позволяет различным процессам работать в согласованном и совместимом окружении, даже если они были разработаны независимо друг от друга или используют разные технологии.

Одной из основных целей интероперабельности процессов является создание гибкого и расширяемого программного обеспечения, которое может взаимодействовать с другими системами и использовать их возможности. Она способствует повторному использованию кода, ускоряет разработку и позволяет строить более сложные системы, объединяющие функциональность различных компонентов и приложений.

Интероперабельность процессов может быть достигнута через использование стандартов и протоколов обмена данными, таких как XML, JSON, REST или SOAP. Эти стандарты обеспечивают единый способ представления и передачи данных между процессами, независимо от их платформы или языка программирования.

Подходы к обеспечению интероперабельности процессов могут варьироваться в зависимости от конкретных потребностей системы. Они могут включать разработку адаптеров или посредников, которые обеспечивают преобразование данных между различными форматами или обеспечивают согласованность взаимодействия между процессами. Также может использоваться разработка API или сервис-ориентированная архитектура (SOA) для предоставления стандартизированных интерфейсов, через которые процессы могут взаимодействовать друг с другом.

В итоге, интероперабельность процессов играет важную роль в построении сложных и совместных систем. Она обеспечивает возможность интеграции различных компонентов и приложений, улучшает гибкость и эффективность системы, а также способствует повышению производительности и функциональности информационных систем.

Проблемы, связанные с интероперабельностью процессов

В процессе обеспечения интероперабельности процессов могут возникать различные проблемы, которые затрудняют успешное взаимодействие и совместную работу различных компонентов или приложений. Некоторые из основных проблем, связанных с интероперабельностью процессов, включают:

Различия в форматах данных и протоколах: Различные процессы или системы могут использовать разные форматы данных и протоколы обмена информацией. Например, одна система может использовать формат XML, в то время как другая - JSON. Это может привести к сложностям при передаче и преобразовании данных между различными форматами. Разработчики должны быть готовы к реализации механизмов преобразования данных и обеспечению согласованности форматов при взаимодействии между процессами.

Различия в языках программирования и платформах: Различные процессы могут быть написаны на разных языках программирования или работать на разных платформах. Это может вызвать проблемы совместимости и взаимодействия. Разработчики должны искать решения, такие как использование промежуточного программного интерфейса (API) или разработку адаптеров, чтобы обеспечить возможность взаимодействия между процессами, независимо от их языка или платформы.

Сложность обеспечения безопасности: Интероперабельность процессов может представлять риски с точки зрения безопасности. При взаимодействии между различными процессами могут возникать уязвимости или возможность несанкционированного доступа к данным. Разработчики должны обеспечивать надежность и защищенность взаимодействия, используя механизмы аутентификации, шифрования и контроля доступа.

Управление версиями и изменениями: При взаимодействии между процессами могут возникать проблемы с управлением версиями и изменениями в интерфейсах и протоколах. Обновление или изменение одного процесса может потребовать соответствующих изменений в других процессах, чтобы сохранить совместимость. Разработчики должны учитывать вопросы управления версиями и разрабатывать стратегии обновления и поддержки интерфейсов для обеспечения согласованности и продолжительности работы системы.

Отладка и тестирование: Интероперабельность процессов усложняет процесс отладки и тестирования системы в целом. При возникновении проблем взаимодействия может быть сложно определить и исправить причину. Тестирование должно включать проверку взаимодействия между различными компонентами и проверку соответствия спецификациям и стандартам интероперабельности.

Разработчики многопоточных приложений должны быть готовы к решению этих проблем и применению соответствующих методов и технологий для обеспечения успешной интероперабельности процессов. Это требует внимательного планирования, проектирования и тестирования, а также учета стандартов и протоколов, чтобы обеспечить гармоничное взаимодействие и эффективную работу системы.

Требования к архитектуре многопоточного приложения в условиях интероперабельности процессов

Архитектура многопоточного приложения должна быть разработана с учетом требований интероперабельности процессов, чтобы обеспечить эффективное взаимодействие и совместную работу различных компонентов или приложений. Ключевые требования, которые следует учитывать при проектировании архитектуры:

Стандартизированные протоколы и форматы данных: При проектировании архитектуры необходимо использовать стандартизированные протоколы и форматы данных для обмена информацией между процессами. Это обеспечит совместимость и возможность взаимодействия даже в случае различных языков программирования или платформ.

Гибкость и расширяемость: Архитектура должна быть гибкой и расширяемой, чтобы легко включать новые компоненты или приложения в систему. Это позволит легко интегрировать новые функциональные возможности и обеспечивать совместную работу с другими процессами.

Стабильность и надежность: Архитектура должна быть стабильной и надежной для обеспечения непрерывной работы системы. Взаимодействие между процессами должно быть надежным и обеспечивать сохранность данных и целостность операций.

Управление версиями и изменениями: Архитектура должна предусматривать механизмы управления версиями и изменениями в интерфейсах и протоколах. Это позволит гибко вносить изменения и обновления в систему без нарушения совместимости и взаимодействия с другими процессами.

Безопасность: Безопасность является важным аспектом интероперабельности процессов. Архитектура должна обеспечивать механизмы аутентификации, авторизации и шифрования для защиты данных и обеспечения безопасного взаимодействия между процессами.

Масштабируемость: Архитектура должна быть масштабируемой, чтобы обеспечить эффективную работу системы при увеличении нагрузки или добавлении новых процессов. Это включает возможность горизонтального и вертикального масштабирования, а также управление ресурсами.

Четкая документация и соглашения: Важно иметь четкую документацию и соглашения относительно интерфейсов, протоколов и общих правил взаимодействия между процессами. Это поможет разработчикам понять и правильно использовать интерфейсы и обеспечит согласованность взаимодействия.

Учитывая эти требования при проектировании архитектуры многопоточного приложения, можно создать систему, которая обеспечивает эффективное взаимодействие и совместную работу различных процессов или приложений, даже при различных языках программирования, платформах или стандартах.

Компоненты архитектуры

Архитектура многопоточного приложения, ориентированного на интероперабельность процессов, состоит из различных компонентов, которые совместно работают для обеспечения эффективного взаимодействия и совместной работы. Вот некоторые основные компоненты, которые можно встретить в такой архитектуре [5]:

Потоки (Threads): Потоки представляют собой базовые строительные блоки многопоточного приложения. Они представляют собой независимые исполняющиеся единицы, которые могут параллельно выполнять различные задачи. Каждый процесс может содержать несколько потоков, которые совместно работают для выполнения общей задачи.

Межпроцессное взаимодействие (Interprocess Communication, IPC): Для обмена данными и синхронизации работы между процессами необходимо использовать механизмы межпроцессного взаимодействия. Это может включать различные методы, такие как использование сокетов, пайпов, разделяемой памяти или сообщений. Механизмы IPC позволяют процессам обмениваться информацией и координировать свою работу.

Промежуточные компоненты (Middleware): Промежуточные компоненты представляют собой слой абстракции, который облегчает взаимодействие между различными процессами и обеспечивает уровень интероперабельности. Эти компоненты могут включать в себя различные технологии, такие как сервисы сообщений, шины данных, адаптеры протоколов и т. д. Промежуточные компоненты упрощают взаимодействие между процессами, скрывая детали реализации и обеспечивая единый интерфейс.

Сервисы (Services): Сервисы представляют собой компоненты, которые предоставляют определенные функциональные возможности для других процессов или приложений. Они могут включать в себя сервисы авторизации, аутентификации, управления данными и другие сервисы, необходимые для эффективной работы системы. Сервисы могут быть предоставлены как локально внутри одного процесса, так и удаленно через механизмы удаленного вызова процедур (Remote Procedure Call, RPC) или веб-сервисы.

Интерфейсы (Interfaces): Интерфейсы определяют способ взаимодействия между компонентами и процессами. Они определяют набор методов, функций или протоколов, которые могут быть использованы для передачи данных и выполнения операций. Интерфейсы должны быть ясно задокументированы и соответствовать стандартам, чтобы обеспечить совместимость и возможность взаимодействия между компонентами.

Компоненты архитектуры многопоточного приложения должны быть тщательно спроектированы и интегрированы, чтобы обеспечить эффективное взаимодействие и совместную работу процессов в условиях интероперабельности. Это требует понимания требований системы, выбора подходящих технологий и стандартов, а также грамотной реализации и интеграции компонентов.

Организация взаимодействия между потоками

В многопоточных приложениях, ориентированных на интероперабельность процессов, взаимодействие между потоками играет важную роль для эффективной работы и совместного выполнения задач. Рассмотрим несколько распространенных методов организации взаимодействия между потоками [6]:

Синхронизация (Synchronization): Синхронизация является ключевым аспектом взаимодействия между потоками. Она позволяет координировать выполнение задач и обеспечивает согласованность данных. Механизмы синхронизации, такие как блокировки, семафоры, мьютексы и условные переменные, используются для предотвращения состояния гонки и обеспечения доступа к общим ресурсам.

Потокобезопасные структуры данных (Thread-Safe Data Structures): Потокобезопасные структуры данных предназначены для обеспечения безопасного доступа к общим данным из разных потоков. Это могут быть потокобезопасные очереди, хеш-таблицы, списки и другие структуры данных, которые обеспечивают синхронизированный доступ к данным и предотвращают конфликты.

Каналы и очереди (Channels and Queues): Использование каналов и очередей позволяет организовать асинхронное взаимодействие между потоками. Один поток может помещать данные в очередь или канал, а другой поток может извлекать их и обрабатывать. Это обеспечивает асинхронность и гибкость взаимодействия между потоками.

Использование событий и сигналов (Events and Signals): События и сигналы используются для уведомления потоков о наступлении определенных событий или изменениях состояния. Они позволяют потокам ожидать определенных условий и реагировать на них. Это может быть полезно при ожидании завершения операции или сигнализации о готовности ресурса.

Пулы потоков (Thread Pools): Пулы потоков представляют собой набор предварительно созданных потоков, которые могут использоваться для выполнения задач. Они позволяют эффективно использовать ресурсы и снизить накладные расходы на создание и уничтожение

потоков. Пулы потоков обеспечивают распределение задач и масштабируемость взаимодействия между потоками.

Механизмы обмена сообщениями (Message Passing): Механизмы обмена сообщениями позволяют потокам передавать данные и команды друг другу через сообщения. Это может включать использование очередей сообщений, асинхронных вызовов процедур или других протоколов обмена сообщениями. Механизмы обмена сообщениями обеспечивают асинхронное и гибкое взаимодействие между потоками.

При организации взаимодействия между потоками важно учитывать требования системы и выбрать подходящие механизмы синхронизации и коммуникации. Это поможет обеспечить эффективное и безопасное взаимодействие между потоками, минимизировать состояния гонки и конфликты данных, а также повысить производительность и отзывчивость приложения.

Механизмы синхронизации и координации

Механизмы синхронизации и координации играют важную роль в архитектуре многопоточных приложений, ориентированных на интероперабельность процессов. Они обеспечивают правильное взаимодействие и согласованную работу потоков и процессов. Ниже приведены распространенные механизмы синхронизации и координации [7]:

Блокировки (Locks): Блокировки используются для обеспечения эксклюзивного доступа к ресурсам или критическим секциям кода. Когда поток получает блокировку, другие потоки должны ждать освобождения блокировки, прежде чем получить доступ к защищенным ресурсам. Блокировки могут быть реализованы с использованием мьютексов, семафоров или атомарных операций.

Семафоры (Semaphores): Семафоры позволяют ограничить количество потоков, которые могут одновременно получить доступ к определенному ресурсу или критической секции. Семафор содержит счетчик, который уменьшается при каждом получении доступа потоком и увеличивается при его освобождении. Это позволяет управлять параллельным выполнением задач и предотвращать перегрузку ресурсов.

Условные переменные (Condition Variables): Условные переменные позволяют потокам ожидать определенного условия или события перед продолжением выполнения. Они могут быть использованы для ожидания завершения операции, появления новых данных или изменения состояния. Условные переменные работают совместно с блокировками и позволяют потокам эффективно управлять своим состоянием ожидания.

Синхронизаторы (Synchronizers): Синхронизаторы представляют собой более высокоуровневые абстракции для управления потоками и их взаимодействия. Они включают в себя семафоры, барьеры, счетчики и другие механизмы, которые позволяют потокам синхронизироваться, согласовывать свою работу и добиться определенных условий перед продолжением выполнения.

Координаторы (Coordinators): Координаторы представляют собой компоненты, ответственные за координацию работы потоков и процессов в многопоточных приложениях. Они могут включать в себя централизованные или распределенные механизмы управления, планирования задач, распределения ресурсов и обмена информацией между потоками.

При выборе механизмов синхронизации и координации необходимо учитывать требования приложения, его архитектуру и особенности интероперабельности процессов.

Оптимальный выбор механизмов позволяет избежать состояний гонки, конфликтов и улучшить производительность приложения.

Заключение

В данной статье были представлены механизмы архитектуры многопоточного приложения, обеспечивающие эффективное взаимодействие между потоками в условиях интероперабельности процессов. Описаны основные компоненты архитектуры, механизмы синхронизации и координации. Данная статья может быть полезна для разработчиков, сталкивающихся с необходимостью создания многопоточных приложений, работающих в различных средах и на разных платформах.

Список литературы

1. Understanding Basic Multithreading Concepts [Электронный ресурс]. – Режим доступа: <https://docs.oracle.com/cd/E19455-01/806-5257/6je9h032e/index.html> (дата обращения: 28.05.2023)
2. Фешина, Е. В. Многопоточность и асинхронность в языке программирования Python / Е. В. Фешина, Д. А. Омельченко, Р. Г. Гонатаев // Инновации. Наука. Образование. – 2021. – № 28. – С. 988-992. – EDN ANHVUX.
3. Гладышев Е.И., Мурыгин А.В. Многопоточность в приложениях // Актуальные проблемы авиации и космонавтики. 2012. №8. URL: <https://cyberleninka.ru/article/n/mnogopotocnost-v-prilozheniyah> (дата обращения: 31.05.2023)
4. Некрасов, А. Г. Проактивный мониторинг процессов интероперабельности и организационной устойчивости в сфере транспорта / А. Г. Некрасов, А. С. Синицына // Академик Владимир Николаевич Образцов - основоположник транспортной науки : труды международной научно-практической конференции, посвященной 125-летию университета, Москва, 22 октября 2021 года. – Москва: Российский университет транспорта, 2021. – С. 637-647. – DOI 10.47581/2022/Obrazcov.85. – EDN ULSRLK.
5. Шалагин, В. И. Основы организации многопоточной обработки данных в вычислительных системах / В. И. Шалагин, А. Л. Марухленко // Современные информационные технологии и информационная безопасность: Сборник научных статей Всероссийской научно-технической конференции, Курск, 17 мая 2022 года. – Курск: Юго-Западный государственный университет, 2022. – С. 40-58. – EDN BSHZOX.
6. Елизаров, В. В. Разработка веб-приложения для организации взаимодействия между пользователями посредством потокового мультимедиа / В. В. Елизаров // NEW SCIENCE GENERATION: сборник статей II Международной научно-практической конференции, Петрозаводск, 25 декабря 2019 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская Ирина Игоревна), 2019. – С. 239-243. – EDN ZUFRDZ.
7. Методы синхронизации потоков в многопоточном приложении на языке C++ [Электронный ресурс]. – Режим доступа: <https://science-pedagogy.ru/ru/article/view?id=1962> (Дата обращения: 29.05.2023).

References

1. Understanding Basic Multithreading Concepts [Elektronnyj resurs]. – Rezhim dostupa: <https://docs.oracle.com/cd/E19455-01/806-5257/6je9h032e/index.html> (data obrashcheniya: 28.05.2023)
 2. Feshina, E. V. Mnogopotochnost' i asinhronnost' v yazyke programmirovaniya Python / E. V. Feshina, D. A. Omel'chenko, R. G. Gonataev // Innovacii. Nauka. Obrazovanie. – 2021. – № 28. – pp. 988-992. – EDN ANHVUX.
 3. Gladyshev E.I., Murygin A.V. Mnogopotochnost' v prilozheniyah // Aktual'nye problemy aviacii i kosmonavтики. 2012. №8. URL: <https://cyberleninka.ru/article/n/mnogopotochnost-v-prilozheniyah> (data obrashcheniya: 31.05.2023)
 4. Nekrasov, A. G. Proaktivnyj monitoring processov interoperabel'nosti i organizacionnoj ustojchivosti v sfere transporta / A. G. Nekrasov, A. S. Sinicyna // Akademik Vladimir Nikolaevich Obrazcov - osnovopolozhnik transportnoj nauki : trudy mezhdunarodnoj nauchno-prakticheskoy konferencii, posvyashchennoj 125-letiyu universiteta, Moskva, 22 oktyabrya 2021 goda. – Moskva: Rossijskij universitet transporta, 2021. – pp. 637-647. – DOI 10.47581/2022/Obrazcov.85. – EDN ULSRLK.
 5. SHalagin, V. I. Osnovy organizacii mnogopotochnoj obrabotki dannyh v vychislitel'nyh sistemah / V. I. SHalagin, A. L. Maruhlenko // Sovremennye informacionnye tekhnologii i informacionnaya bezopasnost': Sbornik nauchnyh statej Vserossijskoj nauchno-tekhnicheskoy konferencii, Kursk, 17 maya 2022 goda. – Kursk: YUgo-Zapadnyj gosudarstvennyj universitet, 2022. – pp. 40-58. – EDN BCHZOX.
 6. Elizarov, V. V. Razrabotka veb-prilozheniya dlya organizacii vzaimodejstviya mezhdou pol'zovatelyami posredstvom potokovogo mul'timedia / V. V. Elizarov // NEW SCIENCE GENERATION: sbornik statej II Mezhdunarodnoj nauchno-prakticheskoy konferencii, Petrozavodsk, 25 dekabrya 2019 goda. – Petrozavodsk: Mezhdunarodnyj centr nauchnogo partnerstva «Novaya Nauka» (IP Ivanovskaya Irina Igorevna), 2019. – pp. 239-243. – EDN ZUFRDZ.
 7. Metody sinhronizacii potokov v mnogopotochnom prilozhenii na yazyke C++ [Elektronnyj resurs]. – Rezhim dostupa: <https://science-pedagogy.ru/ru/article/view?id=1962> (Data obrashcheniya: 29.05.2023).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 640.412

ПОТЕНЦИАЛ VR В ГОСТИНИЧНОМ БИЗНЕСЕ

Багазей Д.И.

Северо-Западный институт управления СЗИУ РАНХиГС, Санкт-Петербург, Россия (199178, г. Санкт-Петербург, Средний просп. Васильевского острова, 57), e-mail: d-bagazey@edu.ranepa.ru

В последние годы виртуальная реальность (virtual reality, далее- VR) стала одним из наиболее быстро развивающихся технологических направлений, затронувших многие отрасли бизнеса. В туристической индустрии VR также нашла свое применение, трансформируя представление о том, как мы познаем и взаимодействуем с миром. Вместе с тем VR открывает и новые возможности для гостиничного бизнеса, которые могут повысить степень комфорта для гостей, обеспечить лучший сервис и привлечь больше потенциальных путешественников. В данной работе исследуется потенциал VR в гостиничном бизнесе, его влияние на данную отрасль, преимущества и успешные примеры применения в индустрии гостеприимства, а также перспективы и выгоды.

Ключевые слова: Виртуальная реальность, VR, индустрия гостеприимства, VR технологии, инструмент маркетинга, инновации.

THE POTENTIAL OF VR IN THE HOSPITALITY INDUSTRY

Bagazey D.I.

Northwestern Institute of Management- Russian Academy of National Economy and Public Administration, St. Petersburg, Russia (199178, St. Petersburg, Middle ave . Vasilievsky Island, 57), e-mail: d-bagazey@edu.ranepa.ru

In recent years, virtual reality (hereinafter referred to as VR) has become one of the fastest growing technological trends, affecting many business sectors. VR has also found its application in the travel industry, transforming the way we experience and interact with the world. At the same time, VR also opens up new opportunities for the hotel industry, which can increase the degree of comfort for guests, provide better service and attract more potential travelers. This paper explores the potential of VR in the hospitality industry, its impact on the industry, the benefits and success stories in the hospitality industry, and the prospects and benefits.

Keywords: Virtual reality, VR, hospitality industry, VR technology, marketing tool, innovations.

Люди - это визуальные существа, что означает, что им нужно видеть объекты и взаимодействовать с ними для лучшего понимания, опыта и общения. Использование виртуальной реальности (VR) позволяет людям взаимодействовать в смоделированной цифровой среде без необходимости покидать их там, где они находятся. Прошли те времена, когда использование виртуальной реальности ограничивалось миром игр и рисовало картины далекого будущего; VR теперь является настоящей технологией, трансформирующей будущее работы - к лучшему и навсегда.

Виртуальная реальность - это компьютерная технология, которая помещает пользователей в трехмерную цифровую среду, которая позволяет им взаимодействовать, а не смотреть на экран. Иммерсивный опыт VR - это самое большое, что отличает его от традиционных пользовательских интерфейсов. Будь то развлечения, образование или электронная коммерция, VR является растущей силой многих развивающихся отраслей. Тем не менее, внедрение виртуальной реальности на рабочем месте трансформирует и переопределяет то, как мы это делаем. Технология VR недавно попала в основное русло с появлением доступных и доступных гарнитур VR для бизнеса. Технология помогла таким отраслям бизнеса, как здравоохранение, розничная торговля и образование, эффективно предоставлять услуги и улучшать качество обслуживания клиентов в виртуальной реальности [2].

История использования VR в гостиничном бизнесе относительно недолгая, и началась она с разработки прототипов систем виртуальной реальности. Развитие VR технологий в последние годы позволило индустрии гостеприимства использовать этот инструмент в самых разных сферах - от маркетинга и продаж до обучения персонала [6].

Вероятно, справедливо сказать, что весь потенциал VR в индустрии гостеприимства еще не открыт, но это обязательно изменится в ближайшие годы. Ниже представлено несколько удивительных примеров того, как виртуальная реальность может революционизировать отрасль.

Виртуальные путешествия

Интерактивные гастрономические впечатления и экскурсии по местным достопримечательностям - это основное внимание для путешественников, планирующих поездку из дома. Использование 360-градусной видеотехнологии в виртуальных путешествиях позволяет путешественникам испытать отдых различных аспектов путешествий [3].

Виртуальные туры по отелю

Благодаря виртуальной реальности у клиентов есть отличная возможность познакомиться с недвижимостью, в которой они собираются остановиться. Им не нужно представлять себе отель, просматривать Интернет или искать изображения веб-сайта и бумажные брошюры. Они могут легко (но практически) посетить отели, в которых они думают остановиться, и узнать, как выглядит ресторан отеля или насколько хорошо оборудован фитнес-центр отеля [3].

Планирование и управление стало проще

С точки зрения гостя, виртуальная реальность может стать настоящим облегчением, когда дело доходит до планирования и управления. Они могут перемещаться по туристическим достопримечательностям и направлениям, как если бы они были там на самом деле, что делает планирование поездки намного проще и удобнее - у путешественника даже есть возможность увидеть пункт назначения с высоты птичьего полета. Им не нужно тратить время на поиск обязательных для посещения мест в Интернете. Гарнитура VR также может быть эффективным инструментом для планирования мероприятий с другими путешественниками, у которых есть оборудование и приложения VR, поскольку они могут общаться друг с другом и обмениваться отзывами о своем предыдущем опыте [1].

Как владельцы гостиничного бизнеса могут извлечь выгоду из виртуальной реальности? До сих пор было пояснение об использовании VR для туристов и потенциальных гостей отеля.

А как насчет владельцев отелей? Прежде всего, включение решений виртуальной реальности (интерактивные медиа, виртуальные туры) в маркетинговую кампанию определенно увеличит количество заказов. Отель будет более привлекательным, что поможет увеличить трафик на сайте отеля и в социальных сетях. Благодаря высококачественному виртуальному туру больше клиентов будут мотивированы делать прямые бронирования в отеле - добавление функции прямого бронирования в виртуальные туры действительно может извлечь из этого выгоду, что приведет к более быстрой конверсии. Более того, VR создаст неизгладимое впечатление, ведь клиентам нравится свобода выбора того, что смотреть, поэтому, если дать им возможность контролировать свой виртуальный опыт, их уникальные потребности будут удовлетворены. И именно можно завоевать их лояльность, предлагая бесценную ценность - потенциальные гости не только могут увидеть уникальные качества вашего отеля из первых рук, но и взаимодействовать с технологиями, которые им предоставляют [10].

С появлением новых VR технологий и гаджетов, таких как Oculus Rift и HTC Vive, VR стала доступна более широкому кругу компаний и стала более эффективным инструментом маркетинга и продаж в гостиничном бизнесе. Это позволило создать симуляции и игры с использованием VR, которые помогают привлечь новых клиентов и повысить уровень сервиса в отелях - что является одним из главных преимуществ применения VR. Туристы из других регионов и даже других стран могут получить представление об отеле, даже если у них нет возможности посетить его лично. [1].

Еще одним ярким преимуществом VR в бизнесе, помимо привлечения новых клиентов, является создание рабочей среды, которая повышает производительность сотрудников, а также может обеспечить безопасную и контролируемую обстановку для обучения и экспериментов. Это помогает лицам, принимающим решения, сделать более осознанный выбор и понять влияние своих решений, прежде чем принять окончательное решение. VR способна предоставить улучшенное обучение. Сотрудники могут практиковаться и учиться в реалистичной, захватывающей среде, которая помогает улучшить свои навыки и знания при одновременном снижении риска [4].

Еще одно преимущество VR заключается в том, что он может помочь предприятиям отличаться от конкурентов и создать более инновационный, дальновидный имидж бренда, давая им конкурентное преимущество. Кроме того, VR может обеспечить экономию средств, устраняя необходимость в дорогостоящем оборудовании или поездках, и может повысить эффективность за счет сокращения времени и ресурсов, необходимых для обучения [10].

Примеры успешного применения VR в гостиничном бизнесе

Сегодня около трех четвертей крупнейших мировых брендов интегрировали VR в свои маркетинговые стратегии. Многим компаниям удается достичь замечательных маркетинговых результатов, используя этот мощный маркетинговый инструмент. Существует несколько примеров успешного применения VR в гостиничном бизнесе, которые помогли компаниям привлечь новых клиентов, повысить уровень сервиса и улучшить общий опыт гостей.

1. Marriott Hotels. Отельный бренд Marriott использовал VR технологии для создания виртуальных туров по своим отелям. Это позволило потенциальным гостям более детально ознакомиться с номерами и удобствами, прежде чем они сделают бронь. Кроме того, Marriott создал программу Virtual Reality Postcards, позволяющую гостям отеля создавать свои собственные VR-туры. Отдельная разработка Marriott- Телепортатор Марриотта (Marriott's Teleporter) - это классический пример VR-маркетинга в индустрии гостеприимства. Являясь

одним из ведущих мировых гостиничных операторов, Marriott всегда ищет способы обновить гостиничный опыт и изобрести будущее путешествий. Кампания "Путешествуйте блестяще" представила своим клиентам 4D VR опыт, в котором причудливо сочетались 3D визуальные (фотореалистичные CGI и 360o видео), аудио, тактильные и обонятельные элементы, чтобы создать ощущение полного тела. Эта инновационная идея VR-путешествия была прекрасно реализована путем установки стенда в стратегически важных местах. Сначала он был установлен возле мэрии Нью-Йорка, чтобы пригласить молодоженов испытать виртуальный медовый месяц. Затем стенд, установленный в СМИ, пригласил влиятельных лиц испытать технологию из первых рук, вызвав тем самым ажиотаж вокруг телепортатора. В итоге за два месяца кампания с телепортатором объехала восемь городов США и собрала более миллиарда впечатлений в СМИ и социальных сетях [8].

2. Hilton Hotels. Сеть Hilton Hotels использовала VR технологии в обучении своих сотрудников. Руководство Hilton отлично знает: чтобы качественно обслуживать гостей, сотрудники отеля должны смотреть на мир их глазами. Для этого компания разработала на платформе Oculus for Business инновационный VR-продукт для обучения. Они создали виртуальные ситуации, которые ограничивались определенными сценариями обслуживания гостей. Сотрудники получили возможность практиковаться в общении с гостями и тренироваться в разрешении конфликтных ситуаций. С помощью VR компании Hilton удалось сократить время очного обучения с 4 часов до 20 минут; кроме того, было выявлено, что 87% сотрудников после подобного обучения начали по-другому относиться к гостям[7].

3. The Cosmopolitan Las Vegas. Отель The Cosmopolitan Las Vegas создал виртуальную реальность, которая помогла гостям ознакомиться с множеством различных мест в отеле, а также событий, мероприятий и культурных мероприятий в городе Лас-Вегас.

Кроме отелей, Управление города для привлечения новых туристов разработало целую стратегию, слоган которой «Вегас: Измените свою реальность». Лас-Вегас - это место, известное своими интегрированными курортами, которые предлагают посетителям азартные игры, развлечения, шопинг и изысканные блюда. Чтобы привлечь внимание путешественников, которые еще не внесли Лас-Вегас в список своих путешествий, Управление по делам конвенций и посетителей Лас-Вегаса стремится донести до них информацию о разнообразии предлагаемых в Вегасе продуктов и позиционировать сказочный город как инновационное направление. В декабре 2018 года Управление запустило кампанию Vegas: Alter Your Reality campaign, чтобы предложить потенциальным гостям 360° виртуальный художественный опыт. Благодаря уникальному и первому в своем роде опыту, все художественные опыты были призваны завлечь людей посетить Вегас. Во время Недели искусств в Майами в декабре 2017 года работы были представлены в галерее Zadok. Посетители могли получить иммерсивный VR-опыт этих художественных репрезентаций Вегаса и увидеть физическое представление работ в галерее. Во время Недели искусств в Майами было зарегистрировано в общей сложности 11 837 просмотров изображения Лас-Вегаса, сделанного художником с помощью VR HMD. Также было зарегистрировано более 2,7 миллиона просмотров VR-передачи на YouTube [9].

5. Four seasons Hotels and Resorts.

В ноябре 2019 года Four Seasons Resort Oahu at Ko Olina Hawaii сотрудничал с иммерсивной велнес-компанией, основанной доктором Адамом Газзали, нейробиологом, и доктором Алексом Теори, психологом, чтобы разработать первый в мире мультисенсорный

велнес VR для клиентов своего Spa & Wellness Centre (Parker, 2020). Учитывая растущее число людей, страдающих от тревоги и депрессии, целью этого сотрудничества была разработка инновационного решения, которое помогло бы их клиентам вернуться в состояние спокойствия. Клиенты могут выбрать "Смешанную реальность" из меню спа-процедур, чтобы расслабиться и насладиться глубоким массажем мозга. Процедура предлагает 20-минутный сеанс "Расслабление", 20-минутный сеанс "Восстановление" или 40-минутный опыт "Полный спектр", или даже комбинацию любых двух сеансов. Клиенты могли видеть, слышать, чувствовать и осязать во время виртуального путешествия природу, а также получать визуальные VR-процедуры, ароматерапию, звуко- и музыкотерапию, виброакустическую стимуляцию, природотерапию и практику осознанности во время таких путешествий, как Deep Space, Ocean Cove, Zen Garden, Crystal Cave, Lost Jungle, Floating Clouds и Deep Space [5].

Список литературы

1. Виртуальная реальность в гостиничном бизнесе. [Электронный ресурс] // Режим доступа: <http://prohotelia.com/2017/05/virtual-reality-and-hotels/> (дата обращения: 20.03.2022)
2. Виртуальная реальность в бизнесе: изменение игры для сбоев в отрасли. [Электронный ресурс] // Режим доступа: <https://www.linezero.com/blog/virtual-reality-in-business> (дата обращения: 21.06.2023)
3. Виртуальный тур по отелю: влияние COVID 19 на тенденции к виртуальной реальности в туристической индустрии. [Электронный ресурс] // Режим доступа: <https://www.yoair.com/ru/blog/virtual-hotel-tour-experience-effects-of-covid-19-on-trends-towards-virtual-reality-in-the-travel-industry/> (дата обращения 13.02.2022).
4. Чуланова О.Л., Буяр В.А. VR-технологии в обучении персонала как глобальный технологический тренд: Актуальные вопросы управления персоналом и экономики труда. Материалы VI научнопрактической конференции. 2020. С. 394-400.
5. Оздоровительные путешествия получают высокотехнологичную модернизацию. [Электронный ресурс] // Режим доступа: <https://www.forbes.com/sites/jenniferleighbarker/2020/02/17/wellness-travel-gets-a-high-tech-upgrade/?sh=2bcbdfbd2e63> (дата обращения: 21.06.2023)
6. Виртуальная реальность и современный туризм, Журнал "Будущее туризма", том 7 № 2, стр. 245-250. [Электронный ресурс] // Режим доступа: <https://doi.org/10.1108/JTF-01-2020-0004> (дата обращения: 26.04.2023)
7. Виртуальная реальность помогла сотрудникам Hilton взглянуть на мир глазами клиентов. [Электронный ресурс] // Режим доступа: <https://business.oculus.com/case-studies/hilton/> (дата обращения: 16.06.2023)
8. Marriott Hotels Introduces The First Ever In-Room Virtual Reality Travel Experience. [Электронный ресурс] // Режим доступа: <https://news.marriott.com/news/2015/09/09/marriott-hotels-introduces-the-first-ever-in-room-virtual-reality-travel-experience> (дата обращения: 20.03.2022)
9. Маркетинг виртуальной реальности в гостеприимстве и туризме. Достижения в сфере гостиничных и информационных технологий. [Электронный ресурс] // Режим доступа: <https://www.doi.org/10.5038/9781732127586>

10. VR-технологии: эффективный инструмент для обучения персонала [Электронный ресурс] // Режим доступа: <https://www.m.eprussia.ru/epr/321-322/9675377.htm> (дата обращения: 25.05.2023)

References

1. Virtual reality in the hospitality industry. [Electronic resource] // Mode of access: <http://prohotelia.com/2017/05/virtual-reality-and-hotels/> (access date: 20.03.2022)
 2. Virtual reality in business: changing the game for disruption in the industry. [Electronic resource] // Access mode: <https://www.linezero.com/blog/virtual-reality-in-business> (access date: 21.06.2023)
 3. Virtual hotel tour: the impact of COVID 19 on virtual reality trends in the travel industry. [Electronic resource] // Mode of access: <https://www.yoair.com/ru/blog/virtual-hotel-tour-experience-effects-of-covid-19-on-trends-towards-virtual-reality-in-the-travel-industry/> (date of reference: 13.02.2022).
 4. Chulanova O.L., Buyar V.A. VR-technologies in personnel training as a global technological trend: Current issues of personnel management and labor economics. Proceedings of the VI Scientific and Practical Conference. 2020. С. 394-400.
 5. Recreational travels get high-tech modernization. [Electronic resource] // Mode of access: <https://www.forbes.com/sites/jenniferleighbarker/2020/02/17/wellness-travel-gets-a-high-tech-upgrade/?sh=2bcdbfd2e63> (date of reference: 21.06.2023)
 6. Virtual reality and modern tourism, Journal of the Future of Tourism, Vol. 7 No. 2, pp. 245-250. [Electronic resource] // Mode of access: <https://doi.org/10.1108/JTF-01-2020-0004> (reference date: 26.04.2023)
 7. Virtual reality helped Hilton employees to look at the world through the eyes of clients. [Electronic resource] // Access mode: <https://business.oculus.com/case-studies/hilton/> (access date: 16.06.2023)
 8. Marriott Hotels Introduces The First Ever In-Room Virtual Reality Travel Experience. [Electronic resource] // Access mode: <https://news.marriott.com/news/2015/09/09/marriott-hotels-introduces-the-first-ever-in-room-virtual-reality-travel-experience> (access date: 20.03.2022)
 9. Virtual reality marketing in hospitality and tourism. Advances in hotel and information technology. [Electronic resource] // Mode of access: <https://www.doi.org/10.5038/9781732127586>
 10. VR-technology: effective tool for staff training [Electronic resource] // Mode of access: <https://www.m.eprussia.ru/epr/321-322/9675377.htm> (access date: 25.05.2023).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

АНАЛИЗ ИТ-АРХИТЕКТУРЫ ДЕПАРТАМЕНТА УПРАВЛЕНИЯ ПРОЕКТАМИ

¹Кириллина Ю.В., ²Олейник А.С.

ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, просп. Вернадского, 78, стр. 4), e-mail: ¹jvk05@mail.ru, ²olejnik.a.s@edu.mirea.ru

Данная статья посвящена анализу существующей ИТ-архитектуры компании Warner Music Russia, определяющей взаимодействие различных компонентов ИТ-системы и их использование для поддержки бизнес-процессов. Авторы представляют ИТ-архитектуру Департамента управления проектами компании в нотации Cisco и приводят её анализ, предлагая решения для улучшения сетевой инфраструктуры. Статья содержит предложения по применению новых технологий и программных продуктов, а также изменений в ИТ-системе компании для улучшения её эффективности. Исследование позволяет лучше понимать значимость ИТ-архитектуры для повышения эффективности работы компании и улучшения её бизнес-процессов.

Ключевые слова: Уровни ИТ-архитектуры, анализ ИТ-архитектуры, особенности ИТ-архитектуры, безопасность, рекомендации для улучшения.

ANALYSIS OF THE IT ARCHITECTURE OF THE PROJECT MANAGEMENT DEPARTMENT

¹Y.V. Kirillina, ²A.S. Oleynik

MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, p. 4), e-mail: ¹jvk05@mail.ru, ²olejnik.a.s@edu.mirea.ru

This article analyzes Warner Music Russia's existing IT architecture, which defines the interaction of various IT system components and their use to support business processes. The authors present the IT architecture of the company's Project Management Department in Cisco notation and analyze it, suggesting solutions to improve the network infrastructure. The paper provides suggestions on how to apply new technologies and software products, as well as changes in the company's IT system to improve its efficiency. The study provides a better understanding of the importance of IT architecture to improve the company's efficiency and business processes.

Keywords: Levels of IT architecture, analysis of IT architecture, features of IT architecture, security, recommendations for improvement.

ИТ-архитектура предприятия — это высокоуровневое описание систем и компонентов ИТ-инфраструктуры компании, которое обеспечивает ее бизнес-потребности и цели. Она определяет, как различные компоненты ИТ-системы компании взаимодействуют между собой, какие технологии и программные продукты используются, а также как эти системы поддерживают бизнес-процессы компании [1].

ИТ-архитектура предприятия состоит из нескольких уровней, которые определяют различные аспекты ИТ-инфраструктуры компании. Эти уровни включают в себя:

1. Уровень бизнес-архитектуры: определяет бизнес-цели и стратегии компании, а также их связь с ИТ-инфраструктурой.

2. Уровень приложений и данных: описывает приложения, базы данных и связи между ними, используемые в компании.

3. Уровень технической архитектуры: определяет технические аспекты ИТ-инфраструктуры, такие как сервера, хранилища данных, сети, безопасность и т.д.

4. Уровень операционной архитектуры описывает процессы, используемые в управлении инфраструктурой, включая управление изменениями, конфигурации, управления рисками и т.д.

ИТ-архитектура предприятия позволяет компании лучше понимать свою ИТ-инфраструктуру, увеличивать ее эффективность и уменьшать затраты на ее обслуживание. Она также помогает сокращать время на реализацию новых бизнес-процессов и разработку новых ИТ-проектов, а также обеспечивает лучшую безопасность и управление рисками. На Рисунке 1 представлена ИТ-архитектура Департамента управления проектами компании Warner Music Russia, реализующего основные бизнес-процессы организации, в нотации Cisco [2].

ИТ-инфраструктура является централизованной и охватывает все подразделения компании. Каждый отдел имеет свою подсеть, которая включена в общую топологию сети. Отделы связаны между собой выделенными каналами связи, что обеспечивает быстрое и надежное соединение между различными узлами сети.

Вся ИТ-инфраструктура компании управляется централизованно через технический отдел, который отвечает за обеспечение безопасности, мониторинг, обновление и поддержку всех сетевых устройств, серверов и приложений. Кроме того, технический отдел осуществляет контроль доступа к сети, что позволяет защитить конфиденциальную информацию компании от несанкционированного доступа [3].

Основной серверный парк состоит из серверов различных типов, включая файловые, веб-серверы, серверы баз данных, серверы приложений, а также серверы виртуализации. Каждый сервер выполняет свои функции и предназначен для определенных задач, что обеспечивает эффективное использование ресурсов и повышает производительность работы компании.

Для управления всей ИТ-инфраструктурой компании используются специальные сервера управления, которые позволяют контролировать работу сети и всех подключенных устройств. Эти сервера осуществляют мониторинг состояния сети и уведомляют о возможных проблемах или сбоях, что позволяет быстро реагировать на них и предотвращать потенциальные проблемы [4].

Таким образом, централизованная ИТ-инфраструктура компании Warner Music Russia обеспечивает высокую производительность и безопасность работы всей компании. Контроль и управление сетью через технический отдел позволяет оперативно решать возникающие проблемы и обеспечивать эффективное использование ресурсов.

Нужно отметить, что безопасность сети является одним из наиболее важных аспектов ИТ-инфраструктуры любой компании, включая Warner Music Russia. Компания должна иметь соответствующие меры безопасности для защиты от несанкционированного доступа к данным и снижения риска утечки конфиденциальной информации [5].

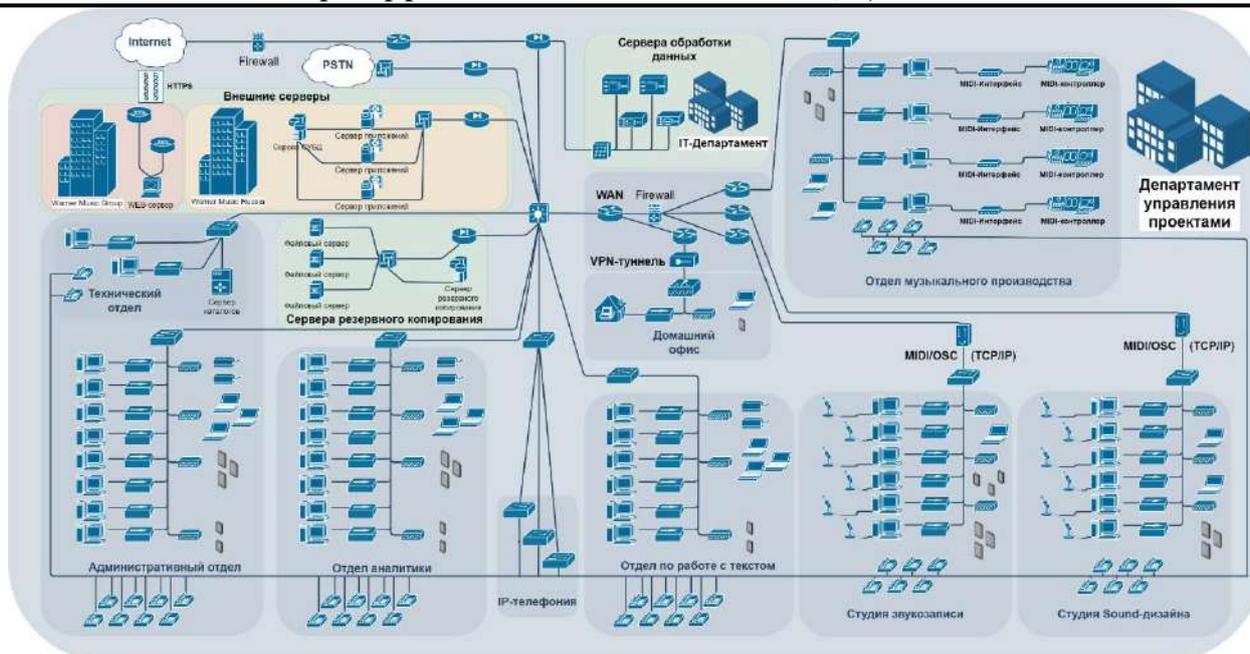


Рисунок 1 – ИТ-архитектура Департамента управления проектами Warner Music Russia

Одной из важных мер по обеспечению безопасности является ограничение прав доступа к сетевым ресурсам. Для этого в компании используется система управления доступом, которая обеспечивает контроль доступа к ресурсам на основе ролей и прав пользователей. Это позволяет предотвратить несанкционированный доступ к конфиденциальной информации и снизить риски в случае утечки данных.

Дополнительной мерой по обеспечению безопасности является анализ и фильтрация трафика. В компании установлены специальные средства, позволяющие анализировать трафик, проходящий через сеть. Это позволяет выявлять и блокировать потенциально опасные соединения, такие как атаки на сетевую инфраструктуру и шпионские программы.

Все точки выхода из сети экстранета компании надежно защищены с помощью файервола, который предотвращает несанкционированный доступ к корпоративным ресурсам. VPN-туннелирование применяется при удаленной работе сотрудников, или при работе с корпоративными ресурсами в командировке и т.д., для защиты данных и обеспечения конфиденциальности. Дополнительные меры, такие как ограничение доступа, контроль доступа и анализ трафика, также применяются для защиты ИТ-инфраструктуры от внешних и внутренних угроз. В целом, система безопасности компании позволяет управлять доступом к информации, защищать её и обеспечивать конфиденциальность.

Сервера резервного копирования играют важную роль в ИТ-инфраструктуре Warner Music Russia. Они обеспечивают сохранность и защиту данных в случае сбоев в работе основных серверов, систем хранения данных или сетевых устройств. В случае их неполадок, сервера резервного копирования автоматически включаются, чтобы поддерживать бесперебойную работу всей системы.

Серверы приложений отвечают за обработку запросов клиентских приложений и их поддержку. Для оптимальной работы системы, топология сети предусматривает распределение нагрузки между различными узлами сети. Это позволяет балансировать нагрузку и повышать производительность всей системы. Для этого используются специальные

алгоритмы, которые позволяют автоматически распределять нагрузку между серверами приложений.

PSTN (Public Switched Telephone Network) — это общественная коммутируемая телефонная сеть, используемая для передачи голосовой и факсимильной связи. PSTN состоит из коммутаторов, телефонных линий и других сетевых элементов, которые позволяют соединять абонентов между собой. PSTN надёжна и обеспечивает корпоративную телефонию, связи с партнерами и клиентами.

В рамках анализа ИТ-архитектуры был выявлен «рациональный» тип ИТ-инфраструктуры. Анализ показал следующие особенности:

1. Централизованное управление осуществляется через технический отдел, который подчиняется ИТ-Департаменту.
 2. Для централизованного администрирования используются службы каталогов и групповых политик.
 3. Контроль и мониторинг функционирования ПО и аппаратного обеспечения автоматизирован.
 4. На рабочих местах установлена антивирусная защита.
 5. Для всех серверов и рабочих станций организовано резервное копирование и восстановление.
 6. Для корпоративных ресурсов организован удаленный доступ через VPN-туннелирование.
 7. Центральный межсетевой экран реализован на программном уровне.
 8. Для изоляции серверов и важных узлов сети используется IPSec.
- Улучшение ИТ-архитектуры может быть реализовано через:
1. Внедрение технологий автоматизации управления идентификацией.
 2. Использование System Management Server для управления серверами.
 3. Управление образами рабочих станций.

Организация защищенного беспроводного сетевого доступа через службу Internet Authentication Service (IAS).

Список литературы

1. Алджанов, В. ИТ-архитектура. Практическое руководство от А до Я. Первое издание / В Алджанов. — Москва: Издательские решения, 2018. — 1380 с.
2. Амато, В. Основы организации сетей Cisco. Том 1. Исправленное издание / Вито Амато. — Москва: Вильямс, 2004. — 250 с.
3. Theorg. [Электронный ресурс] / Warner Music Group. — Режим доступа: <https://theorg.com/org/warner-music-group/>, свободный. Загл. с экрана. Яз. англ. Дата обращения (15.05.2023).
4. Warner music. [Электронный ресурс] / Warner Music Russia. История компании. — Режим доступа: <http://warnermusic.ru/about-back/history/>, свободный. Загл. с экрана. Яз. рус. Дата обращения (16.05.2023).
5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. — Москва: ФОРУМ, 2022. — 416 с.

References

1. Aldzhanov, V. IT Architecture. A practical guide from A to Z. First edition / V Aldzhanov. — Moscow: Izdatel'skie resheniia Publ., 2018. — 1380 p.
 2. Amato, V. Fundamentals of Cisco networking. Volume one. Revised edition/ Vito Amato. — Moscow: Vil'iams, 2004. —.250 p.
 3. Theorg. [Electronic resource] / Warner Music Group. — Available at: <https://theorg.com/org/warner-music-group/>, free. Screen title. English. Date of access (15.05.2023).
 4. Warner music. [Electronic resource] / Warner Music Russia. Istoriia kompanii. — Available at: <http://warnermusic.ru/about-back/history/>, free. Screen title. Data obrashcheniia (16.05.2023).
 5. SHan'gin V.F. Information security of computer systems and networks / V.F. SHan'gin. — Moskva: FORUM, 2022. — 416 p
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

АНАЛИЗ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СФЕРЕ СТРОИТЕЛЬНОГО КОНТРОЛЯ АВТОМОБИЛЬНЫХ ДОРОГ

Яшин С.О., ¹Соловьев Я.А.

ФГАОУ ВО «Северо-Кавказский Федеральный Университет», Ставрополь, Россия (355017, г. Ставрополь, ул. Пушкина, 1), e-mail: ¹yarsolv@yandex.ru

Строительный контроль автомобильных дорог включает в себя множество задач, связанных с обеспечением безопасности дорожного движения и соблюдением требований к качеству дорожной инфраструктуры. В последние годы все большее значение приобретают цифровые технологии, которые способствуют улучшению эффективности и точности проведения строительного контроля.

Ключевые строительный контроль; цифровые технологии; БПЛА; BIM-технологии; автомобильные дороги; строительство.

ANALYSIS OF THE USE OF DIGITAL TECHNOLOGIES IN THE FIELD OF CONSTRUCTION CONTROL OF HIGHWAYS

Yashin S.O., ¹Soloviev Ya.A.

North Caucasus Federal University, Stavropol, Russia (355017, Stavropol, 1A Pushkin Street), e-mail: ¹yarsolv@yandex.ru

The construction control of highways includes many tasks related to ensuring road safety and compliance with the requirements for the quality of road infrastructure. In recent years, digital technologies have become increasingly important, which contribute to improving the efficiency and accuracy of construction control.

Keywords: construction control; digital technologies; UAVs; BIM technologies; highways; construction.

Современные цифровые технологии активно применяются во всех секторах экономики и не стали исключением для сферы строительного контроля автомобильных дорог. В данной области цифровые технологии применяются для повышения точности и эффективности контроля качества дорожного покрытия, а также для улучшения эргономики труда инженеров и специалистов, занятых в строительстве и контроле автомобильных дорог. В данном исследовании будут рассмотрены современные технологии, используемые в сфере строительного контроля автомобильных дорог, и их положительный вклад в повышение качества дорожного покрытия.

Технологии цифрового контроля являются одним из ключевых инструментов в процессе строительства и управления дорожными системами. Они позволяют сократить время, затрачиваемое на обследование, анализ и оценку качества дорожного покрытия, а также увеличивают точность и детализацию данных, получаемых при проведении контрольных мероприятий. Среди таких технологий можно выделить системы контроля шероховатости

дорог, автоматические системы термического контроля, геодезические системы, используемые для измерения поверхности и высотных отметок дорожного покрытия и другие.

Повышение эффективности контроля качества дорожного покрытия, осуществляемого с помощью цифровых технологий, способствует улучшению безопасности на дорогах, сокращению времени, затрачиваемого на ремонт и обслуживание дорог, а также позволяет снизить экологическую нагрузку на окружающую среду.

Таким образом, применение цифровых технологий в сфере строительного контроля автомобильных дорог имеет важное значение для обеспечения высокого качества дорожного покрытия и обеспечения безопасности дорожного движения. В дальнейшем, развитие этих технологий будет способствовать улучшению дорожной инфраструктуры в целом и повышению качества жизни населения.

Применение программных комплексов на этапе документооборота между всеми участниками строительства. Применение программных комплексов на этапе документооборота между всеми участниками строительства является необходимым для обеспечения эффективной работы и сокращения времени на выполнение административных процедур.

Вот примеры программных комплексов:

- Программный комплекс «СтройКонтроль», (Участник II Всероссийского открытого конкурса «ВМ-технологии 2017», Специальная номинация: «ВМ-идея года»);

Как отмечается на официальном сайте, это информационная система для наведения порядка в работе строительного контроля и автоматизация выдачи предписаний с помощью мобильных устройств. Применение снижает дополнительные расходы на строительство за счет повышения эффективности взаимодействия всех участников строительства. В среднем, использование подобных решений сокращает сроки приемки объекта в 2 раза, а бюджет на доработки – на 25%.

- «EXON Управление строительством»;

Этот программный комплекс призван объединять всех участников строительства. Такая платформа обеспечивает структурированное хранение документации, быстрая передача задач новому специалисту и прозрачность выполнения работ; простое формирование, проверка, редактирование и согласование сокращают время на доработку документации; система для всех участников строительства с различным уровнем доступа, которая сохраняет данные по всем видам работ; онлайн-проверку документации и возможность последовательного или параллельного согласования и многое другое для проведения качественного строительного контроля.

- «Vitro-CAD» (входит в Реестр отечественного ПО (Приказ Минкомсвязи России № 203 от 19.05.2016, Приложение №1)) – система управления проектно-сметной документацией, позволяющая проектным организациям значительно повысить эффективность управления инженерными данными и облегчить выполнение множества повседневных задач проектировщика. Об этом программном комплексе более подробно будет рассмотрено ниже.

Новейшее программное обеспечение, установленное на ПК специалистов организации, позволяет выполнять задачи любой сложности по обработке информации, а также по её сбору и безопасному хранению.

Для координации работы по рассмотрению рабочей, технологической и проектной документации рассмотрим программное обеспечение Vitro-CAD.

К целям разработки модуля технической экспертизы Vitro-CAD можно отнести рассмотрение следующих видов документации и запросов:

- Проектная документация;
- Рабочая документация;
- Технологическая документация;
- Запросы на согласование технических решений;
- Запросы на согласование материалов субподрядчиков и поставщиков.

Вся вышеперечисленная документация хранится в электронном виде и доступна для всех участников процесса документооборота. Участниками являются: канцелярия, диспетчер проекта, технические эксперты, согласующий руководитель, подписывающий руководитель, переводчики.

К задачам, решаемым данным модулем можно отнести:

- Регистрация и хранение входящих писем и документов;
- Выдача поручений исполнителям (техническим экспертам);
- Контроль исполнения поручений;
- Согласование результатов исполнения поручений руководителем и Заказчиком;
- Автоматическое ведение отчетности;
- Подготовка исходящих писем для Заказчика.

Жизненный цикл процесса начинается с работы канцелярии. Она регистрирует входящий документ, который поступает на рассмотрение и направляет диспетчеру проекта. Диспетчер проекта инициирует поручение на рассмотрение материалов для технического эксперта. Эксперт рассматривает документацию и оформляет свое заключение в системе. После этого автоматически результаты рассмотрения направляются согласующему руководителю. Он может согласовать или отправить на доработку с комментариями. Если есть необходимость диспетчер согласовывает с заказчиком, либо после выполнения поручения оформляет исходящее письмо, смотреть рисунок 1.

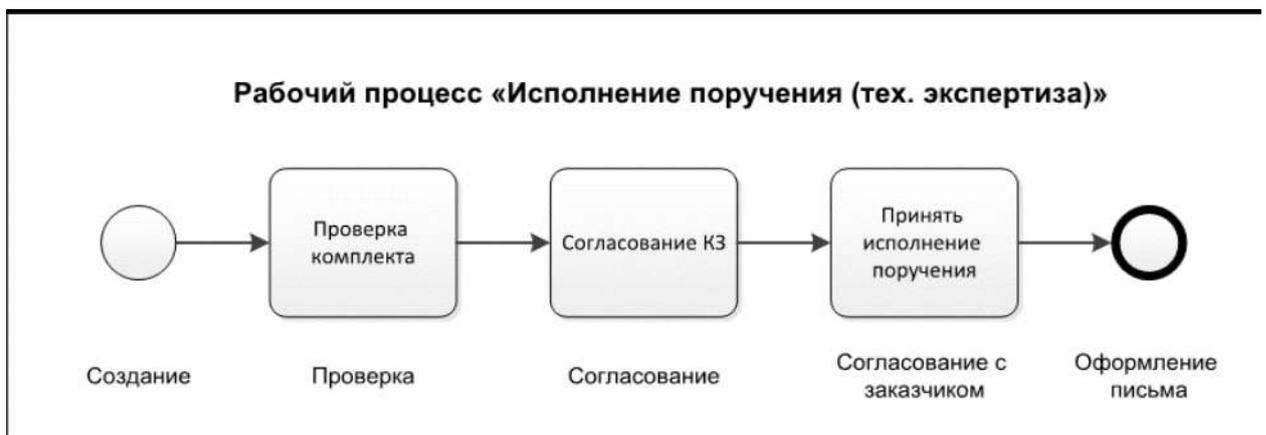


Рисунок 1 – Жизненный цикл процесса технической экспертизы в Vitro-CAD

Таким образом, программные комплексы позволяют автоматизировать процесс обмена документами между всеми участниками строительства, упрощая и ускоряя процесс подготовки и согласования необходимой документации. Благодаря этому, сокращается время

на выполнение административных процедур и улучшается координация между всеми участниками строительства.

Применение интеллектуальной летательной системы при строительном контроле.

В наши дни без очень стремительно развивается технологический процесс. В современном строительстве без точных приборов, таких как нивелиры, тахеометры, теодолиты, дальнометры и т.п. не обойтись. Но все это оборудование должно постоянно совершенствоваться, для того чтобы повышать точность при производстве работ, тем самым повышая качество выполненных работ. Но, как бы не были совершенны эти приборы, насколько бы они не были точны, человеческий фактор играет очень важную роль, поэтому развиваться нужно в сторону исключения человеческого фактора, т.е. исключать участие человека при проведении замеров.

Дроны (ИЛС/БПЛА) являются производительным методом для обеспечения жизнедеятельности объекта. Далее представлен список задач, которые они могут решать, при использовании их в сфере строительства:

- Обследование труднодоступных и протяженных линейных объектов (элементы мостов, газопроводы, ГЭС, ТЭС, линии электропередач и т.п.);
- Проведение необходимых измерений (расстояние, влажность, температура, давление, скорость ветра и т.п.);
- Осуществление фотофиксации и видеофиксации со стройплощадки;
- Создание картографических материалов;
- Контроль точности монтажа строительных конструкций;
- Взятие проб воздуха;
- Замеры уровней шума, радиации;
- Трансляция видеозахвата в реальном времени.

Кроме этих задач, БПЛА в строительстве могут служить хорошим помощником и для рабочих, так как могут выполнять доставку небольших грузов или осуществлять монтаж на высотных объектах. Благодаря данному функционалу дронов можно значительно снизить риски и травмы при работе на высоте, также вред от некоторых строительных материалов. К способам использования данной техники также можно отнести поиск несанкционированных свалок и выявления незаконных построек.

Интеллектуальные летательные системы (ИЛС) являются эффективным инструментом для проведения строительного контроля в сфере автодорог. Они позволяют получать высокоточные данные о состоянии объекта, быстро обрабатывать их и получать результаты, что значительно сокращает время и улучшает качество контроля.

Рассмотрим преимущества применения БПЛА в строительном контроле:

1. Возможность дистанционного обследования участков строительства:
 - Без необходимости приостанавливать работы;
 - Высокая степень автоматизации процесса обработки;
 - Группа камеральной обработки может размещаться удаленно.
2. Сокращение трудозатрат при осуществлении работ по сбору данных на протяженных участках:
 - Уменьшение количества персонала;

- Уменьшение времени, необходимого для выполнения работ по сбору данных на протяженных участках объектов строительства.

Как мы можем убедиться, использование ИЛС (БПЛА) может существенно упростить задачу человека, осуществляющий строительный контроль, а также существенно удешевить и без того дорогой процесс строительного контроля. Использование БПЛА в качестве инструмента все ближе к нынешним реалиям, выходящим за границу медиа и развлекательной сферы.

Применение BIM-технологий для мониторинга хода строительства. BIM технологии (Building Information Modeling) представляют собой инновационный подход к проектированию, строительству и эксплуатации объектов инфраструктуры, который позволяет улучшить качество и эффективность строительного процесса.

Применение BIM-технологий позволяет принимать эффективные решения на всех стадиях жизненного цикла зданий - от инвестиционного закрытия до эксплуатации и до демонтажа. Это важно и для бюджетных затрат, и для строительства и эксплуатации любого объекта.

Что входит в жизненный цикл объекта строительства (рисунок 2).



Рисунок 1.2 – Жизненный цикл объекта строительства

Можно выделить важные преимущества при использовании BIM-технологий и моделей объектов:

1. Улучшение точности и качества проектирования. Благодаря использованию BIM технологий, проектировщики могут создавать детальные 3D-модели дорожных объектов, которые позволяют увидеть все аспекты проекта в одном месте. Это помогает избежать ошибок и проблем, которые могут возникнуть в процессе строительства.

2. Оптимизация бюджета и сокращение сроков строительства. Благодаря BIM технологиям, проект можно оптимизировать до мельчайших деталей, что позволяет снизить затраты на строительство и сократить сроки проекта.

3. Улучшение координации и сотрудничества между участниками проекта. BIM модель позволяет разным участникам проекта работать в одной общей среде, что улучшает коммуникацию и сотрудничество между ними.

4. Лучшее управление проектом и более точный контроль за выполнением работ. BIM модель позволяет отслеживать выполнение работ в режиме реального времени, что помогает контролировать прогресс проекта и своевременно реагировать на любые проблемы.

5. Улучшение качества и безопасности дорожных объектов. Благодаря использованию BIM технологий, можно улучшить качество и безопасность дорожных объектов, так как проектировщики смогут предвидеть и устранить любые потенциальные проблемы, связанные с проектированием и строительством.

Такая технология внедрена в строительство потому что она призвана облегчить, удешевить проект, а также сократить сроки производства работ. Как правило все участники строительства обменивались информацией с помощью бумажных носителей, например, письма, которые доставлялись Почтой России или другими почтовыми организациями, проектная документация, передаваемая так же заказными письмами или на твердом носителе, заключение экспертизы, сметная документация, акты строительного контроля и т.д. Благодаря строительной информационной модели, решаются ряд задач в строительной деятельности:

- Контроль проведения работ на строительной площадке;
- Мониторинг исполнения графика работ по объекту;
- План-фактный анализ производства работ с визуализацией на трехмерной модели сооружения;
- Сбор и хранение информации об объектах транспортной инфраструктуры на протяжении всего жизненного цикла;
- Привязка нормативной, разрешительной и исполнительной документации к элементам сооружения или всему сооружению;
- Своевременная актуализация информации;
- Наглядное представление информации на трехмерной модели с привязкой к элементам (сегментам) объекта;
- Фиксация нарушений и с возможностью фото- и видео- фиксации;
- Визуальный инструмент для принятия управленческих решений.

Применение XR технологий.

XR Технологии - создают условия понятной для клиента презентации объекта строительства и его этапов. Технология VR - это виртуальная реальность, которая позволяет более детально ознакомиться с технически сложными решениями модели для объекта. Технология AR - дополненная реальность.

Платформа VR – дает возможность представлять технически сложные конструкционные решения строительного объекта с помощью технологий виртуальной реальности.

Платформа AR (дополненная реальность) чаще используется для решения задач по обучению специалистов. С применением такой технологии работники могут выполнять различные операции по онлайн инструкции.

Что получит ваш специалист строительного контроля от технологий XR:

- Экономия времени за счет быстрого согласования проекта с клиентом. Благодаря VR понимание, как будет реализован проект, формируется быстрее.
- Демонстрацию последовательности сборки по сложным решениям объекта;
- Доступ к списку материалов для грамотного планирования;
- Предварительную сборку конструкции в виртуальном режиме с целью обучения персонала;

Сохраненные в программе 3D-модели отображаются на дисплее мобильного устройства в трех вариантах:

режим AR - дополненная реальность. Виртуальная 3D-модель создается после запуска приложения, когда камера фокусируется на распечатанном плане здания;

режим VR - виртуальная реальность. 3D-модели можно просматривать простыми жестами пальцев, используя различные функции - например, масштабирование, поворот;

режим MR - смешанная реальность. 3D-модель в оригинальном размере проецируется на строительную площадку.

При применении XR технологий значительно сокращается вероятность ошибок - благодаря 3D-моделированию коллизии устраняют еще на этапе проектирования, а это в свою очередь позволяет соблюдать запланированный график работ без задержек на внесение корректировок и дополнительных затрат. Также можно совместить технологию БПЛА и XR для быстрого, а главное безопасного осмотра и оцифровки сооружения в опасных для человека местах. Для этого потребуется вооружить БПЛА специальной камерой и датчиками, необходимыми для сканирования сооружения. В конечном итоге специалист, ничем не рискуя, может обследовать часть сооружения при помощи вышеперечисленных AR/VR технологий в мельчайших подробностях.

Список литературы

1. Топчий Д.В., Скакалов В.А. Разработка организационно-технологической модели осуществления строительного контроля при возведении многоэтажных жилых зданий // журнал «Научное обозрение» Издательство: Издательский дом "Наука образования" г. Москва, ISSN: 1815-4972.
2. Топчий Д.В., В.А. Скакалов «Структурно функциональное моделирование многоуровневых и многокритериальных связей организационно-технологических, управленческих структур и информационного обеспечения при осуществлении строительного контроля в ходе перепрофилирования промышленных объектов» // журнал «Перспективы науки» №10 (97), ISSN 2077-6810, С. 44- 48.
3. Бойков В.Н., Неретин А.А., Скворцов А.В. Апробирование информационных моделей дорог на стадии реализации проектов // САПР и ГИС автомобильных дорог. 2015. No 2(5). DOI: 10.17273/CADGIS.2015.2.5, С. 30–36
4. Ассоциация электронных коммуникаций (РАЭК). URL: <http://raec.ru/live/position/9547/>.
5. Васильева, Н.В., Бачуринская, И.А. Проблемные аспекты цифровизации строительной отрасли // Вестник Алтайской академии экономики и права - 2018 - №7. - С. 39-46.

References

1. Topchiy D.V., Skakalov V.A. Development of an organizational and technological model for the implementation of construction control during the construction of multi-storey residential buildings // journal "Scientific Review" Publishing House: Publishing House "Science of Education", Moscow, ISSN: 1815-4972.
 2. Topchiy D.V., V.A. Skakalov "Structural and functional modeling of multilevel and multicriteria connections of organizational, technological, managerial structures and information support in the implementation of construction control during the conversion of industrial facilities" // Journal "Prospects of Science" No. 10 (97), ISSN 2077-6810, pp. 44-48.
 3. Boikov V.N., Neretin A.A., Skvortsov A.V. Approbation of information models of roads at the stage of project implementation // CAD and GIS of highways. 2015. No 2(5). DOI: 10.17273/CADGIS.2015.2.5, pp. 30-36
 4. Association of Electronic Communications (RAEC). URL: <http://raec.ru/live/position/9547>
 5. Vasilyeva, N.V., Bachurinskaya, I.A. Problematic aspects of digitalization of the construction industry // Bulletin of the Altai Academy of Economics and Law - 2018 - No. 7. - pp. 39-46..
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 65.011.56

РОЛЬ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ПРОЦЕССОВ В ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ

Дементьев С.Ю., ¹Воробьев В.В.

ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», Красноярск, Россия (660037, Красноярский край, город Красноярск, проспект имени газеты «Красноярский рабочий», д. 3), e-mail: ¹super.wark@mail.ru

Четвертая промышленная революция характеризуется интеграцией передовых технологий в различные отрасли промышленности, что позволяет собирать и анализировать огромные объемы данных. В этом контексте интеллектуальный анализ процессов стал мощным инструментом для использования потенциала этих процессов, управляемых данными. В этой статье исследуется роль интеллектуального анализа процессов в Четвертой промышленной революции, освещаются его возможности, преимущества и проблемы. Анализируя журналы событий и генерируя полезную информацию, интеллектуальный анализ процессов позволяет организациям оптимизировать свои операции, повысить эффективность и добиться более эффективного принятия решений. В статье также обсуждаются будущие перспективы и потенциальные направления исследований в этой развивающейся области.

Ключевые слова: интеллектуальный анализ процессов, Четвертая промышленная революция, процессы, управляемые данными, оптимизация, эффективность, принятие решений.

THE ROLE OF PROCESS MINING IN THE FOURTH INDUSTRIAL REVOLUTION

Dementev S.Y., ¹Vorobyov V.V.

Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia (660037, Krasnoyarsk Krai, Krasnoyarsk city, prospect named after the newspaper "Krasnoyarsk worker", 3), e-mail: ¹super.wark@mail.ru

The Fourth Industrial Revolution (4IR) is characterized by the integration of advanced technologies into various industries, enabling the collection and analysis of vast amounts of data. In this context, process mining has emerged as a powerful tool to leverage the potential of these data-driven processes. This article explores the role of process mining in the 4IR, highlighting its capabilities, benefits, and challenges. By analyzing event logs and generating actionable insights, process mining enables organizations to optimize their operations, improve efficiency, and achieve better decision-making. The article also discusses the future prospects and potential research directions in this evolving field.

Keywords: Process mining, Fourth Industrial Revolution, data-driven processes, optimization, efficiency, decision-making.

The Fourth Industrial Revolution (4IR) encompasses the convergence of digital technologies, such as artificial intelligence (AI), big data analytics, Internet of Things (IoT), and automation, leading to significant transformations across industries. This revolution has brought about a paradigm shift in how organizations operate, process data, and make decisions. One of the key enablers in this era is process mining, a data-driven approach that leverages event logs to analyze and optimize

business processes. This article aims to explore the role of process mining in the 4IR and its potential impact on various industries [1].

Process mining is a discipline that combines techniques from data mining, business process management, and data analytics to extract valuable insights from event logs generated by information systems. It provides organizations with a visual representation of their processes, enabling them to identify bottlenecks, inefficiencies, and deviations from desired workflows. By uncovering the actual execution of processes, process mining offers an opportunity to bridge the gap between the intended and actual process, facilitating process improvement initiatives.

Leveraging Process Mining in the Fourth Industrial Revolution [2]:

1. **Data-Driven Decision Making:** In the 4IR, organizations generate massive volumes of data from various sources, including sensors, machines, and user interactions. Process mining utilizes this data to create a comprehensive understanding of processes, enabling data-driven decision making. By analyzing event logs, organizations can identify patterns, trends, and anomalies, empowering them to optimize processes and make informed decisions based on accurate and real-time information.

2. **Process Optimization and Efficiency:** Process mining provides organizations with a holistic view of their operations, helping them identify inefficiencies and areas for improvement. By visualizing process models and analyzing performance metrics, organizations can pinpoint bottlenecks, redundant activities, and resource allocation issues. These insights enable process optimization initiatives, leading to improved efficiency, reduced costs, and enhanced customer satisfaction.

3. **Compliance and Risk Management:** In the 4IR, organizations face increasingly complex regulatory requirements and risk challenges. Process mining helps organizations ensure compliance by identifying deviations from established standards and regulations. By analyzing event logs, organizations can detect non-compliant activities, potential fraud, or security breaches. Process mining also facilitates proactive risk management by providing insights into process variations and their impact on outcomes, enabling organizations to take preventive measures.

Process mining has been applied in various real-world cases across industries, showcasing its effectiveness in uncovering insights, optimizing processes, and driving improvements. Here are a few notable examples [3]:

1. **Manufacturing Optimization:** Process mining has been successfully used in the manufacturing industry to identify bottlenecks, reduce cycle times, and improve overall efficiency. By analyzing event logs from production systems, process mining techniques have helped organizations identify process variations, optimize resource allocation, and enhance product quality. This has resulted in cost savings, increased throughput, and improved customer satisfaction.

2. **Healthcare Process Improvement:** In the healthcare sector, process mining has been utilized to analyze patient pathways, identify inefficiencies, and streamline processes. By examining event logs from electronic health records, process mining has enabled hospitals to optimize patient flow, reduce waiting times, and improve care coordination. This has led to enhanced patient outcomes, increased capacity utilization, and better resource allocation.

3. **Fraud Detection and Compliance:** Process mining has proven effective in detecting and preventing fraudulent activities within organizations. By analyzing event logs and process deviations, process mining techniques can identify patterns indicative of fraud or non-compliant behavior. This has been particularly useful in industries such as finance, insurance, and procurement, where ensuring

compliance is crucial. Process mining has helped organizations proactively identify potential fraudulent activities, minimize risks, and strengthen internal controls.

4. Customer Journey Analysis: Process mining has been employed to analyze customer journeys and improve customer experience. By examining event logs from customer interaction systems, organizations can gain insights into customer behavior, preferences, and pain points. This knowledge helps optimize processes, personalize offerings, and enhance customer satisfaction. For example, in e-commerce, process mining has been used to identify and resolve bottlenecks in the ordering and delivery process, leading to improved customer retention and increased sales.

5. Supply Chain Optimization: Process mining has been utilized to optimize supply chain processes, improve inventory management, and enhance logistics operations. By analyzing event logs from various systems involved in the supply chain, organizations can identify inefficiencies, track order fulfillment, and optimize transportation routes. This has resulted in reduced costs, minimized stockouts, and improved supply chain visibility and agility.

6. IT Service Management: Process mining has been applied in IT service management to analyze IT processes, identify performance bottlenecks, and enhance service delivery. By analyzing event logs from IT systems and service desk platforms, organizations can gain insights into response times, incident resolution, and resource allocation. This helps optimize IT processes, improve service quality, and reduce downtime, leading to increased productivity and customer satisfaction.

These real-life cases demonstrate the versatility and value of process mining across industries. From manufacturing and healthcare to finance and customer service, process mining offers organizations valuable insights and actionable recommendations to optimize their processes, enhance efficiency, and deliver better outcomes.

The implementation prospects for process mining in Russia are promising. While the adoption of process mining in Russia is still in its early stages, there is growing recognition of its potential benefits across various industries. Here are some key factors influencing the prospects for process mining implementation in Russia [3]:

1. Digital Transformation Initiatives: Russia has been actively pursuing digital transformation initiatives to modernize its industries and improve competitiveness. Process mining aligns well with these goals by leveraging data analytics to optimize processes and enhance operational efficiency.

2. Increasing Data Availability: With the advancement of digital technologies and the growing digitization of processes, there is a significant increase in the availability of data in Russia. This data can be harnessed through process mining techniques to gain insights and drive improvements.

3. Industry-Specific Applications: Process mining can be applied across a wide range of industries in Russia, including manufacturing, energy, finance, healthcare, and logistics. Each industry can benefit from process optimization, cost reduction, and enhanced decision-making enabled by process mining.

4. Regulatory Compliance: Russia has specific regulatory requirements in various sectors. Process mining can play a vital role in ensuring compliance by identifying non-compliant activities, detecting anomalies, and enhancing transparency in processes.

5. Collaboration and Knowledge Exchange: Collaboration between academia, industry, and government institutions is essential for the successful implementation of process mining. Encouraging partnerships and knowledge exchange can accelerate the adoption of process mining techniques, best practices, and skill development.

6. **Awareness and Education:** Promoting awareness about the benefits and potential of process mining is crucial for its widespread implementation in Russia. Organizations and professionals need to be educated about the value proposition of process mining and trained in the necessary skills and tools.

7. **Data Privacy and Security:** Addressing concerns related to data privacy and security is vital for the successful implementation of process mining in Russia. Ensuring compliance with data protection regulations and adopting robust security measures will build trust and confidence in the use of process mining techniques.

8. **Government Support:** Government support and policies that encourage the adoption of digital technologies and data-driven approaches can further facilitate the implementation of process mining in Russia. Initiatives such as funding for research and development, innovation programs, and industry-specific incentives can drive adoption.

Overall, the prospects for the implementation of process mining in Russia are promising, considering the ongoing digital transformation efforts, increasing data availability, and the potential benefits across various industries. However, it is essential to address challenges such as data privacy, skill development, and awareness to fully leverage the potential of process mining in Russia [5].

While intelligent process analysis, including process mining, offers numerous benefits, there can be potential negative effects or challenges associated with its implementation. One example of a negative effect is the misuse or misinterpretation of process mining results, leading to erroneous decision-making or unintended consequences.

Process mining relies on data analysis and algorithms to uncover insights and patterns within processes. However, if the results are misinterpreted or misunderstood, it can have detrimental effects on process improvement initiatives. For instance, if an organization solely focuses on optimizing a specific aspect of a process based on process mining findings without considering the broader context, it may inadvertently introduce inefficiencies in other parts of the process [5].

Let's consider an example in a customer service scenario. Through process mining, it is identified that a particular step in the customer complaint resolution process takes longer than expected. The organization decides to optimize that specific step by reducing the time allocated to it. However, without considering the reasons behind the longer duration, such as complex customer issues or the need for thorough investigation, the reduction in time allocation may result in rushed resolutions, decreased quality of service, and customer dissatisfaction [6].

In this case, the negative effect arises from the misinterpretation of process mining results, leading to suboptimal process changes that do not address the underlying factors contributing to the longer duration. It highlights the importance of considering contextual knowledge, domain expertise, and understanding the limitations of process mining to ensure appropriate actions are taken based on the insights gained [6].

To mitigate such negative effects, it is essential to approach process mining as a collaborative effort involving domain experts, process owners, and data analysts. This interdisciplinary collaboration can help ensure that the insights derived from process mining are correctly interpreted, validated, and aligned with organizational goals and objectives. Additionally, continuous monitoring and evaluation of the implemented process changes are crucial to identify any unintended consequences and make further adjustments as needed.

Overall, while intelligent process analysis, such as process mining, has significant advantages, it is essential to exercise caution in the interpretation and implementation of its findings to avoid potential negative effects and ensure optimal outcomes.

While process mining offers significant benefits in the 4IR, there are several challenges to overcome. These include data quality issues, privacy concerns, and the need for specialized skills and tools. Future research should focus on addressing these challenges and exploring advanced process mining techniques, such as real-time process monitoring, predictive analytics, and the integration of AI and machine learning algorithms. Additionally, interdisciplinary collaboration and knowledge sharing between academia, industry, and policymakers are crucial to harness the full potential of process mining in the 4IR.

Process mining plays a crucial role in the Fourth Industrial Revolution by leveraging the vast amounts of data generated by organizations. It enables data-driven decision making, process optimization, and compliance management, thereby improving operational efficiency and effectiveness. Despite challenges, process mining holds immense potential for future advancements, driving the digital transformation of industries. Organizations that embrace process mining as a strategic tool in the 4IR will gain a competitive edge and be better equipped to navigate the complexities of the data-driven era.

Список литературы

1. Van der Aalst, W. M. P. *Process mining: Data science in action* / W. M. P. Van der Aalst // Netherland: Springer, 2016. – 467 p.
2. Buijs, J. C. On the role of fitness, precision, generalization and simplicity in process discovery / J. C. Buijs, Van Dongen, B. F., Van der Aalst, W. M., Van der Werf, J. M. // *Data mining and knowledge discovery*. – 2012. – No. 24(3). – pp. 607-645.
3. Dementev, S. Y. *Production modernization toolkit for the transition to Industry 4.0* / S. Y. Dementev // . – 2022. – No. 21. – P. 243-245. – EDN HWTEK.
4. Fortino, G. *Intelligent process mining in the Industry 4.0 era* / G. Fortino, A. Guerrieri, W. Russo // *Journal of Ambient Intelligence and Humanized Computing*. – 2020. – No. 11(6). – pp. 2719-2733.
5. Luo, Z. *A comprehensive survey on process mining: algorithm and tool review* / Z. Luo, L. Wen, Z. He, Y. Xie // *Journal of Intelligent Manufacturing*. – 2019. – 30(6). – pp. 2577-2599.
6. Talla, M. N. *Real-time process mining: Challenges, techniques, and applications* / M. N. Talla, F. M. Nakhli, S. Rinderle-Ma // *Information Systems*. – 2021. – No. 99. – pp. 602-620.

References

1. Van der Aalst, W. M. P. *Process mining: Data science in action* / W. M. P. Van der Aalst // Netherland: Springer, 2016. – 467 p.
2. Buijs, J. C. On the role of fitness, precision, generalization and simplicity in process discovery / J. C. Buijs, Van Dongen, B. F., Van der Aalst, W. M., Van der Werf, J. M. // *Data mining and knowledge discovery*. – 2012. – No. 24(3). – pp. 607-645.
3. Dementev, S. Y. *Production modernization toolkit for the transition to Industry 4.0* / S. Y. Dementev // . – 2022. – No. 21. – pp. 243-245. – EDN HWTEK.

4. Fortino, G. Intelligent process mining in the Industry 4.0 era / G. Fortino, A. Guerrieri, W. Russo // *Journal of Ambient Intelligence and Humanized Computing*. – 2020. – No. 11(6). – pp. 2719-2733.
 5. Luo, Z. A comprehensive survey on process mining: algorithm and tool review / Z. Luo, L. Wen, Z. He, Y. Xie // *Journal of Intelligent Manufacturing*. – 2019. – 30(6). – pp. 2577-2599.
 6. Talla, M. N. Real-time process mining: Challenges, techniques, and applications / M. N. Talla, F. M. Nakhli, S. Rinderle-Ma // *Information Systems*. – 2021. – No. 99. – pp. 602-620.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ВЫЗОВЫ И РИСКИ СОВРЕМЕННОГО МИРА В ЦИФРОВОЙ СРЕДЕ

¹Балановский В.Л., ²Подъяконов В.М., ³Алборова М.Б.

¹Академия военных наук, Москва, Россия (119330 Москва, Университетский пр., 14)

²Военный университет МО РФ, Москва, Россия (125047 Москва, Большая Садовая ул., 14)

³Центр Международной информационной безопасности МГИМО МИД России, Москва, Россия (119454, г.Москва, просп. Вернадского, 76, корп. В.), e-mail: alborova2205@mail.ru

В статье рассматриваются основные возможности и риски информационного общества, обусловленные вхождением в постиндустриальный технологический уклад, цифровизацией, техно-гуманитарным дисбалансом и некоторыми другими феноменами цифровой эпохи.

Ключевые слова: Цифровая эпоха, информационное общество, постиндустриальный технологический уклад, искусственный интеллект, цифровизация, вызовы цифровой эпохи.

CHALLENGES AND RISKS OF THE MODERN WORLD IN THE DIGITAL ENVIRONMENT

¹Balanovsky V.L., ²Podyakonov V.M., ³Alborova M.B.

¹Academy of Military Sciences, Moscow, Russia (119330 Moscow, Universitates pr., 14)

²Military University of the Ministry of Defense of the Russian Federation, Moscow, Russia (125047 Moscow, Bolshaya Sadovaya st., 14)

³Center for International Information Security, MGIMO, Ministry of Foreign Affairs of Russia, Moscow, Russia (119454, Moscow, Prospekt Vernadskogo, 76, building V), e-mail: alborova2205@mail.ru

The article examines the main opportunities and risks of the information society caused by the entry into the post-industrial technological order, digitalization, techno-humanitarian imbalance and some other phenomena of the digital age.

Keywords: digital age, information society, post-industrial technological structure, artificial intelligence, digitalization, challenges of the digital age.

Цифровая цивилизация формируется стремительно и становится драйвером для развития инновационных технологий, имеющих как положительные, так и отрицательные стороны. Скорость, многоспекторность и масштабность изменений, которые влияют на жизнь современного общества имеют беспрецедентный характер и требуют высокого уровня анализа текущих явлений для понимания как их значимости, так и рисков.

Человечество все больше погружается в новый технологический мир цифровизации, нано, био и когно технологий, плотно взаимодействующих с передовыми ИКТ. В этих условиях Интернет сеть стала основной информационной инфраструктурой, связав многие процессы в единое глобальное пространство. Количество интернет-пользователей растет

ежегодно, в 2023 г., согласно отчёту Global Digital 2023, уже насчитывает 5, 16 миллиарда,¹ а это значит, что более 60 % населения земли является пользователями Интернета. Обостряется борьба за лидерство в управлении этим стратегическим ресурсом.

Технологическая сила государств на современном этапе во многом определяется наличием у него своей собственной комплексной инфраструктуры, базой данных (хранение информации), суперкомпьютеров (обработка данных), а также корневых серверов и доступа к широкополосному Интернету (передача информации). Не маловажную роль имеет и полноценная система подготовки и переподготовки кадров, способных не только успешно работать с уже созданными технологиями, но и быстро и творчески реагировать на вызовы и риски, возникающие в условиях современных противоречий и угроз информационного пространства. Динамически развивающаяся научно-технологическая составляющая является значимым фактором конкурентоспособности на международной арене и необходимым элементом обеспечения государственного суверенитета.

Мы живем в эпоху экспоненциального роста количества технологий. Наиболее успешно развиваются многочисленные приложения искусственного интеллекта для анализа больших объемов данных, создаются новые возможности для сети связи 5G, активно распространяется технология блокчейна. Технологии искусственного интеллекта открывают новые направления в области машинного обучения, эволюции вычислений планировании и так далее. Уже сегодня использование приложений ИИ выросло многократно и применяется в авиации, космосе, медицине, банковской сфере, безопасности критической инфраструктуры и др. В последние годы технологии ИИ применяются в сфере правопорядка и национальной обороны.

Развитие данной технологии позволяет сформировать качественно новые условия для экономической и социальной сферы в жизни общества. Совершенно очевидно, что государства, лидирующие в этом направлении, получают конкурентное преимущество.

В 2017 г. Президент России В.В. Путин подчеркивая значение технологии искусственного интеллекта сказал, что страна, добившаяся лидерства в данной сфере «будет властелином мира»², осознание роли и инновационного потенциала искусственного интеллекта требует и от Российской Федерации формирования комплекса мер как по разработке данной технологии, так и по подготовке кадров в этом направлении. Важно отметить, что у России есть качественная научная и практическая база для реализации технологии ИИ.

Инновации приводят к изменению жизни общества, трансформируя его, создавая с одной стороны уникальные возможности, с другой стороны формируя риски и потенциальные угрозы. Важно вовремя анализировать деструктивный потенциал, который заложен в инновационных технологиях и может негативно отразиться на всех сферах общественной жизни. Уже сегодня мы видим глобальные изменения в экономике, на рынке труда, все больше меняются социальные запросы, трансформируются моральные ценности. Развивающиеся социальные сети создают информационную среду, в которой с помощью инновационных технологий возможно манипулировать общественным сознанием применяя дипфейки и

¹ Цифровой 2023: глобальный обзорный отчет. <https://datareportal.com/reports/digital-2023-global-overview-report> (дата обращения: 08.05.2023)

² Открытый урок «Россия, устремленная в будущее» // 01.09.2017 URL: <http://kremlin.ru/events/president/news/55493> (дата обращения: 08.05.2023)

расставляя акценты с определенным контекстом³. В совокупности с этой проблемой необходимо рассматривать и вопрос информационного воздействия на подрастающее поколение. Современные технологии социального инжиниринга широко используются для управления обществом.

Рассматривая широкие возможности ИИ нельзя не заострить внимание на вопросах угроз безопасности, связанных с применением подобных технологий, причем риски могут быть как технического характера (использование результатов анализа больших баз данных в преступных целях), так и социального (применение ИИ технологий очевидно меняет рынок труда, сокращаются многие профессии, растет безработица).

Нельзя не отметить и риски для национальной безопасности, которые проявляются на фоне обострения технологической конкуренции и цифрового разрыва, что в свою очередь ведет ущемлению интересов стран, не имеющих подобных технологий. Кроме того, деструктивный потенциал искусственного интеллекта может быть использован для вмешательства во внутреннюю политику стран, влияния на протестные настроения, рост агрессии и паники.

Важно отметить, что отставание в технологическом прогрессе ведет к рискам сохранения суверенности государств, их уязвимости в новом мире цифры, подобная ситуация становится новым цивилизационным вызовом, с которым столкнулось человечество в XXI веке.

В 2020 г. выступая на заседании Генассамблеи ООН, Генеральный секретарь ООН Антониу Гутерриш отметил, что новые технологии используются для преступлений, разжигания ненависти, распространения ложной информации и эксплуатации людей.⁴

Разработка и повсеместное внедрение цифровых информационных технологий проявили все три основных направления угроз: гражданское, военное и преступное. Новым фактором современных угроз для всего мирового сообщества стало использование многомерного потенциала сети Интернет и других цифровых ИКТ международными криминальными структурами. В условиях современного геополитического кризиса количество киберпреступлений увеличилось значительно, а ущерб от них для мировой экономики, по оценкам ООН в 2023 году вырастет до 10, 5 трлн долл.

Уязвимость государств становится все очевиднее. Столь масштабное, бесконтрольное применение информационно-коммуникационных технологий может быть использовано для подрыва государственной стабильности и суверенитета⁵. Риски глобального информационного пространства не имеют границ. Осознание и понимание угроз нового технологического мира должно стать основой для значительной работы международного сообщества в сфере обеспечения безопасности в условиях новой реальности.

В Концепции внешней политики Российской Федерации отмечается необходимость: «Формирования и совершенствования международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях»⁶.

³ Булва В.И. Феномен социальных сетей в контексте информационной безопасности / В. И. Булва // Международная жизнь. – 2023. – № 3. – С. 53.

⁴ Генсек ООН назвал четыре угрожающих миру «всадника Апокалипсиса» <https://ria.ru/> (дата обращения: 8.05.2023).

⁵ Международная информационная безопасность: подходы России : Аналитический доклад / А. В. Крутских, Е. С. Зиновьева, В. И. Булва [и др.]. – Москва : Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, 2022. – 48 с.

⁶ <https://www.mid.ru/ru/detail-material-page/1860586/>

Важно отметить, что Россия с конца XX века принимает все необходимые меры для обеспечения национальной и международной информационной безопасности, поднимая вопрос о противодействии угрозам нового глобального цифрового мира как на международном уровне, так и на региональном и национальном. 4 декабря 1998 года по инициативе России впервые был принят Генеральной Ассамблеей ООН проект резолюции (№ 53/70) под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»⁷. С этого момента начинается официальный процесс создания международно-правового режима, регулирующего вопросы обеспечения безопасности в новом мире технологий.

Многоаспектность технологических рисков наиболее четко проявилась и в условиях кризиса 2022 года. Очевидное расширение милитаризации глобального информационного пространства становится все более активным. Увеличилось и количество кибератак на критическую информационную инфраструктуру. Сегодня многие страны стали наращивать свои военные возможности в сфере информационно-коммуникационных технологий. Страны блока НАТО открыто заявляют о возможности нанесения превентивных киберударов по недружественным им государствам. Усиливающиеся международные противоречия создают условия для использования инновационного технологического потенциала для доминирования над развивающимися странами. Глобальное цифровое пространство все больше становится местом для межгосударственной конкуренции и конфликтов.

Российская позиция направлена на приоритет мирного развития информационного пространства, уважение государственного суверенитета, недопущение использования силы или угрозы силой в цифровой среде. На современном этапе необходимо формировать глобальную систему международной информационной безопасности, в рамках которой надо заключить на международном уровне универсальные и юридически обязывающие договоренности в информационной сфере.

Список литературы

1. Бiryukov A. V., Alborova M. B. Социально-гуманитарное измерение международной информационной безопасности. М.: Аспект Пресс, 2019.
2. Крутских А., Бiryukov A. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. № 2. С. 6-26.
3. Ларина Е.С. Человеческое мышление и искусственный интеллект: российский аргумент в международном сотрудничестве // В кн. Международная информационная безопасность: новая геополитическая реальность. М.: Аспект Пресс, 2021. С. 79–85
4. Международная информационная безопасность: теория и практика: В 3 т. / Под общ. ред. А. В. Крутских. М.: Аспект Пресс, 2021.

References

1. Biryukov A.V., Alborova M. B. Social and humanitarian dimension of international information security. M.: Aspect Press, 2019.

⁷ Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. 04.01.1999. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement>

2. Krutskikh A., Biryukov A. New geopolitics of international scientific and technological relations // *International processes*. 2017. No. 2. pp. 6-26.
 3. Larina E.S. Human thinking and artificial intelligence: the Russian argument in international cooperation // In the book. *International Information Security: A New Geopolitical Reality*. Moscow: Aspect Press, 2021. pp. 79-85
 4. *International information security: theory and practice: In 3 volumes / Under the general editorship of A.V. Krutskikh*. M.: Aspect Press, 2021.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ОПРЕДЕЛЕНИЕ ПРАКТИЧЕСКОЙ ЗНАЧИМОСТИ И ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ОПТИМАЛЬНОГО СПОСОБА ВЗАИМОДЕЙСТВИЯ С КЛИЕНТОМ ДЛЯ УВЕЛИЧЕНИЯ ДОХОДНОСТИ МАРКЕТИНГОВЫХ КАМПАНИЙ И СНИЖЕНИЯ ИЗДЕРЖЕК НА НИХ

Обливальный Н.Д.

ФГБОУ ВО "Челябинский Государственный Университет", Челябинск, Россия (454001, г. Челябинск, ул. Братьев Кашириных, 129), e-mail: rfrepe@gmail.com

В данном исследовании предметом изучения была задача поиска оптимального способа взаимодействия с клиентами с целью повышения доходности маркетинговых кампаний и снижения издержек. Для достижения этой цели были выполнены следующие задачи: определен универсальный подход к моделированию эффекта коммуникации; обеспечивающий максимальную точность модели; определен универсальный метод Uplift моделирования; проведены A/B тесты подтверждающие практическую ценность методов и рассчитана экономическая эффективность на реальном кейсе. Решение задач было применено в качестве прикладной области телеком провайдера. Практический результат работы представляет собой сервис, который позволяет определить необходимость и оптимальный способ коммуникации с клиентами телеком провайдера, имеющими задолженность.

Ключевые слова: Uplift моделирование, машинное обучение, большие данные, коммуникация с клиентами, доходность маркетинговых кампаний, телеком провайдер, расчет экономической эффективности.

DETERMINING THE PRACTICAL SIGNIFICANCE AND ECONOMIC EFFICIENCY OF THE OPTIMAL WAY OF INTERACTING WITH THE CLIENT TO INCREASE THE PROFITABILITY OF MARKETING CAMPAIGNS AND REDUCE THEIR COSTS

Oblivalny N.D.

Chelyabinsk State University, Chelyabinsk, Russia (454001, Chelyabinsk, Brothers Kashirin str., 129), e-mail: rfrepe@gmail.com

In this study, the subject of the study was the task of finding the optimal way to interact with customers in order to increase the profitability of marketing campaigns and reduce costs. To achieve this goal, the following tasks were performed: a universal approach to modeling the communication effect was determined; providing maximum accuracy of the model; a universal method of Uplift modeling was determined; A/B tests were conducted confirming the practical value of the methods and economic efficiency was calculated on a real case. Problem solving was applied as an application area of a telecom provider. The practical result of the work is a service that allows you to determine the need and the optimal way to communicate with customers of a telecom provider who have debts.

Keywords: Uplift modeling, machine learning, big data, communication with customers, profitability of marketing campaigns, telecom provider, calculation of economic efficiency.

Современные технологии играют важную роль в бизнесе, особенно в сегменте B2C. Взаимодействие с клиентом является ключевым элементом любого бизнеса, нацеленного на увеличение доходов. Правильное взаимодействие мотивирует клиентов на действия, такие как: оформление подписки, покупка товара и т.д. Выбор наиболее эффективного канала связи с клиентом актуален и при планировании бюджета, необходимо грамотно распределить средства и добиться выполнения стратегических целей. Однако информационный шум, вызванный неконтролируемым количеством уведомлений, может снизить внимание клиентов и уменьшить эффективность каналов коммуникации. В связи с этим, данная магистерская диссертация предлагает решение по определению наилучшего способа взаимодействия с клиентами для достижения желаемой эффективности маркетинговых компаний.

Методы

Uplift моделирование - это метод машинного обучения, который используется для определения воздействия на клиентов в маркетинговых кампаниях [2]. В отличие от классических моделей, которые прогнозируют вероятность реакции клиентов на воздействие, uplift моделирование определяет, насколько сильно клиент изменит свое поведение в ответ на воздействие, и измеряет этот эффект в абсолютных числах.

Основным понятием в uplift моделировании является uplift (подъем) - это разница между вероятностью реакции клиента на воздействие и вероятностью реакции на отсутствие воздействия. То есть uplift показывает реальный эффект воздействия на клиента, учитывая его индивидуальные характеристики.

Однако uplift моделирование имеет свои ограничения [6]. Оно может не учитывать другие факторы, которые могут влиять на поведение клиентов, например, экономическую ситуацию или изменения в рынке. Кроме того, этот метод требует большого объема данных и тщательного подбора моделей для достижения точных результатов. Поэтому важно определить их степень влияния на конечный результат, так как при выборе универсального подхода они могут оказать решающее значение.

В рамках данной работы будут рассматриваться три основных метода: метод с использованием двух независимых моделей, метод преобразования класса и метод постоянный на использовании деревьев.

Метод, основанный на использовании двух моделей, является одним из подходов в uplift моделировании. Данный подход позволяет определить причинно-следственные связи между воздействием и поведением клиента. Данный подход состоит из двух моделей: модели прогнозирования вероятности реакции клиента на воздействие и модели прогнозирования вероятности реакции клиента на отсутствие воздействия. Затем uplift рассчитывается как разница между этими двумя вероятностями.

Метод преобразования класса (Class Transformation) в Uplift моделировании представляет собой подход, где целевая переменная изменяется перед обучением модели [5].

Вместо прямого прогнозирования uplift, метод преобразования класса предлагает прогнозировать измененную целевую переменную, которая является функцией от оригинальной целевой переменной и флага коммуникации (бинарный флаг, указывающий, была ли проведена коммуникация с клиентом).

Новый класс равен 1, если мы знаем, что на конкретном наблюдении результат при взаимодействии был бы таким же или лучше, как и в контрольной группе, если бы мы могли знать результат в обеих группах. Иначе новый класс будет равен 0.

Этот подход позволяет учесть влияние коммуникации на целевую переменную и сделать прогнозы на основе измененной целевой переменной.

Методы, основанные на деревьях в Uplift моделировании, являются эффективным и широко используемым подходом [3]. Они позволяют оценить влияние факторов на изменение целевой переменной в зависимости от воздействия на клиента.

Один из таких методов основан на использовании деревьев решений с измененным критерием разбиения. Вместо стандартных критериев, таких как энтропия или критерий Джини, используется дивергенция между распределениями целевой переменной у контрольной и целевой групп. Таким образом, дерево строится таким образом, чтобы максимизировать расстояние между этими распределениями.

Одним из преимуществ метода на основе деревьев с измененным критерием разбиения является возможность эффективной обработки категориальных признаков.

Одним из недостатков этого метода является то, что он может быть чувствителен к выбросам и неустойчив к изменению данных. Кроме того, он может потребовать большого количества данных для получения точных результатов.

В рамках предыдущей статьи «Определение оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых компаний и снижения издержек на них» были рассмотрены перечисленные методы и определен универсальный [1].

После проведения всех экспериментов можно выделить два метода. Результаты сравнения всех моделей представлены в таблице 1 [4, 8].

Лучшие результаты показал метод преобразования класса. Вторым по точности оказался метод с использованием двух независимых моделей. Оба подхода использовали в качестве классификатора XGBoost [7].

Для получения достоверных данных о качестве данных подходов для каждого из них было проведено А/В тестирование на реальных должниках телеком провайдера.

А/В тестирование лучших методов

Эксперименты с использованием А/В тестирования были поставлены на должниках телеком провайдера. Для этого были отобраны имеющие задолженность абоненты на начало месяца. Для каждого должника была собрана информация для получения прогноза, и определено значение uplift от взаимодействия с ним. В данном случае взаимодействием был звонок с напоминанием о задолженности.

Тестирование было проведено на двух лучших методах. Первым тестировался подход с использованием двух независимых моделей. Для этого были отобраны должники на начало месяца и разделены на 4 группы: «Убеждаемые», «Не беспокоить», «Лояльные» и «Потерянные». Каждая группа определяется по значению Uplift. На рисунке 1 представлено распределение должников по группе.

Лучшие результаты показал метод преобразования класса. Вторым по точности оказался метод с использованием двух независимых моделей. Оба подхода использовали в качестве классификатора XGBoost [7].

Для получения достоверных данных о качестве данных подходов для каждого из них было проведено А/В тестирование на реальных должниках телеком провайдера.

Таблица 1 – Сравнение всех методов uplift моделирования

Методы	f1 (целевой группы)	uplift@20%	AUQC
Две независимые модели	0.553	0.6594	0.3484
Две зависимые модели (зависимое представление данных)	0.53	0.0597	0.0903
Две зависимые модели (перекрестная зависимость)	0.051	0.0368	0.0846
Class transformer (XGBoost)	0.58	0.855	0.3618
Class transformer (CatBoost)	0.56	0.851	0.3472
Class transformer (LogReg)	0.51	0.832	0.3295
Decision Tree Classifier (Kullback-Leibler)	0.1	0.048	0.081
Decision Tree Classifier (Euclidean Distance)	0.23	0.136	0.102
Decision Tree Classifier (DDP)	0	0.02	0.078
Decision Tree Classifier (CTS)	0.28	0.15	0.067
Random Forest Classifier (Kullback-Leibler)	0.19	0.03	0.118
Random Forest Classifier (Euclidean Distance)	0.09	0.075	0.119
Random Forest Classifier (DDP)	0.11	0.08	0.115
Random Forest Classifier (CTS)	0.05	0.04	0.073

Источник: анализ автора

А/В тестирование лучших методов

Эксперименты с использованием А/В тестирования были поставлены на должниках телеком провайдера. Для этого были отобраны имеющие задолженность абоненты на начало месяца. Для каждого должника была собрана информация для получения прогноза, и определено значение uplift от взаимодействия с ним. В данном случае взаимодействием был звонок с напоминанием о задолженности.

Тестирование было проведено на двух лучших методах. Первым тестировался подход с использованием двух независимых моделей. Для этого были отобраны должники на начало

месяца и разделены на 4 группы: «Убеждаемые», «Не беспокоить», «Лояльные» и «Потерянные». Каждая группа определяется по значению Uplift. На рисунке №1 представлено распределение должников по группе.

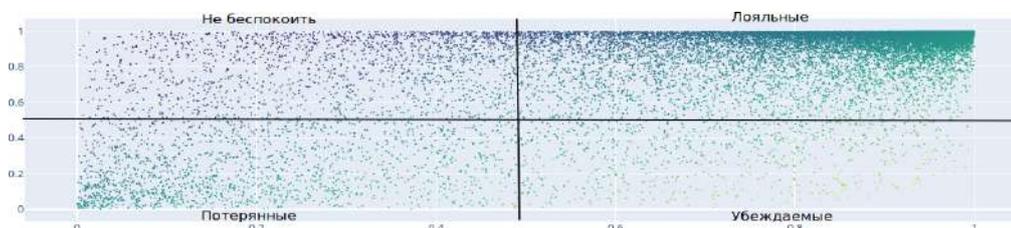


Рисунок 1 – Распределение должников по группам uplift

Источник: анализ автора

Должники распределяются по группам по следующим условиям:

- Убеждаемые = uplift целевой >0.5 и uplift контрольной <= 0.5
- Лояльные = uplift целевой > 0.5 и uplift контрольной > 0.5
- Потерянные = uplift целевой < 0.5 и uplift контрольной < 0.5
- Не беспокоить = uplift целевой <= 0.5 и uplift контрольной > 0.5

Процент распределения должников по группам представлен в таблице №2

Таблица 2. Процент распределения должников по группам uplift в апреле

Группы	Процент от всех должников
Не беспокоить	10,66%
Потерянный	5,41%
Лояльный	74,12%
Убеждаемый	9,81%

Источник: анализ автора

По итогам первого А/В тестирования метода использования двух независимых моделей эффект от использования подтвердился. Результаты эксперимента представлены в таблице 3.

Как видно из таблицы 3 группа «Убеждаемые» имеет значимо больший процент при звонке, а группа «Не беспокоить» наоборот при звонке имеет меньшую конверсию в оплату. Остальные две группы не имеют статистической значимости.

Данные результаты подтверждают корректность работы модели и показывают на реальных данных прирост конверсии в оплату задолженности у должников.

В следующий календарный месяц было произведено тестирование второго метода с преобразованием класса. Распределение между группами Uplift имело похожее распределение. В таблице 4 процент распределения должников по группам uplift.

Таблица 3 – Результаты А/В теста подхода с использованием двух независимых полей

Группы	Конверсия в оплату		Доверительный интервал		Значимость
	А (звонок)	В (без звонка)	1	2	
Убеждаемые	30,65%	17,81%	-21,97%	-3,72%	Значимое
Потерянные	14,02%	10,57%	-8,08%	1,18%	Незначимое
Лояльные	64,73%	63,35%	-3,76%	1%	Незначимое
Не беспокоить	20,45%	25,48%	0,4%	10,03%	Значимое

Источник: анализ автора

Таблица 4 – Процент распределения должников по группам uplift в мае

Группы	Процент от всех должников
Не беспокоить	8,92%
Потерянный	7,65%
Лояльный	72,04%
Убеждаемый	11,39%

Источник: анализ автора

Результаты А/В тестирования метода с преобразованием класса представлены в таблице 5.

Таблица 5 – Результаты А/В теста подхода с использованием метода преобразования класса

Группы	Конверсия в оплату		Доверительный интервал		Значимость
	А (звонок)	В (без звонка)	1	2	
Убеждаемые	26,13%	9,52%	-24,23%	-9%	Значимое
Потерянные	9,41%	8,19%	-5,03%	2,59%	Незначимое
Лояльные	67,82%	68,66%	-1,43%	3,12%	Незначимое
Не беспокоить	16,85%	22,93%	0,77%	11,38%	Значимое

Источник: анализ автора

По итогам второго тестирования также подтвердилась теория взаимодействия с группами Uplift. Второй подход показал на реальных данных чуть больший прирост по

конверсии в оплату. Сравнение прироста конверсии по итогам двух тестов представлен в таблице 6.

Таблица 6 – Сравнение прироста конверсии по итогам А/В тестирования

Группы	Две независимые модели	Class transformer
Убеждаемые	12,84%	16,61%
Потерянные	3,45%	1,22%
Лояльные	1,38%	0,84%
Не беспокоить	5,03%	6,08%

Источник: анализ автора

По итогам А/В теста можно сделать вывод о том, что получившиеся модели действительно имеют практический эффект. Они определяют группу людей, с которыми коммуникация будет наиболее эффективна, и группу людей, с которыми нет практической ценности взаимодействовать.

Экономическая эффективность модели.

Для того, чтобы оценить экономическую эффективность, нужно определить, как именно модель будет влиять на текущую ситуацию. Ранее был описан основной эффект от использования Uplift моделирования на должниках.

Ключевым эффектом является сокращение выборки должников, с которыми нужно взаимодействовать для достижения оплаты задолженности. Получается за счет прогноза модели мы можем отобрать процент должников, с которыми нужно взаимодействовать.

По результатам проведенных тестов известно, что в среднем в каждом месяце всего 10% должников, с которыми нужно взаимодействовать. В данной ситуации мы можем сэкономить ресурс операторов и сократить количество звонков на 90%.

Вторым эффектом от использования Uplift является увеличение конверсии в целевое действие. В рассматриваемой прикладной задаче этот эффект наблюдается, но имеет совсем небольшие значения. С помощью модели можно увеличить конверсию в оплату у групп «Не беспокоить» на 5% и «Убеждаемые» на 13%. В абсолютных значениях (от общей конверсии) прирост составляет $5\%*10\%$ (доля группы «Не беспокоить») + $13\%*10\%$ (доля группы «Убеждаемые») = 1.8%.

Итоговый эффект от применения Uplift моделирования будет складываться из экономии на неэффективных звонках и увеличении возврата задолженности.

Обзвоном должников занимается отдельная группа операторов. Она состоит из 9 операторов. В месяц данная группа успевает обзвонить от 84%-92% должников. Если группа успевает поговорить с 85% должников, то часть операторов перенаправляется на другие типы обзвонив. Чаще всего на холодные обзвоны.

Для расчета стоимости обзвона должников необходимо определить стоимость одного оператора в месяц. Зарплата оператора составляет 32 000 рублей. С учетом налогов и накладных расходов один оператор обходится компании в $32000*30\%+32000*60\%+32000 = 60$

800 рублей. В данной группе работает 9 человек и в месяц на них затрачивается 547 200 рублей.

Итоговая стоимость обзвона с применением и без применения Uplift моделирования показана в таблице 7.

Таблица 7 – Стоимость обзвона должников

Подход	Стоимость обзвона всех должников	Процент обзвона должников	Стоимость обслуживания процесса	Стоимость обзвона
Без применения Uplift	р.547 200	85%	р.0,00	р.465 120
С применением Uplift	р.547 200	10%	р.8 938	р.63 658

Источник: анализ автора

Для расчета увеличения процента оплаты от применения Uplift модели потребуется определить количество должников, вернувшихся за счет модели. Взяв процент прироста конверсии и умножив его на количество должников и на среднюю стоимость тарифа компании, мы получим экономический эффект от увеличения конверсии, 60 750 рублей.

Итоговый экономический эффект будет рассчитываться как разница между подходами и добавлением суммы увеличению конверсии в оплату, которая равна $465120 - 63658 + 60750 = 462212$ рублей.

Как видно из расчетов при учете сокращения штата данные инвестиции на проект окупаются в первый же месяц. Но в реальности компания не стала прибегать к данному способу. Штат операторов не был сокращен, но был изменен бизнес-процесс.

В начале каждого месяца все 9 человек работают с должниками и после завершения необходимого количества номеров группа операторов переключалась на холодные звонки и на выявление адресов. В таком случае экономический эффект от применения Uplift модели не совсем корректно брать за снижение издержек.

Получается, что фактический прирост в погашении задолженности у должников составил всего 1,8% или 60 750 рублей.

Перейдем к расчету инвестиционных показателей: NPV, IRR, ROI, PI и DPP.

NPV (Net Present Value) или чистая приведенная стоимость – это текущая стоимость будущих денежных потоков инвестиционного проекта, рассчитанная с учетом дисконтирования, за вычетом инвестиций (1).

$$NPV = \sum_{t=0}^n \frac{CF_t}{(1 + R)^m}, (1)$$

где:

n, t — количество временных периодов,

m — количество периодов,

CF — денежный поток (Cash Flow),

R — стоимость капитала (ставка дисконтирования, Rate. Она складывается из ключевой ставки ЦБ РФ, уровня инфляции и рискованности проекта: $7,25\% + 8,13\% + 7\% = 22,38\%$ по данным за 25 мая 2023 года).

NPV = 319 237 рубль. Таким образом, NPV проекта больше нуля. Это говорит о выгодности проекта.

Следующим исследуемым инвестиционным показателем будет IRR. IRR - это внутренняя норма доходности показывает процент, при котором приведенная стоимость всех денежных потоков инвестиционного проекта равна нулю, рассчитывается по формуле (2).

$$0 = \sum_{t=0}^n \frac{CF_t}{(1 + IRR)^t}$$

где:

CF t — денежные потоки от проекта в момент времени t;

n — количество периодов времени;

IRR — внутренняя норма доходности.

IRR = 19%. Таким образом, IRR больше ежемесячной ставки дисконтирования, что еще раз подтверждает выгодность реализации проекта.

Следующим на очереди будет показатель PI. PI - это отношение суммы прибыли к абсолютной величине инвестиций. Он показывает количество прибыли, которое удастся получить за каждую вложенную единицу средств. Формула для расчетов PI выглядит следующим образом (3):

$$PI = \frac{\sum_{n=1}^N \frac{NCF_n}{(1+R)^n}}{\sum_{n=1}^N \frac{I_n}{(1+R)^n}} = \frac{NPV}{I_0}, (3)$$

где:

CF n - чистый дисконтированный денежный поток в n периоде;

I n - начальные инвестиции в n периоде (или суммарные инвестиции);

R – ставка дисконтирования;

NPV (Net present value) – чистый дисконтированный (приведенный) доход.

$$PI = \frac{319\,237,40 \text{ руб.}}{239\,020 \text{ руб.}} = 1,34$$

Так как PI больше единицы, то проект выгоден.

Следующим рассматриваемым показателем является ROI. ROI — коэффициент окупаемости. Этот показатель демонстрирует прибыльность или убыточность той или иной инвестиции, измеряется в процентах. Чтобы его рассчитать, потребуется знать две вещи: доход от вложений и их размер. Формула для расчетов выглядит следующим образом (4):

$$ROI = \frac{\text{Доход от вложений} - \text{Расходы вложений}}{\text{Размер вложений}} \times 100\% (4)$$
$$ROI = \frac{729\,000 - 346\,276}{239\,020} \times 100 = 116,12\%$$

Так как ROI больше 100 процентов, то проект выгоден.

В конце будет рассмотрен дисконтированный период окупаемости DPP. Главное отличие от простой формулы срока окупаемости – это дисконтирование денежных потоков и приведение будущих денежных поступлений к текущему времени. Формула для расчета DPP выглядит следующим образом (5):

$$DPP = \min n, \text{ при котором } \sum_{t=1}^n \frac{CF_t}{(1+R)^t} > IC, (5)$$

где:

DPP (Discounted Payback Period) – дисконтированный срок окупаемости инвестиций;

CF_t — денежные потоки от проекта в момент времени t ;

n — количество периодов времени;

R - ставка дисконтирования;

IC (Invest Capital) – первоначальные инвестиционные затраты в проекте.

Вложения окупятся уже в первый месяц. Выясним точный период окупаемости:

$$DPP = 5 \text{ мес.} + \left(1 - \frac{246\,374 - 239\,020}{47\,630} \times 30\right) \approx 25 \text{ дней}$$

Период окупаемости составляет 5 месяцев и 25 дней. Такой продолжительный срок объясняется тем, что мы не учитываем экономию за счет сокращения штата и извлечение выгоды для компании за счет перенаправления ресурсов на другие процессы.

После подсчета всех экономических показателей можно сделать вывод о выгодности реализации проекта. Все ключевые показатели указывают на положительный результат при внедрении модели в текущий бизнес-процесс.

Заключение

В рамках исследования подходов к Uplift моделированию были определены универсальные подходы. Универсальным подходом стал метод преобразования класса. Но не менее высокие результаты показал метод с использованием двух независимых моделей. Оба метода являются универсальными, так как при условии дисбаланса между контрольной и целевой группой метод с использованием двух независимых моделей будет показывать результаты лучше, чем метод преобразования класса.

Оба алгоритма были проверены в реальных условиях при помощи А/В тестирования. По результатам тестирования была подтверждена ценность Uplift моделирования в работе с должниками телеком провайдера.

На основе проведенных тестов оценен экономический эффект от применения модели. Все инвестиции, вложенные в формирование универсального подхода к uplift моделированию окупаются за 6 месяцев.

Результаты данной работы были приняты для дальнейшего использования в провайдере для работы с должниками и другими задачами, связанными с взаимодействиями с клиентами.

Список литературы

1. Обливальный Н.Д., Определение оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них. Международный журнал информационных технологий и энергоэффективности, [s.l.], v.

Обливальный Н.Д. Определение практической значимости и экономической эффективности оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 80–90

- 8, n. 4(30), p. 084-091, апр. 2023. Issn 2500-1752. Режим доступа: <http://www.openaccessscience.ru/index.php/ijcse/article/view/327>., свободный
2. Artem Betlei, Eustache Diemert, Massih-Reza Amini. Uplift Modeling with Generalization Guarantees, 2021.
 3. Henrik Karlsson, Linda Wanstrom. Uplift Modeling: Identifying Optimal Treatment Group Allocation and Whom to Contact to Maximize Return on Investment, 2019.
 4. LogisticRegression documentation. - Режим доступа: <https://scikit-learn.org/stable/index.html>, свободный.
 5. Robin M. Gubela, Stefan Lessmann. Interpretable Multiple Treatment Revenue Uplift Modeling, 2021.
 6. Ta-Wei Huang, Eva Ascarza. When Less is More: Using Short-term Signals to Overcome Systematic Bias in Long-run Targeting, 2022.
 7. Xgboost documentation. - Режим доступа: <https://xgboost.readthedocs.io/en/stable/>, свободный.
 8. Catboost documentation. - Режим доступа : <https://catboost.ai/en/docs/>, свободный.

References

1. Oblivny N.D., Determining the optimal way to interact with the client to increase the profitability of marketing campaigns and reduce their costs. International Journal of Information Technology and Energy Efficiency, [s.l.], v. 8, n. 4(30), p. 084-091, Apr. 2023. Issn 2500-1752. Access mode: <http://www.openaccessscience.ru/index.php/ijcse/article/view/327>., free
 2. Artem Betlei, Eustache Diemert, Massih-Reza Amini. Uplift Modeling with Generalization Guarantees, 2021.
 3. Henrik Karlsson, Linda Wanström. Uplift Modeling: Identifying Optimal Treatment Group Allocation and Whom to Contact to Maximize Return on Investment, 2019.
 4. LogisticRegression documentation. - Access mode: <https://scikit-learn.org/stable/index.html>, free.
 5. Robin M. Gubela, Stefan Lessmann. Interpretable Multiple Treatment Revenue Uplift Modeling, 2021.
 6. Ta-Wei Huang, Eva Ascarza. When Less is More: Using Short-term Signals to Overcome Systematic Bias in Long-run Targeting, 2022.
 7. Xgboost documentation. - Access mode: <https://xgboost.readthedocs.io/en/stable/>, free.
 8. Catboost documentation. - Access mode: <https://catboost.ai/en/docs/>, free.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ ОГРАНИЧЕНИЙ СИСТЕМ В ОТДЕЛЕ ПРОЕКТНОЙ РАЗРАБОТКИ ИТ КОМПАНИИ

Осипович П.А.

Иркутский национальный исследовательский технический университет, Иркутск, Россия (664074, г.Иркутск, ул. Лермонтова, 83), e-mail: osipovich.polina@mail.ru

Данная статья исследует применение Теории Ограничений Систем в области информационных технологий, а конкретно в проектной разработке. В статье рассматриваются применение ТОС и ее инструментов в контексте ИТ-проектов. Основной фокус исследования — это идентификация и управление ограничениями в разработке программного обеспечения, управлении проектами и других процессах ИТ, а также важность отслеживания денежных потоков и расчета потока.

Ключевые слова: теория ограничений систем, ограничение системы, внедрение тос, алгоритм внедрения, денежные потоки, проток.

THE APPLICATION OF THE METHODS OF THE THEORY OF SYSTEMS CONSTRAINTS IN THE DESIGN DEPARTMENT OF AN IT COMPANY

Osipovich P.A.

Irkutsk National Research Technical University, Irkutsk, Russia (664074, Chelyabinsk, Brothers Kashirin str., 129), e-mail: rfrepe@gmail.com

This paper explores the application of Systems Constraints Theory in the field of information technology, specifically in project development. The paper examines the application of CBT and its tools in the context of IT projects. The main focus of the study is the identification and management of constraints in software development, project management and other IT processes, and the importance of cash flow tracking and flow calculation.

Keywords: theory of constraints, system constraints, TOS implementation, implementation algorithm, cash flows, throughput.

Для достижения высокой рентабельности компании необходимо управлять ее деятельностью на многих уровнях, включая управленческое звено. Оно выполняет множество функций, таких как прогнозирование, планирование, организация, координация, мотивация и контроль, используя специальные методы и технологии, которые помогают достигать поставленных целей.

Одной из теорий, которая может помочь в этом, является теория ограничения систем (ТОС), созданная Элияху Голдраттом. Эта теория утверждает, что эффективность любой деятельности зависит от умения находить и управлять ограничениями системы, которые являются ее слабыми сторонами и могут замедлить ее развитие. [1]

Данная теория изначально получила свое развитие в области промышленного производства, но с течением времени ее принципы были адаптированы и используются по сей день в различных типах бизнесов, в том числе и в работе ИТ компаний.

Целью данного исследования является описание применения основных принципов ТОС в работе отдела проектной разработки ИТ компании. Для достижения данной цели необходимо изучить теорию на основе книги «Цель. Процесс непрерывного совершенствования» Голдратта, сформулировать основные моменты данной теории и описать их практическое применение в работе отдела проектной разработки.

Применить методологию, которая изначально создавалась для оптимизации промышленного производства, в процессе разработки ИТ проектов позволяют некоторые ее особенности. Во-первых, как и говорилось ранее ограничения могут быть найдены в любой системе, независимо от ее области. Во-вторых, ТОС ставит упор на постоянное улучшение системы. Это применимо к любой организации или системе, независимо от их размера или отрасли. Постоянное улучшение является ключевым фактором успешного функционирования в современном бизнесе. Так же теория, предложенная Голдраттом, не предписывает жестких правил или шаблонов, а скорее предоставляет фреймворк для анализа и улучшения системы. Это позволяет применять ТОС в различных областях и контекстах.

Популярность концепции обусловлена не только ее универсальностью. Самое значимое в Теории Ограничений систем заключается в том, что она позволяет эффективно использовать имеющиеся ресурсы для достижения более высокой прибыли. Она способствует интенсивному развитию, а не бесконтрольному увеличению объемов и расходов. Методы и принципы ТОС позволяют охватить всю ситуацию и выявить проблемные аспекты, позволяя таким образом принимать более обоснованные решения. Теория Ограничений устанавливает реальную связь между экономическими и финансовыми аспектами бизнеса и управлением операциями. Она позволяет руководству сосредоточиться на ключевых факторах, определяющих прибыльность. Так же водятся элементы научного мышления в управление, предлагая простой, но строгий подход. И как итог, усиливает и систематизирует предпринимательский творческий потенциал и интуицию, что приводит к расширению возможностей всей организации.

В концепции ТОС, ограничения, как отрицательные факторы, стимулируют к преодолению разрыва между текущим и желаемым состоянием звена и являются ключом к эффективному управлению. Методология ориентирована на практику и помогает ответить на вопросы, связанные с изменением компании, а также обеспечивает процесс непрерывных улучшений. Этот процесс обеспечивается выполнением пяти основных шагов.

Первый шаг в применении ТОС — это идентификация основных ограничений, которые ограничивают производительность системы. Ограничения могут быть физическими (например, ограниченная пропускная способность машины) или логическими (например, узкие места в процессах или неэффективные политики и правила).

Второй шаг состоит в максимизации использования ограниченного ресурса или устранении факторов, которые усиливают ограничение. Это может включать улучшение расписания, оптимизацию процессов, перераспределение ресурсов или улучшение квалификации персонала, чтобы максимально использовать ограниченный ресурс.

Третий шаг заключается в том, чтобы настроить и согласовать все остальные аспекты системы с ограничением, чтобы обеспечить максимальную эффективность. Это означает, что все процессы, решения и ресурсы должны быть подчинены цели устранения ограничения и улучшения системы в целом.

Применение этих шагов помогает обеспечить контроль над системой, повысить ее предсказуемость и надежность. Они также позволяют устранить потери и проблемы, связанные с работой системы, уже на начальном этапе внедрения ТОС. Важно, чтобы система находилась в стабильном состоянии, что дает возможность сосредоточиться на научных разработках для дальнейшего роста и максимизации прибыли. Для достижения этих целей необходимо применить следующие шаги, описанные далее.

Четвертый шаг состоит в создании системы контроля, которая позволяет отслеживать и измерять производительность системы после внесения изменений. Это помогает определить, какие улучшения работают и какие могут быть внесены дополнительные изменения для достижения лучших результатов.

Последний шаг включает повторение процесса ТОС. После внесения изменений и оценки их эффективности, процесс повторяется для постоянного улучшения системы. Это подразумевает непрерывный цикл планирования, выполнения, проверки и корректировки для достижения оптимальных результатов. [2]

Одна из основных идей ТОС заключается в том, что производительность системы ограничена ее слабым звеном. Этот принцип применим к различным областям, будь то производство, услуги, логистика или ИТ. Всюду есть ограничения, которые могут замедлять процессы и ухудшать результаты, и ТОС помогает идентифицировать и управлять этими ограничениями. Следовательно, процесс оптимизации по Теории Ограничений в структуре ИТ отдела может выглядеть следующим образом.

Первый шаг, который состоит в идентификации основных ограничений, в применении к ИТ системам представляет собой выявление узких мест в процессах разработки программного обеспечения, проблем сетевой инфраструктуры, ограничений в производительности серверов и так далее.

Далее необходимо провести оптимизацию ограничений - работы баз данных, балансировку нагрузки на серверах, улучшение процессов разработки ПО или обеспечить эффективное использование доступных сетевых ресурсов. Цель состоит в том, чтобы получить максимальную пользу от ограниченных ресурсов и улучшить производительность системы.

Применение третьего шага ТОС может состоять из согласования различных компонентов ИТ инфраструктуры, принятия решений, которые учитывают ограничения, и создание процессов, которые поддерживают устранение ограничений и улучшение системы в целом.

Дальнейшие шаги в целом соответствуют своему стандартному представлению. Внедрение системы контроля может подразумевать систему отслеживания работы сотрудников, мониторинг стабильности работы сетевых ресурсов.

Применить методологию, которая изначально создавалась для оптимизации промышленного производства, в процессе разработки ИТ проектов позволяют некоторые ее особенности. Во-первых, как и говорилось ранее ограничения могут быть найдены в любой системе, независимо от ее области. Во-вторых, ТОС ставит упор на постоянное улучшение системы. Это применимо к любой организации или системе, независимо от их размера или отрасли. Постоянное улучшение является ключевым фактором успешного функционирования в современном бизнесе. Так же теория, предложенная Голдраттом, не предписывает жестких правил или шаблонов, а скорее предоставляет фреймворк для анализа и улучшения системы. Это позволяет применять ТОС в различных областях и контекстах.

Люди, которые обладают хорошими знаниями Теории ограничений (ТОС), понимают, что каждое специфическое ограничение в организации должно определять политику и нормы поведения, которые могут отличаться от других ограничений. Особенно заметна зависимость от ограничения, когда оно связано с оборотными средствами, так как это мешает приобретению необходимых материалов и использованию доступных ресурсов, и, таким образом, нарушает поток жизни организации. Это приводит к прекращению притока доходов, которые могли бы быть использованы для получения еще больших доходов и сокращения дефицита денежных средств. В такой ситуации деньги становятся и целью, и неотъемлемой необходимостью для продолжения бизнеса. Это уникальная ситуация с важными последствиями, которая должна заставить руководство действовать иначе, чем в других случаях. Когда нехватка денег угрожает существованию организации, вся концентрация высшего руководства направлена на борьбу с непрерывными кризисами, связанными с неоплатой. [3]

Этот сложный фактор, когда деньги являются целью, ограничением и непосредственной угрозой для организации, делает знание Теории ограничений и умение правильно управлять ограничением крайне важными. Хорошая новость заключается в том, что правильное поведение способствует быстрому восстановлению денежных средств в нелинейной зависимости.

Таким образом, мы подошли к еще одному важному концепту в методологии - "Пропуск" (Throughput). Пропуск определяется как скорость, с которой система генерирует "единицы цели". В контексте ТОС, Пропуск всегда выражается в единицах цели за единицу времени (например, час, день, месяц или год) или на единицу продукции. Так как по ТОС валовая прибыль является одним из основных показателей успешности бизнеса, логичным является использование денежных единиц в качестве единицы измерения цели. Таким образом, Пропуск будет выражаться в объеме денег за определенный период времени и на единицу продукции. В разрезе ИТ компании пропуск можно измерять следующими способами.

Во-первых, путем измерения доходов от продажи услуг. Это является ключевым аспектом оценки денежного потока в ИТ-компании. Это может включать доходы от разработки программного обеспечения, консалтинговых услуг, облачных сервисов и других ИТ-услуг. Например, оплату за выполненные проекты, подписку на услуги, ежемесячные или годовые платежи от клиентов. Измерение платежей, полученных от клиентов, является важным для оценки денежного притока в компанию.

Важно проводить анализ и оптимизацию денежного потока в ИТ-компании с целью максимизации притока денежных средств и управления расходами. Это может включать улучшение системы выставления счетов, контроль над задолженностями клиентов, управление проектами и ресурсами, а также управление поставщиками. Эти аспекты помогут компании более точно оценить и управлять денежными потоками, что является важным для финансовой устойчивости и роста ИТ-бизнеса.

Так же необходимо учитывать и операционные расходы, при расчете прохода. Операционные расходы в денежном потоке описывают затраты, связанные с основной операционной деятельностью компании. В контексте ИТ-компании, они могут включать следующие аспекты: зарплата и премии сотрудникам, аренда офисного пространства, затраты на оборудование и программное обеспечение, на маркетинг и рекламу.

Высокие операционные расходы могут снижать валовую прибыль компании. Если расходы превышают доходы, компания может работать в убыток. Это может оказать негативное влияние на денежный поток, поскольку компания тратит больше денег, чем получает. Так же такая тенденция может ограничивать возможности компании инвестировать в рост и развитие. Если большая часть денежных средств идет на покрытие операционных расходов, то остается меньше средств для инвестиций в новые проекты, исследования и развитие, маркетинг или развитие новых продуктов. Высокие операционные расходы могут увеличивать риск нехватки ликвидности, особенно если денежные поступления от клиентов задерживаются или непредсказуемы. [4]

Учитывая все вышесказанное, для оценки эффективности проектной разработки в ИТ отделе подходит модель расчета протока в контексте этапа разработки и этапов ожидания денежных средств от клиента. Это связано с тем, что эти два аспекта оказывают основное влияние на срок получения прибыли, и на такой важный по Теории Ограничений показатель как Коэффициент Окупаемости Инвестиций (КОИ).

Процесс расчета протока может проходить по следующему алгоритму. Во-первых, определите единицы измерения: прежде чем начать подсчет протока, определите, что вы собираетесь измерять. Например, это может быть количество выполненных задач, строк кода, часов работы и т.д. Далее, определите период измерения: решите, за какой период времени вы будете подсчитывать проток. Это может быть день, неделя, месяц или другой удобный вам интервал. Следующим шагом нужно получить информацию о выполненных задачах или других метриках, которые были выбраны для подсчета протока - информация из системы управления проектами, журналов работников, системы контроля версий и т.д. Используйте собранные данные для расчета протока с помощью простых математических операций, таких как деление количества выполненных задач на период времени. [5]

После расчета протока проанализируйте полученные данные. Посмотрите на тренды, сравните с предыдущими периодами или с целевыми показателями. Это поможет вам оценить эффективность процесса разработки и принять соответствующие меры, если это необходимо. Важно отметить, что процесс подсчета протока может варьироваться в зависимости от конкретных потребностей и методологии разработки, которую вы используете.

В идеальной ситуации протоки по разработке и по этапу ожидания денежных средств должны быть равны и иметь максимально возможное значение. Тогда никакой этап не является ограничением и не сдерживает денежные потоки.

Список литературы

1. Элияху М. Голдратт, Джеф Кокс. Цель. Процесс непрерывного совершенствования. – М.: Попурри, 2009.
2. Нечитайло И. А.. "Пять направляющих шагов теории ограничений систем: проблемы применения в стратегическом анализе" Управленческое консультирование, no. 6 (138), 2020, pp. 97-109.
3. Уильям Детмер. Теория ограничений Голдратта: системный подход к непрерывному совершенствованию. – М.: Альпина, 2008.
4. Акимов К. Управление крупным промышленным предприятием с помощью теории ограничений [Электронный ресурс] // ТОС центр: здравый смысл решений. – 2007. – Режим доступа: http://www.toc-center.ru/library/articles/big_plant_on_TOC.html.

5. Сергина А.А.. "Алгоритм внедрения теории ограничений" Социально-экономические науки и гуманитарные исследования, no. 4, 2015, pp. 36-39.

References

1. Eliyahu M. Goldratt, Jeff Cox. Goal. The process of continuous improvement. – М.: Potpourri, 2009.
 2. Nechitailo I.A. "Five heads of the theory of the boundary system: possible applications in strategic analysis". Consulting, No. 6 (138), 2020, pp. 97-109.
 3. William Detmer. Goldratt's theory of constraints: a systematic approach to continuous improvement. – М.: Alpina, 2008.
 4. Akimov K. Management of a large industrial enterprise using the theory of constraints [Electronic resource] // CBT center: common sense solutions. – 2007. – Access mode: http://www.toc-center.ru/library/articles/big_plant_on_TOC.html .
 5. Sergina A.A. "Algorithm of entry into the theory of boundaries", research papers, No. 4, 2015, pp. 36-39.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

КВАНТОВАЯ УСТРЕМЛЕННОСТЬ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

¹Лукашев А.В., ²Шабуня В.В., ³Сарафанников В.С., ⁴Билан В.В.

ФГКВОУ ВО "Военная Орденов Жукова и Ленина Краснознаменная Академия связи имени Маршала Советского Союза С.М.Буденного" МО РФ, Санкт-Петербург, Россия (194064, г. Санкт-Петербург, Тихорецкий просп., 3), e-mail: ¹lukasheff@mail.ru, ²vvsch1970@mail.ru, ³was16@mail.ru, ⁴bilanvictoriya@yandex.ru.

В статье рассмотрены повсеместно и широко внедряемые в сферы управления квантовые технологии, представляющие новые угрозы информационной безопасности, а также некоторые подходы к их снижению.

Ключевые слова: Квантовые технологии, информационная безопасность, квантовые коммуникации, способы защиты от угроз.

QUANTUM ASPIRATION AS A THREAT INFORMATION SECURITY

¹Lukashev A.V., ²Shabunya V.V., ³Sarafannikov V.S., ⁴Bilan V.V.

Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia (194064, St. Petersburg, Tikhoretsky prosp., 3), e-mail: ¹lukasheff@mail.ru, ²vvsch1970@mail.ru, ³was16@mail.ru, ⁴bilanvictoriya@yandex.ru

The article discusses quantum technologies that are widely and widely implemented in the management sphere, which pose new threats to information security, as well as some approaches to their reduction.

Keywords: Quantum technologies, information security, quantum communications, ways to protect against threats.

Международным советом ассоциаций квантовой промышленности, который был учрежден 31 января 2023 года и объединил четыре ассоциации (Quantum Industry Canada, QIC – Канада, Консорциум квантового экономического развития, QED-C – США, Quantum Strategic Industry Alliance for Revolution, Q-STAR – Япония и Европейский консорциум квантовой промышленности, QuIC – Европа), в коммюнике по итогам первого заседания заявлено: «Мы находимся в начале глобальной технологической революции» [1]. Из этой небольшой фразы можно сделать весьма определенный вывод: на текущий момент развитие квантовых технологий находится в ряду важнейших задач научно-технического прогресса.

Дорожная карта создания и развития интегрированной квантовой информационной сети с космическим сегментом Евросоюза предусматривает три этапа, рассчитанных на период с 2020 по 2036 год. Подобная дорожная карта существует и в России [2].

Таким образом, мы являемся свидетелями перехода на новый технологический уровень в сфере развития систем связи. Этому послужили многочисленные открытия, эксперименты и

разработки, в том числе в области коммуникаций. Особое значение приобретают не только вычисления и коммуникации с использованием квантовых технологий, но и попутно создаваемые угрозы существующим системам криптографии. Поэтому ниже рассмотрены такие угрозы и некоторые подходы к их снижению.

Новые угрозы информационной безопасности со стороны квантовых технологий

4 мая 2023 года российское электронное периодическое издание «3DNews», со ссылкой на американское агентство Semiconductor Digest, сообщило о начале проектирования квантовых процессоров для квантовых компьютеров емкостью миллион кубитов [3]. Ранее, 4 января 2023 года, китайские исследователи опубликовали [4] результат успешного эксперимента по взлому криптографического ключа RSA-48 с помощью разработанного ими протокола QAOA (Quantum Approximation Optimization Algorithm) на 10-ти кубитном квантовом компьютере применительно к алгоритму Шнора [5]. Авторы эксперимента предоставили аналитические расчеты по характеристикам квантового компьютера, способного взломать криптографические ключи различной длины одной из основных систем шифрования (см. таблицу 1).

Таблица 1 – Расчетные характеристики квантового компьютера для взлома криптосистем RSA

RSA number	Qubits	K _n -depth	2DSL-depth	LNN-depth
RSA-128	37	113	121	150
RSA-256	64	194	204	258
RSA-512	114	344	357	458
RSA-1024	205	617	633	822
RSA-2048	372	1118	1139	1490

В статье представлены экспериментальная установка и алгоритм реализации взлома ключа шифрования. Ценность опубликованного эксперимента состоит в декларации угрозы со стороны квантовых компьютеров в ближайшем будущем.

К этому следует добавить, что еще в ноябре прошлого года компания IBM ввела в эксплуатацию квантовый компьютер Orsey емкостью 433 кубита, а к концу текущего года запустит систему Quantum System Two емкостью 1127 кубитов. Сопоставляя эти сообщения, приходится сделать вывод о наличии реальных угроз информационной безопасности в критически важных областях, в том числе, в системах управления войсками и оружием. И уже не в отдаленном, как считалось до недавнего времени, а в ближайшем будущем.

Подходы к обеспечению информационной безопасности

Существуют различные подходы к решению возникшей проблемы безопасности. Если отбросить позицию, что ничего не надо делать, так как угроза мнимая, есть три основных варианта. Один из них – разработка и внедрение постквантовых (квантовобезопасных) алгоритмов шифрования. Другой – создание и освоение квантовых технологий, в первую очередь, квантового распределения ключей [6]. Разумный подход заключается в оптимизации соотношения этих вариантов, когда на наиболее важных информационных направлениях используются квантовые, а на менее важных – постквантовые системы криптографии.

Здесь мы формулируем подход к детализации сосуществования двух различных подходов. На рисунке 1 этот подход представлен в динамике.



Рисунок 1 – Динамическое сосуществование существующих, квантовых и постквантовых систем криптографии (ОКР – опытно-конструкторские работы, НИР – научно-исследовательские работы, КРК – квантовое распределение ключей).

Суть нашего подхода состоит в следующих основных положениях:

- квантовые технологии создают риски взлома существующим системам криптографии, однако нет гарантий того, что в будущем такой же угрозе не могут подвергнуться и постквантовые системы;
- постквантовые системы могут и должны модернизироваться с целью повышения устойчивости к взлому;
- на первом этапе внедрения квантовых технологий в системы связи специального назначения целесообразно применять квантовое распределение ключей на наиболее важных информационных направлениях. При этом необходимо уделять внимание важности исследований в создании систем связи на принципах нелокальности [7];
- на менее важных направлениях могут использоваться постквантовые (квантоустойчивые) алгоритмы шифрования;
- по мере роста угроз со стороны квантовых компьютеров, следует постепенно переводить направления с постквантовых на квантовые системы. Для упорядоченной организации такого перехода необходимо всесторонне анализировать зарубежные эксперименты и отечественные достижения в сфере развития квантовых систем вычислений с целью обоснованной оценки рисков, а также планового создания резервов квантовых систем и оборудования, подготовки кадров для их эксплуатации;
- поскольку сами квантовые системы коммуникации подвержены квантовым атакам, следует развивать методы защиты от них, в том числе создание гибридных систем, например, развитием стеганографии [8] внутри квантовых систем коммуникаций;

- с учетом аналитических оценок рисков для существующих и постквантовых систем криптографии, целесообразно создавать планы перехода на квантовые системы коммуникаций информационных направлений в соответствии с их ранжированием по важности. В свою очередь, такие планы позволяют своевременно организовать закупки оборудования для квантовых систем в промышленности.

На рисунке дополнительно показаны блоки доподготовки научных и преподавательских кадров, в том числе с использованием экспериментальных полигонов, районов и лабораторий для симуляции, либо натуральных систем для квантовых атак и разработки методов защиты от них. В этом аспекте целесообразно установить требование к защите диссертационных и дипломных работ по темам квантовых коммуникаций по результатам успешного эксперимента. Такое требование создаст условия для более оперативного решения задач, развития и укрепления информационной безопасности и в полной мере обеспечит загрузку развернутых экспериментальных полигонов.

Таким образом, суть подхода нивелирования рисков в различных сферах управления, в первую очередь, в критически важных отраслях, сводится к объективной оценке рисков и к планированию перехода систем управления на новый технологический уровень с использованием квантовых коммуникаций, что в статье представлено в общем виде. Основной этап может заключаться в создании квантовых систем на принципе нелокальности. Этот переход предполагает окончательное решение проблемы безопасности информационных систем, а квантовое распределение ключей предложено рассматривать как первый этап такого перехода.

Список литературы

1. International quantum industry councils formally joining forces for the development of quantum technologies, 02.02.2023, <https://qt.eu/about-quantum-flagship/newsroom/international-quantum-industry-councils-formally-joining-forces-for-the-development-of-quantum-technologies/>.
2. Дорожная карта развития высокотехнологичной области «Квантовые коммуникации» на период до 2030 года. Министерство цифрового развития РФ, №17 от 27.08.2020 г.
3. Детинич Г., – Процессоры для квантового компьютера на 1 млн кубитов будут выпускать в США на заводе прошлого века, 04.05.2023, Сетевое агентство 3ДНьюс, Daily Digital Digest/10-86179, <https://protsessri-dlya-rvantovogo-kompyutera-na-million-kubitov-budut-razrabativat-i-vipuskat-v-ssha-na-zavjde-proshlogo-veka>.
4. Bao Yan et.al. Factoring integers with sublinear resources on a superconducting quantum processor, <https://arxiv.org/pdf/2212.12372.pdf>.
5. C. P. Schnorr, Fast factoring integers by SVP algorithms, corrected, Cryptology ePrint Archive (2).
6. Bennett C.H., Brassard G., Quantum cryptography: public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 10-12 December, New York: IEEE Press, 1984. V. 560. P. 175-179.
7. Einstein A, Podolsky B, Rosen N (1935). “Can Quantum-Mechanical Description of Physical Realty Be Considered Complete?”. Phys. Rev. 47 (10): 777-780/ DOI: 10.1103/PhysRev./47.777; Bor N. “Can Quantum-Mechanical Description of Physical Realty Be Considered Complete?”. Phys. Rev. 48 (8): 696-702/ DOI: 10.1103/PhysRev./48.696.

8. Что такое стеганография? – <https://www.kaspersky.ru/recourse-centere/definitions/what-is-steganography>.

References

1. International quantum industry councils formally joining forces for the development of quantum technologies, 02.02.2023, <https://qt.eu/about-quantum-flagship/newsroom/international-quantum-industry-councils-formally-joining-forces-for-the-development-of-quantum-technologies/>.
 2. Roadmap for the development of the high-tech field "Quantum Communications" for the period up to 2030. Ministry of Digital Development of the Russian Federation, No. 17 dated August 27, 2020
 3. Detinich G., - Processors for a quantum computer with 1 million qubits will be produced in the USA at a factory of the last century, 05/04/2023, 3DNews Network Agency, Daily Digital Digest/10-86179, <https://protsessri-dlya-rvantovogo-kompyutera-na-million-kubitov-budut-razrabativat-i-vipuskat-v-ssha-na-zavjde-proshlogo-veka>.
 4. Bao Yan et al. Factoring integers with sublinear resources on a superconducting quantum processor, <https://arxiv.org/pdf/2212.12372.pdf>.
 5. C. P. Schnorr, Fast factoring integers by SVP algorithms, corrected, Cryptology ePrint Archive (2).
 6. Bennett C.H., Brassard G., Quantum cryptography: public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 10-12 December, New York: IEEE Press, 1984. V. 560. P. 175-179.
 7. Einstein A, Podolsky B, Rosen N (1935). "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?". Phys. Rev. 47 (10): 777-780/ DOI: 10.1103/PhysRev./47.777; Bor N. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?". Phys. Rev. 48 (8): 696-702/ DOI: 10.1103/PhysRev./48.696.
 8. What is steganography? – <https://www.kaspersky.ru/recourse-centere/definitions/what-is-steganography>.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004

ВИРТУАЛЬНЫЙ ТУР ПО УНИВЕРСИТЕТУ ДЛЯ АБИТУРИЕНТОВ

¹Васильева Д.Е., ²Сидорова А.А., ³Макуха Л.В., ⁴Сидоров А.Ю.

ФГАОУ ВО «Сибирский федеральный университет», Институт космических и информационных технологий, Красноярск, Россия (660074, г. Красноярск, ул. Академика Киренского, 26, корп. 1.), e-mail: ¹dinochka2000@list.ru, ²ayliena04@gmail.com, ³makuha_lv@mail.ru, ⁴asidorov@kgau.ru.

В век информационных технологий практически каждая организация имеет спектр всевозможных информационных сервисов. Одним из таких является виртуальный тур. Виртуальные туры создают «эффект присутствия» и дают потенциальному клиенту более полное представление об объектах и их интерьерах, нежели самые качественные цифровые фото. Их можно отнести к эффективным средствам маркетинга. Для каждого университета важно привлечь как можно больше абитуриентов, наличие такого тура на сайте – хорошая реклама для организации. Виртуальный тур может использоваться в качестве инструмента маркетинга, позволяющего показать потенциальным студентам, что может им предложить университет.

Ключевые слова: Виртуальный тур, иммерсивность, эквидистантное изображение, панорама.

VIRTUAL TOUR OF THE UNIVERSITY FOR APPLICANTS

¹Vasilyeva D.E., ²Sidorova A.A., ³Makukha L.V., ⁴Sidorov A.Yu.

Siberian Federal University, Institute of Space and Information Technologies, Krasnoyarsk, Russia (660074, Krasnoyarsk, Academician Kirensky str., 26, building 1.), e-mail: ¹dinochka2000@list.ru, ²ayliena04@gmail.com, ³makuha_lv@mail.ru, ⁴asidorov@kgau.ru.

In the age of information technology, almost every organization has a range of various information services. One of these is a virtual tour. Virtual tours create a "presence effect" and give a potential client a more complete picture of the objects and their interiors than the highest quality digital photos. They can be attributed to effective marketing tools. It is important for each university to attract as many applicants as possible, the presence of such a tour on the website is a good advertisement for the organization. A virtual tour can be used as a marketing tool to show potential students what the university can offer them.

Keywords: Virtual tour, immersiveness, equidistant image, panorama.

Каждый студент встречался с такой проблемой, что нет информации о том, где находится то или иное место в университете в первое время. Особенно тяжёлым испытанием это становится для абитуриентов – чаще всего они незнакомы с институтом и просто адрес какого-либо места может оказаться бессмысленным – потому что неизвестно, где именно будет проходить то или иное мероприятие.

Виртуальный тур по университету поможет будущим студентам быстрее найти приемную комиссию, ведь с помощью него они могут быстро найти расположение приемной комиссии на кампусе, что поможет им сэкономить время и избежать неудобств, связанных с

поиском. Кроме того, виртуальный тур может дать студентам возможность получить представление о том, что они могут ожидать от посещения приемной комиссии, что может улучшить их общий опыт поступления в университет. Приемная комиссия является важным мероприятием, где абитуриенты могут получить необходимую информацию о процессе поступления, а также задать вопросы, связанные с учебной деятельностью. Для каждого университета важно привлечь как можно больше абитуриентов, наличие такого тура на сайте – хорошая реклама для организации. Виртуальный тур может использоваться в качестве инструмента маркетинга, позволяющего показать потенциальным студентам, что университет предлагает, тур даёт возможность показа красивых и удобных учебных помещений, современного оборудования и других объектов, которые могут заинтересовать потенциальных студентов. Это может быть особенно полезно для международных студентов, которые не могут лично посетить университет, но могут использовать виртуальный тур для того, чтобы получить представление о кампусе и принять решение о поступлении. Кроме того, виртуальный тур может привлечь внимание не только студентов, но и родителей, спонсоров и других заинтересованных лиц.

Виртуальный тур включает в себя технологию визуализации среды, благодаря которой становится возможным перемещаться по университету, не находясь в нём. Возможность перемещаться по территории кампуса от первого лица делает экскурсию реалистичной, тем самым создавая эффект иммерсивности. Иммерсивные технологии отвечают за эффект присутствия: в своей простейшей форме виртуальная реальность включает 360-градусные изображения или видео. Достижение эффекта полного погружения в виртуальную реальность до уровня, когда пользователь не может отличить визуализацию от реальной обстановки, является задачей развития технологии [1]. Виртуальный тур по университету — это эффективный инструмент для привлечения новых студентов и повышения узнаваемости бренда университета в сети. Создание такого тура требует использования различных технологий и методов, а также соблюдения определенных принципов, которые помогут сделать тур интерактивным, реалистичным и удобным в использовании.

В этой части работы рассмотрены принципы, которые можно применить для создания высококачественного виртуального тура, который поможет привлечь новых студентов и повысить репутацию университета в целом:

- 1) Выбор подходящей платформы;
- 2) создание интерактивных элементов;
- 3) реалистичность и детализация;
- 4) удобство использования.

Процесс создания виртуальных туров достаточно трудоёмкий, включающий в себя несколько этапов: создание динамической карты по территории кампуса, фотосъемка, обработка и склейка изображений, 3D моделирование и представление готового сервиса виртуального тура.

Перед этапом фотосъемки нужно изучить план местности, которая будет включена в тур. Схематично составить карту для удобства выполнения задания.

Возможность перемещаться внутри тура является составляющей данной работы. Маршрут следования в туре не должен отличаться от действительности и должен совпадать с реальным расположением объектов КрасГАУ (Красноярского государственного аграрного университета) [2]. Для этой цели была составлена динамическая карта с маршрутами по

территории кампуса, с учетом расположения объектов университета – рисунок 1. Где Н – начало виртуального тура; ПК1, ПК2, ПК3 – приемные комиссии для абитуриентов; Р – парковка; ОБ – общежитие для абитуриентов; О0, О1, О2, О3, О4, О5 – обзорные точки виртуального тура.

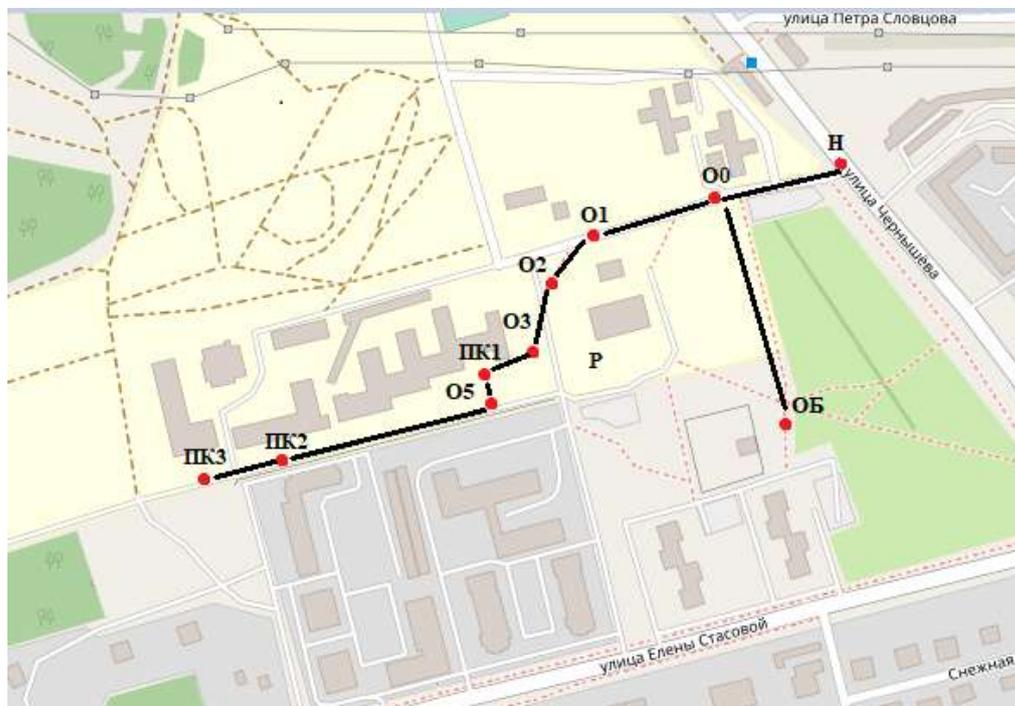


Рисунок 1 – Динамическая карта кампуса

Исходя из плана перемещений, была составлена диаграмма, отображающая связь между обзорными точками. Перемещения по туру возможны строго по линиям связи между точками. Диаграмма связей представлена на рисунке 2.

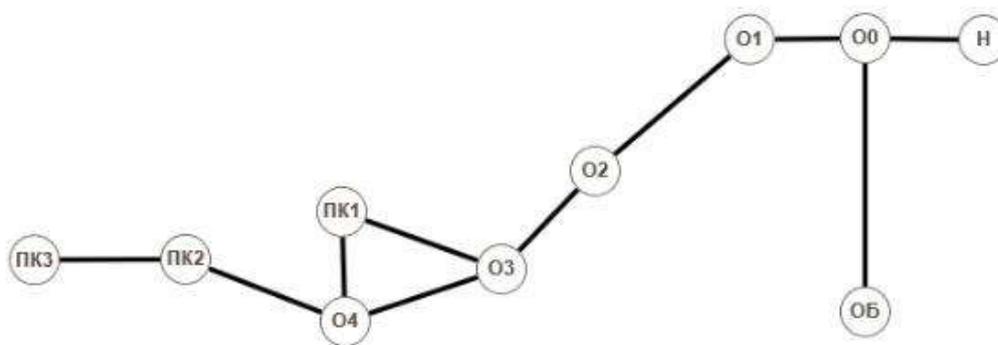


Рисунок 2 – Диаграмма связей обзорных точек

Проведение съемки – один из основных этапов работы, так как без наличия качественных изображений реализация тура становится невозможной. Съемку панорамных изображений можно проводить на различных устройствах, включая квадрокоптеры. Исходя из плана местности кампуса КрасГАУ была составлена динамическая карта. Находясь на территории кампуса, были определены конкретные положения камеры при съемке.

Квадрокоптеры могут использоваться для съемки панорамных изображений. Они оснащены камерами, которые позволяют снимать панорамы с воздушной перспективы. Квадрокоптер является средством стабилизированной съемки с возможностью свободно перемещать камеру на 360 градусов. Целесообразно упомянуть то, что при съемке на квадрокоптер нет необходимости использовать штатив, возможность свободно снять пространство без посторонних предметов (штативов, ног оператора, падающих теней) позволяет достичь реалистичности изображения и эффекта иммерсивности.

Съемка была проведена на камеру квадрокоптера Dji mini 2 [3]. Получившиеся снимки требовали последующей обработки и приведения к эквидистантной форме отображения. Это стало возможным с помощью высокоуровневого языка программирования Python и использованием его библиотек для работы с изображениями и возможностью визуализации – OpenCV. У квадрокоптеров есть множество преимуществ, поэтому было решено использовать именно его для получения необходимого результата, модель представлена на рисунке 3.



Рисунок 3 – Модель квадрокоптера Dji mini 2

Экспорт изображений с устройства производится в удобном для дальнейшей обработки формате jpg, что позволяет провести дальнейшую обработку.

Основным элементом виртуального тура являются панорамы с разворотом на 360 градусов. Данные изображения отличаются от снимков пространства отснятыми стандартными методами. Создание готовых панорамных изображений требует программной обработки.

На рисунке 4 представлены два снимка полученные при съемке. Данные снимки имеют общие точки, которые будут являться «якорями» для склеивания изображений.



Рисунок 4 – Снимки с общими точками

Алгоритм склеивания снимков состоит в обнаружении общих точек на изображениях, затем вычисляются дескрипторы, описывающие окрестность особой точки. Точки двух изображений сопоставляются на основе их сходства. После того как алгоритм нашел соответствующие точки происходит склейка изображения с помощью применения матрицы гомографии.

С целью реализации панорамных изображений для виртуального тура наиболее известны и широко применимы библиотеки 3D моделирования языка Python [4]. OpenCV — это библиотека с открытым исходным кодом, которая предоставляет мощный инструментарий для обработки изображений, включая функции сшивания панорам из нескольких снимков. Данная библиотека работает с имеющимися изображениями, проанализировав их на пиксельном уровне. С помощью OpenCV можно производить выравнивание изображений, устранение искажений, наложение и объединение снимков для создания готовых панорамных изображений, которые используются в виртуальных турах.

Виртуальный тур не должен ничем отличаться от прогулки по территории университета, поэтому функции данного тура должны обладать свойством иммерсивности. Пользователь должен полностью погрузиться в виртуальную среду. Варианты использования виртуального тура изображены на диаграмме, отображенной на рисунке 5.

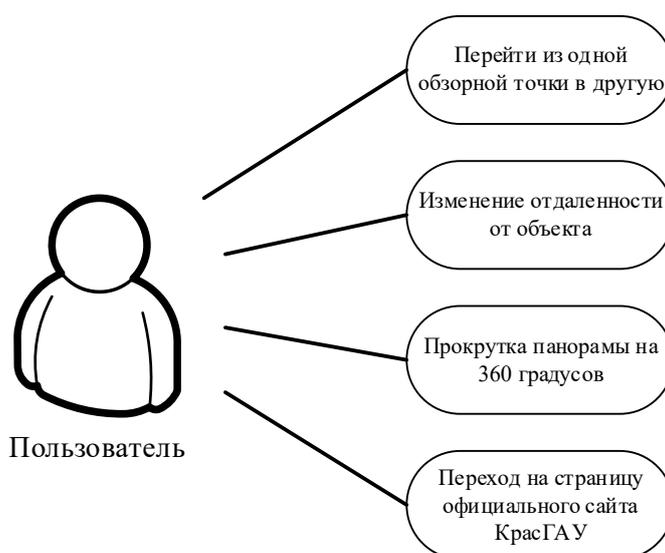


Рисунок 5 – Диаграмма вариантов использования

Изучив несколько программ для создания виртуальных туров, выбор был остановлен на программе Rapo2VR [5]. В данной программе есть возможность собрать виртуальный тур из созданных панорамных изображений с помощью языка Python. В программе есть возможность создавать зависимости между изображениями, делать между ними переходы через специальные точки (хотспоты), преобразование изображений в эквидистантную форму, прокрутка изображения на 360 градусов вокруг собственной оси, приближение и увеличение изображения. Начальная страница разработанного тура изображена на рисунке 6.

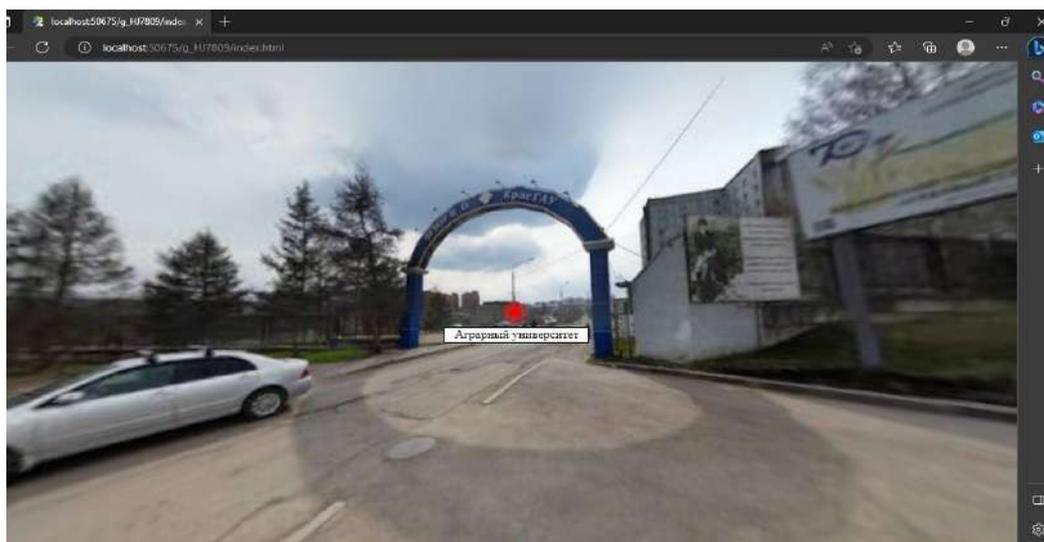


Рисунок 6 – Начальная страница виртуального тура

При помощи использованных программ и устройств получилось сделать качественный виртуальный тур, позволяющий полностью погрузиться в окружающую среду для тех, кто не может оказаться там в реальности из-за ограничений в виде расстояния и времени. Тур выполняет множество функций и является не только ознакомительным путешествием по территории КрасГАУ со станциями в виде приёмной компании, но и маркетинговым ходом для повышения популярности института в глазах абитуриентов и их родителей, что является несомненным плюсом для любой организации, что захочет сделать подобный виртуальный тур для показа себя для тех, кто заинтересован в том, чтобы стать частью данной организации.

Список литературы

1. КонсультантПлюс. оф. сайт [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_335562/d1b4d4646a5105543af88227be6909c7738c75ee (дата обращения 10.06.2023).
2. Красноярский государственный аграрный университет. Оф. Сайт [Электронный ресурс] – Режим доступа: <http://www.kgau.ru/>. (дата обращения 10.06.2023).
3. Руководство пользователя. [Электронный ресурс] – Режим доступа: https://dl.djicdn.com/downloads/DJI_Mini_2/20210222/DJI_Mini_2_User_Manual_RU.pdf. (дата обращения 10.06.2023).
4. Питон. Оф. сайт [Электронный ресурс] – Режим доступа: <https://www.python.org/>. дата обращения 10.06.2023).

References

1. ConsultantPlus. office website [Electronic resource] - Access mode: http://www.consultant.ru/document/cons_doc_LAW_335562/d1b4d4646a5105543af88227be6909c7738c75ee (accessed 06/10/2023).
 2. Krasnoyarsk State Agrarian University. Of. Website [Electronic resource] - Access mode: <http://www.kgau.ru/>. (Accessed 06/10/2023).
 3. User manual. [Electronic resource] - Access mode: https://dl.djicdn.com/downloads/DJI_Mini_2/20210222/DJI_Mini_2_User_Manual_RU.pdf. (accessed 10.06.2023).
 4. Python. Of. website [Electronic resource] - Access mode: <https://www.python.org/>. accessed 10.06.2023).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

ИССЛЕДОВАНИЕ ЗНАЧИМОСТИ ПРИЗНАКОВ ПЕРЕМЕННЫХ ПРИ ЛОКАЛЬНОМ ДИАГНОСТИРОВАНИИ ПОЛЯРНЫХ СИЯНИЙ

¹Ильясов Р.Р., Рахимов А.Р., Сахаутдинов А.А., Хайруллин Р.Д.

ФГБОУ ВО «Уфимский университет науки и технологий», Уфа, Россия (450076, г.Уфа, ул. Заки Валиди, 32), e-mail: ¹rustam.iljasov2015@yandex.ru.

Данная статья посвящена анализу временных рядов данных наблюдения полярных сияний на примере геофизической станции Ловозеро. Наиболее значимым является определение признаков, так или иначе влияющих на возникновение полярных сияний. В статье рассматриваются критерий Хи-квадрат, метод главных компонент, критерий Джини и метод прироста информации, использующихся для выявления наилучшим образом связанных переменных, при диагностировании исходных данных, а также модель, содержащая признаки и результаты наблюдения полярных сияний в зените.

Ключевые слова: полярные сияния, временной ряд, бинарная классификация, признаки, диагностирование.

INVESTIGATION OF THE SIGNIFICANCE OF VARIABLE SIGNS IN THE LOCAL DIAGNOSIS OF AURORAS

¹Ilyasov R.R., Rakhimov A.R., Sakhautdinov A.A., Khairullin R.D.

Ufa University of Science and Technology, Ufa, Russia (450076, Ufa, Zaki Validi St., 32), e-mail: ¹rustam.iljasov2015@yandex.ru.

This article is devoted to analysis of time series of auroral observation data by the example of geophysical station Lovozero. The most important is to determine the features which somehow influence on the occurrence of auroras. The article considers Chi-square criterion, method of main components, Gini criterion and information increment method used to identify the best related variables, when diagnosing the initial data, as well as the model containing signs and results of aurora borealis observations in the zenith.

Keywords: auroras, time series, binary classification, attributes, diagnostics.

Определение значимости признаков в задаче бинарной классификации является важным шагом для оптимизации процесса моделирования и улучшения качества модели. Если модель использует множество признаков, которые не оказывают значимого влияния на результат классификации, то это может привести к переобучению модели и низкой точности предсказаний на новых данных. Использование нескольких методов может помочь в выявлении взаимосвязей между признаками.

Статистические методы

При определении значимости признаков в задаче бинарной классификации используются различные методы, наиболее распространёнными из которых являются корреляция Спирмена, критерий Джини, Mutual information, критерий Хи-квадрат и другие. В

данной статье рассмотрим конкретно критерий Хи-квадрат, метод главных компонент, критерий Джини и метод прироста информации. Критерий Хи-квадрат используется для проверки гипотезы о том, что две категориальные переменные независимы. Значение критерия Хи-квадрат показывает, насколько значима связь между признаком и классом. Чем выше значение критерия, тем сильнее связь между признаком и классом, и тем более значим признак. Однако, следует учитывать, что критерий Хи-квадрат может дать ложноположительные результаты, если используется небольшое количество признаков. Поэтому необходимо проводить дополнительные тесты и оценки модели, чтобы убедиться в правильности их выбора. Рассмотрим метод главных компонент. Он представляет собой ортогональное линейное преобразование, которое отображает данные из исходного пространства признаков в новое пространство меньшей размерности. С каждой главной компонентой связана определённая доля общей дисперсии исходного набора данных. В свою очередь, дисперсия, являющаяся мерой изменчивости данных, может отражать уровень их информативности. Также данные анализировались с помощью критерия Джини, используемого для оценки качества разделения классов в задачах классификации, в том числе бинарной. Он измеряет степень неоднородности (гетерогенности) данных в узле дерева решений или ветви разделения. При использовании алгоритма дерева решений для классификации данных, критерий Джини оценивает, насколько хорошо данный узел (или разделение) разделяет классы входных данных. Чем ниже значение критерия Джини, тем лучше разделение и тем более однородные классы получаются в результирующих поддеревьях. При выводе данных критерий интерпретировался так, что чем больше число получилось при выводе, тем сильнее зависимость признака. Ещё одним задействованным методом является метод прироста информации, основанный на понятии энтропии, которая измеряет неопределённость в данных. Данный метод использует метрику, называемую информационным коэффициентом, который измеряет разницу между начальной энтропией и суммарной энтропией после разбиения данных на основе признака. Чем больше прирост информации, тем более значимым является признак.

Оценка результатов исследования

Крайне важно, чтобы результаты исследования имели максимально достижимую точность. Для реализации этой цели был выполнен анализ данных, а так же ранжирование признаков по их значимости с применением языка программирования Python. Каждый из рассматриваемых признаков имеет отношение к полярным сияниям и, так или иначе, влияет на возникновение этого явления. Использование нескольких методов позволило увидеть более полную картину значимости признаков. На Рисунках 1-4 показаны результаты исследования.

feature	p_value
diff_LOZ_F	0.00e+00
diff_LOZ_Z	0.00e+00
diff_LOZ_E	0.00e+00
diff_LOZ_N	0.00e+00
diff_delta_LOZ_Z	0.00e+00
diff_delta_LOZ_E	0.00e+00
diff_LOZ_H	0.00e+00
diff_delta_LOZ_N	0.00e+00
LOZ_I	2.56e-305
LOZ_D	2.82e-256
AP	8.14e-154
abs_delta_LOZ_E	6.03e-78
abs_delta_LOZ_N	1.49e-75
abs_delta_LOZ_Z	8.30e-64
SMR	2.38e-34
delta_LOZ_N	7.37e-33
delta_LOZ_E	3.63e-32
SME	7.49e-28
delta_LOZ_Z	6.03e-27
LOZ_Z	1.16e-08
LOZ_E	4.58e-06
LOZ_N	3.73e-05
LOZ_H	1.32e-03
LOZ_F	5.66e-03

Рисунок 1 – Оценка результатов исследования критерием Хи-квадрат

diff_LOZ_N:	0.48657888351381356
delta_LOZ_N:	0.05785316656824976
LOZ_F:	0.056688710698743684
diff_LOZ_F:	0.05664553412785451
LOZ_D:	0.045565566227290376
LOZ_Z:	0.04413968388836338
LOZ_E:	0.03100976185713527
diff_LOZ_H:	0.020251529880875856
SMR:	0.019733642149983473
delta_LOZ_E:	0.0174463488331049
delta_LOZ_Z:	0.016768613128416827
diff_delta_LOZ_N:	0.01596559347732985
abs_delta_LOZ_E:	0.014999236369752087
LOZ_N:	0.01454600581291811
abs_delta_LOZ_N:	0.014492949380883356
diff_delta_LOZ_E:	0.013334266206174233
diff_LOZ_Z:	0.01100172768605685
AP:	0.010582696987286701
diff_delta_LOZ_Z:	0.010451649432754177
diff_LOZ_E:	0.010304137624196616
LOZ_H:	0.01004553537334826
abs_delta_LOZ_Z:	0.008962386354313555
SME:	0.006391669937802115
LOZ_I:	0.006240709714978787

Рисунок 2 – Оценка результатом исследования критерием Джини

```
diff_LOZ_E: 0.24916686344615310289
diff_delta_LOZ_E: 0.24915274236170426025
diff_LOZ_Z: 0.24675907709180067151
diff_delta_LOZ_Z: 0.24674910282598605527
diff_LOZ_F: 0.24666741356132521057
abs_delta_LOZ_N: 0.24622369880771904915
diff_delta_LOZ_N: 0.24193194351239896700
diff_LOZ_N: 0.24192606617217665699
diff_LOZ_H: 0.24168660620381290927
abs_delta_LOZ_E: 0.22759755799501368845
delta_LOZ_N: -0.22725851341734026878
SME: 0.22053153161021096795
AP: 0.22007294697885704249
LOZ_H: -0.21453731369515025018
abs_delta_LOZ_Z: 0.20771114049675770685
LOZ_N: -0.20635259368666289403
LOZ_I: 0.19078525104956406411
delta_LOZ_E: 0.19052126257368390272
SMR: -0.16665366974438378112
LOZ_D: 0.12340970300788797753
LOZ_E: 0.08093936307153734577
LOZ_F: -0.04239590690438941462
delta_LOZ_Z: -0.02373080534442671002
LOZ_Z: -0.01560708420469443178
```

Рисунок 3 – Оценка результатов методом главных компонент

```
diff_LOZ_F (0.315924)
diff_delta_LOZ_N (0.313000)
diff_LOZ_N (0.312154)
diff_LOZ_Z (0.310819)
diff_LOZ_H (0.308714)
diff_delta_LOZ_Z (0.308202)
abs_delta_LOZ_N (0.287647)
diff_LOZ_E (0.275748)
diff_delta_LOZ_E (0.275485)
delta_LOZ_N (0.261736)
SME (0.236958)
AP (0.236281)
abs_delta_LOZ_E (0.222483)
abs_delta_LOZ_Z (0.214448)
delta_LOZ_E (0.186486)
delta_LOZ_Z (0.180540)
SMR (0.150853)
LOZ_F (0.149657)
LOZ_Z (0.141910)
LOZ_H (0.138375)
LOZ_N (0.122769)
LOZ_D (0.121148)
LOZ_I (0.109257)
LOZ_E (0.102780)
```

Рисунок 4 – Оценка результатов исследования критерием прироста информации

Анализ данных о полярных сияниях показал, что наиболее важными признаками являются первые производные по северной (diff_LOZ_N), восточной (diff_LOZ_F) и вертикальной (diff_LOZ_Z) составляющими. Примерно на среднем уровне значимости находятся индексы геомагнитной активности (AP, SMR, SME), а менее важными являются простые северные (LOZ_N), восточные (LOZ_F) и вертикальные (LOZ_Z) составляющие.

Заключение

Таким образом, в ходе исследования были рассмотрены различные методы определения значимости признаков в задаче бинарной классификации. Анализ полученных результатов показал, что данные методы дают схожие результаты в определении значимости признаков. Естественно, результаты подвержены определённой погрешности, но комбинация методов позволяет учесть и устранить возможные искажения, связанные с этой погрешностью, а также помочь в качественном анализе и дальнейшем использовании полученных данных в исследовании полярных сияний.

Список литературы

1. А. В. Воробьев, В. А. Пилипенко, Т. А. Еникеев, Г. Р. Воробьева, О.И. Христуло. Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций (2021). Научная визуализация 13.1: 162 - 176, DOI: 10.26583/sv.13.1.11
2. Воробьев А.В., Пилипенко В.А.. Подход к восстановлению гео- магнитных данных на базе концепции цифровых двойников. Солнеч- но-земная физика. 2021. Т. 7, No 2. С. 53–62. DOI: 10.12737/szf- 72202105.
3. Воробьев А.В., Пилипенко В.А., Сахаров Я.А., Селиванов В.Н. Статистические взаимосвязи вариаций геомагнитного поля, авро- рального электроджета и геоиндуцированных токов. Солнечно-земная физика. 2019. Т. 5, No 1. С. 48–58. DOI: 10.12737/szf-51201905.
4. Vorobev, A. V., V. A. Pilipenko, R. I. Krasnoperov, G. R. Vorobeva, and D. A. Lorentzen (2020), Short-term forecast of the auroral oval position on the basis of the “virtual globe” technology, Russ. J. Earth. Sci., 20, ES6001, doi:10.2205/2020ES000721.
5. Воробьев, А.В. Геоинформационная система для анализа динамики экстре- мальных геомагнитных возмущений по данным наблюдений наземных станций / А.В. Воробьев, В.А. Пилипенко, Т.А. Еникеев, Г.Р. Воробьева // Компьютерная оптика. – 2020. – Т. 44, No 5. – С. 782-790. – DOI: 10.18287/2412-6179-CO-707.

References

1. A.V. Vorobyov, V. A. Pilipenko, T. A. Enikeev, G. R. Vorobyova, O.I. Hristodulo. A system for dynamic visualization of geomagnetic disturbances based on data from ground-based magnetic stations (2021). Scientific visualization 13.1:162 - 176, DOI: 10.26583/sv.13.1.11
2. Vorobyov A.V., Pilipenko V.A. An approach to the restoration of geo-magnetic data based on the concept of digital twins. Solar-but-terrestrial physics. 2021. Vol. 7, No 2. pp. 53-62. DOI: 10.12737/szf- 72202105.

3. Vorobyev A.V., Pilipenko V.A., Sakharov Ya.A., Selivanov V.N. Statistical interrelations of variations of geomagnetic field, auroral electrojet and geinduced currents. Solar-terrestrial physics. 2019. Vol. 5, No 1. pp. 48-58. DOI: 10.12737/szf-51201905.
 4. Vorobev, A.V., V. A. Pilipenko, R. I. Krasnoperov, G. R. Vorobeva, and D. A. Lorentzen (2020), Short-term forecast of the auroral oval position on the basis of the “virtual globe” technology, Russ. J. Earth. Sci., 20, ES6001, doi:10.2205/2020ES000721.
 5. Vorobyov, A.V. Geoinformation system for analyzing the dynamics of extreme geomagnetic disturbances based on observations of ground stations / A.V. Vorobyov, V.A. Pilipenko, T.A. Enikeev, G.R. Vorobyova // Computer optics. – 2020. – Vol. 44, No. 5. – pp. 782-790. – DOI: 10.18287/2412-6179-CO-707.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.773

РЕАЛИЗАЦИЯ ВЕБ-ЧАТА С ИСПОЛЬЗОВАНИЕМ WEBSOCKET НА ЯЗЫКЕ GOLANG

Микрюков И.И.

ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург, Россия (190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А), e-mail: ilya.mikryukov.2001@mail.ru

В данной статье рассматривается реализация веб-чата для обмена сообщениями между пользователями в реальном времени. Для создания чата использовался язык программирования Golang и библиотека Gorilla WebSocket. В статье также есть сравнение некоторых протоколов для передачи данных между клиентом и сервером, после был сделан выбор в пользу WebSocket.

Ключевые слова: Веб-чат, Веб-сервер, WebSocket, HTTP, Golang, протоколы передачи данных.

WEB-CHAT IMPLEMENTATION USING WEBSOCKET IN GOLANG LANGUAGE

Mikryukov I.I.

St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia (190000, St. Petersburg, Bolshaya Morskaya St., 67, letter A), e-mail: ilya.mikryukov.2001@mail.ru

This article discusses the implementation of a web chat for real-time messaging between users. The chat was created using the Golang programming language and the Gorilla WebSocket library. The article also has a comparison of some protocols for transferring data between a client and a server, after which the choice was made in favor of WebSocket.

Keywords: Web chat, Web server, WebSocket, HTTP, Golang, data transfer protocols.

Данная работа посвящена вопросам разработки веб-чата, который можно использовать для прямой трансляции или в других системах, где необходимо обмениваться информацией в реальном времени с минимальной задержкой между большим количеством пользователей. На основе сравнительного анализа различных технологий передачи данных между сервером и клиентом выбран наиболее подходящий протокол для разработки такого веб-чата и описана работа как со стороны сервера, так и со стороны клиента.

Сравнение протоколов обмена данными в сети Интернет

Существуют различные способы обмена данными в сети Интернет. Рассмотрим и сравним самые популярные из них и на этой основе сделаем выбор. При сравнении протоколов использовалась информация с сайтов [1] и [2]. Самый используемый протокол передачи данных между клиентом и сервером, это HTTP (HyperText Transfer Protocol — «протокол передачи гипертекста»). HTTP – является однонаправленным протоколом передачи данных, хорошо подходит, если необходимо единожды сделать запрос информации с сервера, после

чего соединение будет автоматически разорвано. На рисунке 1 схематично представлена передача данных по HTTP протоколу. Для передачи большого объёма информации в реальном времени значительному количеству пользователей такая передача не подходит, так как имеет следующие недостатки:

- нет постоянного двунаправленного соединения;
- необходимо часто отправлять запросы на сервер, чтобы проверить, есть ли новая информация;
- каждый раз отправляется заголовок, где указывается, какой тип запроса хотим сделать;
- медленная скорость работы и лишняя нагрузка на сеть;
- перезагрузка страницы после выполнения запроса.

Есть некоторое усовершенствование HTTP запросов, это асинхронные запросы с использованием JavaScript и XML (eXtensible Markup Language — «расширяемый язык разметки»), то есть AJAX (Asynchronous Javascript and XML — «асинхронный JavaScript и XML») запросы. Они решают проблему того, что автоматически получают и отправляют данные без перезагрузки всей веб-страницы, а только некоторой части. Так как это асинхронные запросы, то пользователь во время выполнения запроса может совершать другие действия на веб-странице. Ответ от сервера можно получать не только в формате XML, но также в виде обычного текста и в формате JSON (JavaScript Object Notation — «текстовый формат обмена данными, основанный на JavaScript»). За счет асинхронных запросов последнюю проблему можно считать решенной, но предыдущие недостатки все-таки заставляют сделать вывод о нецелесообразности использования протокола HTTP при создании веб-чата.

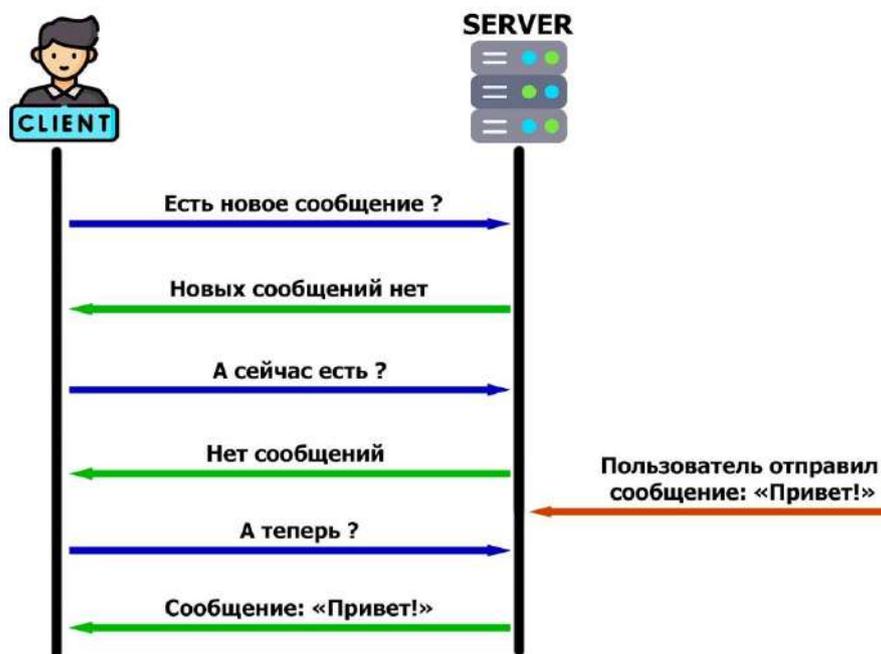


Рисунок 1 – Передача сообщения по протоколу HTTP

Еще один протокол передачи данных, заслуживающий внимания для решения поставленной задачи, это протокол WebSocket. Проанализировав информацию с сайта [3], отметим, что в данном протоколе проблемы, присущие протоколу HTTP, решены. Во-первых,

протокол WebSocket является двунаправленным, то есть можно одновременно отправлять и получать данные. На рисунке 2 схематично представлена передача данных по протоколу WebSocket. Кроме того, установленное соединение можно использовать повторно, что повышает скорость работы и уменьшает нагрузку на сеть. Пользователь отправляет на сервер запрос, при котором происходит как бы “рукопожатие” с сервером и “согласование” того, что будет использоваться WebSocket протокол. Также данный протокол поддерживает возможность сжатия данных. В протоколе реализован механизм, проверяющий подключён ли ещё пользователь или нет. Он работает следующим образом: сервер периодически посылает запрос пользователю, чтобы тот сделал “ответный” запрос на сервер, если ответ в течение некоторого времени не приходит, то происходит разрыв соединения. С его помощью можно реализовать не только веб-чат, но и другие системы, где передаётся большое количество информации между пользователями и сервером, например: биржи, push-уведомления, игровые приложения.

Рассмотрение особенностей протокола WebSocket показывает, что его использование в веб-чате более целесообразно, чем HTTP.

После выбора протокола перейдём к описанию технической части реализации веб-чата. Рассмотрим вопросы, связанные с проектированием серверной и клиентской сторон веб-чата.

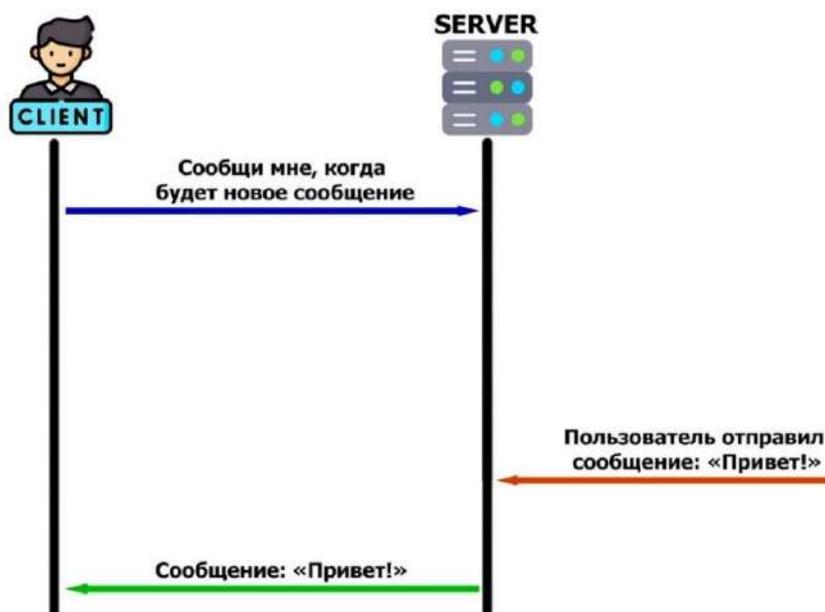


Рисунок 2 – Передача сообщения по протоколу WebSocket

Программный модуль сервера, обрабатывающего сообщения от пользователей, было решено написать на языке программирования Golang, так как его производительность в некоторых случаях выше, чем у языков PHP, JavaScript, Python и близка к C++. Golang – это компилируемый многопоточный язык, в котором есть такое понятие как goroutines (горутини). Горутини — это легковесные потоки, которые реализуют конкурентное программирование. С их помощью можно создать большое количество потоков и при этом потратить меньше памяти, чем если бы это реализовывалось на других языках программирования. Если рассматривать это в контексте веб-чата, то для масштабирования данной системы, горутини отлично подойдут.

При написании сервера использовалась информация, представленная на сайте [4]. Для реализации соединений с сервером по WebSocket была выбрана библиотека Gorilla WebSocket. Более подробная информация для работы с данной библиотекой имеется на сайте [5]. Библиотека имеет хорошую документацию и в настоящее время пользуется большой популярностью.

Рассмотрим детально, как выполняются этапы работы с созданным сервером.

- На сервере есть функция, которая принимает HTTP запросы и обновляет их до WebSocket, то есть совершает “рукопожатие”.
- Далее после успешного установления соединения, клиент записывается в массив подключенных в данный момент к серверу пользователей.
- Также есть функция, которая принимает сообщения от пользователя и передаёт их в канал данных.
- Следующая функция читает данные из канала и отправляет их всем пользователям, которые находятся в массиве активных пользователей.
- Имеется также функция, которая проверяет соединение с пользователями и разрывает его, если они неактивны.
- Сервер при получении нового сообщения от клиентов сдвигает значения ячеек массива с последними 10 сообщениями на одну позицию вверх пока не дойдёт последнего элемента, а в последнюю ячейку массива будет записываться только что полученное новое сообщение от клиента.
- При подключении к чату новый клиент будет получать последние 10 сообщений.

Теперь перейдём к рассмотрению клиентской части веб-чата. Она написана на JavaScript и работает в браузере. Изначально создаётся переменная типа WebSocket. Так как данные с сервера на клиент отправляются в JSON формате, то в функции получения сообщений, которая запускается при совершении события “получения сообщения” в вебсокет, необходимо распарсить полученные с сервера данные (записать данные в определенную структуру), после чего записать в элементы интерфейса.

Кроме того, имеется функция для отправки сообщения от клиента на сервер. В ней данные, полученные из пользовательского интерфейса, записываются в структуру, которая переводится в JSON формат и передаётся на сервер. На рисунке 3 показан веб-интерфейс разработанного чата.

Подводя итог проделанной работе, можно сказать, что обоснованный выбор протокола WebSocket, а также проектирование серверной и клиентской сторон веб-чата, подробное описание которых приведено в данной статье, позволили создать полностью рабочий веб-чат, обеспечивающий обмен информацией между большим количеством пользователей в реальном времени с минимальной задержкой.

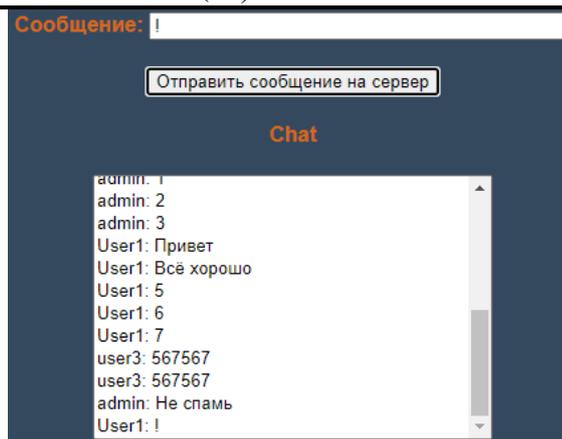


Рисунок 3 – Работа веб-чата в браузере

Список литературы

1. Почему протокол WebSocket - лучший выбор: сравнение с HTTP. [Электронный ресурс] – Режим доступа: <https://webformyself.com/websockets-vs-http/>
2. WebSocket (WSS): что это и как работают сокет, асинхронный сервер. [Электронный ресурс] – Режим доступа: <https://blog.skillfactory.ru/glossary/websocket/>
3. WebSocket. [Электронный ресурс] – Режим доступа: <https://learn.javascript.ru/websocket>
4. Простейший сервер на Gorilla WebSocket / Хабр. [Электронный ресурс] – Режим доступа: <https://habr.com/ru/articles/599737/>
5. websocket package - github.com/gorilla/websocket - Go Packages. [Электронный ресурс] – Режим доступа: <https://pkg.go.dev/github.com/gorilla/websocket>

References

1. Why the WebSocket protocol is the best choice: comparison with HTTP. [Electronic resource] – Access mode: <https://webformyself.com/websockets-vs-http/>
 2. WebSocket (WSS): what is it and how sockets work, asynchronous server. [Electronic resource] – Access mode: <https://blog.skillfactory.ru/glossary/websocket/>
 3. Web socket. [Electronic resource] – Access mode: <https://learn.javascript.ru/websocket>
 4. The simplest server on Gorilla WebSocket / Sudo Null IT News [Electronic resource] – Access mode: <https://habr.com/ru/articles/599737/>
 5. websocket package - github.com/gorilla/websocket – Go Packages. [Electronic resource] - Access mode: <https://pkg.go.dev/github.com/gorilla/websocket>
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.773.5

РЕАЛИЗАЦИЯ ПРЯМОЙ ТРАНСЛЯЦИИ С ПОМОЩЬЮ NGINX-RTMP МОДУЛЯ

Микрюков И.И.

ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург, Россия (190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А), e-mail: ilya.mikryukov.2001@mail.ru.

В данной статье рассматривается реализация прямой трансляции с использованием веб-сервера NGINX и его модуля NGINX-RTMP. Для работы сервера используется дистрибутив Linux – Ubuntu. Для запуска трансляции использовалась программа OBS, а воспроизведение происходило в плеере веб-браузера. Помимо описания работы прямых трансляций есть сравнение между собой некоторых протоколов для передачи видео. После выбора протоколов были проведены тесты с различными настройками и получено самое наименьшее время задержки.

Ключевые слова: Прямая трансляция, NGINX, NGINX-RTMP-module, HLS, DASH, протокол передачи видео.

IMPLEMENTING LIVE STREAMING USING THE NGINX-RTMP MODULE

Mikryukov I.I.

St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia (190000, St. Petersburg, Bolshaya Morskaya St., 67, letter A), e-mail: ilya.mikryukov.2001@mail.ru.

This article covers the implementation of live streaming using the NGINX web server and its NGINX-RTMP module. The server uses a Linux distribution - Ubuntu. The OBS program was used to start the broadcast, and the playback took place in the player of the web browser.

In addition to describing the operation of live broadcasts, there is a comparison between some protocols for transmitting video. After choosing the protocols, tests were carried out with various settings and the shortest delay time was obtained.

Keywords: Live streaming, NGINX, NGINX-RTMP-module, HLS, DASH, video transfer protocol.

Передача видео и звука по сети в реальном времени используется во многих приложениях и сайтах, которые работают как на стационарных компьютерах, так и на телефоне.

Существуют различные типы прямых трансляций, например, peer to peer подключения для общения между двумя людьми в мессенджере. В данном случае часто используется технология WebRTC (real-time communications — коммуникации в реальном времени). Такой тип подключения хорошо подходит для небольшой группы людей и не требует отдельно сервера для обработки видео. Также есть прямые трансляции, где один вещающий пользователь и много слушателей, подобные трансляции использует YouTube, Twitch.

Для создания сервиса с прямой трансляцией для очень большого количества людей уже необходимо использовать сервер, который будет обрабатывать получаемое видео и отправлять всем пользователям. В таком случае используются дополнительные сервисы,

которые могут это реализовать за определенную плату или пишутся свои решения, что довольно затратно.

В данной статье рассмотрена задача создания прямой трансляции, а также выбор технологий и инструментов, которые позволят это реализовать за короткий промежуток времени и будут бесплатными. После необходимо будет сделать тесты задержки видео на трансляции и подобрать подходящие настройки, чтобы как можно сильнее уменьшить задержку.

Рассмотрим прямую трансляцию, когда ведущий отправляет видео на сервер, сервер обрабатывает его и рассылает слушателям в браузер. В данном случае будет один источник видео и много слушателей, то есть это пример обычной прямой трансляции для большого количества людей. Дополнительную информацию можно найти на сайте [1]. Подробную информацию об установке сервера можно найти на сайте [2].

Перед тем как видео дойдёт до зрителя, ему необходимо пройти несколько этапов, рисунок 1:

- с помощью энкодера (в данном случае используется программа OBS (Open Broadcaster Software)) видео записывается, сжимается, преобразуется в заданный формат;
- данные отправляются на сервер для дальнейшей обработки по протоколу RTMP (Real Time Messaging Protocol);
- сервер, получив данные, может обработать их с целью, например, изменения. После сервер транскодирует видео в определенные форматы, которые могут воспроизводить зрители;

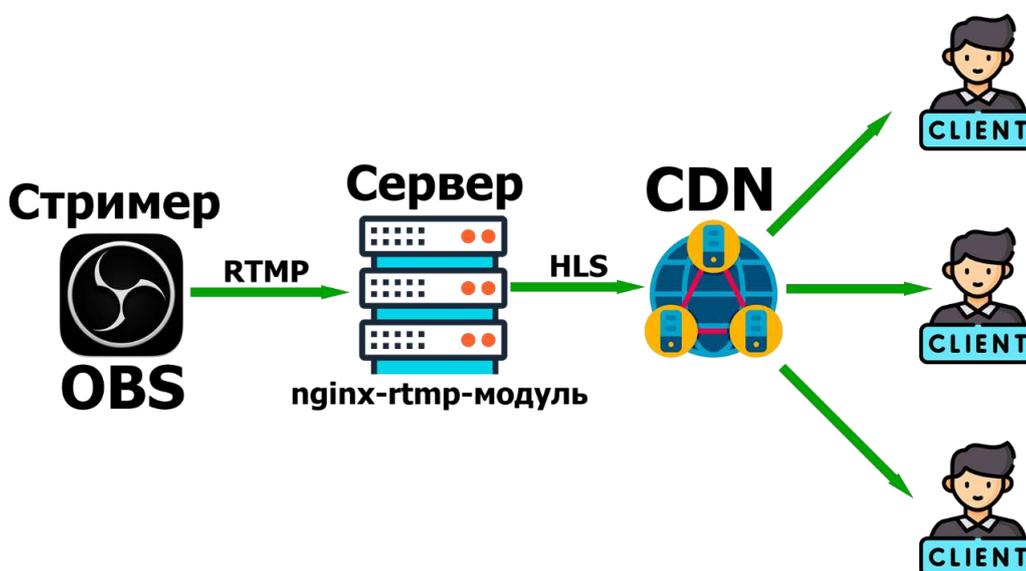


Рисунок 1 – Этапы доставки видео

- транскодированное видео передаётся по определенным протоколам (в данном случае используется протокол HLS (HTTP Live Streaming)) передачи видео зрителю. Часто используются CDN (Content Delivery Network), что представляет собой систему серверов, расположенных в разных физических местах.

Протоколы передачи видео в сети Интернет

Сначала рассмотрим протокол RTMP. Это протокол обмена информацией в реальном времени. Поддерживается на различных платформах и имеет совместимость с разными устройствами записи и серверами обработки видео.

Данные передаются с задержкой около 5 секунд, создаётся постоянный поток данных пользователям. Но этот протокол в данный момент уже мало где поддерживается в браузерах. Данные необходимо преобразовывать, чтобы их могло воспроизвести как можно большее число устройств, и передавать уже по другим протоколам.

Для решения этой задачи используются следующие протоколы: DASH (Dynamic Adaptive Streaming over HTTP) или HLS. В данном случае используется протокол HLS так как его было проще настроить. Этот протокол хорошо подходит для трансляции очень большому количеству людей. Его поддерживают много устройств и браузеров. Он поддерживает передачу видео с адаптивным битрейтом, то есть он будет изменяться в зависимости от скорости интернет-соединения.

Изначально задержка доставки видео могла достигать десятков секунд, что явно не подходит для прямых трансляций. Но в новой версии, которую поддерживают все браузеры и мобильные устройства, можно добиться времени задержки, не превышающего двух секунд.

В данном протоколе видео делится на фрагменты заданной длины. Также создаётся индексный файл, в котором хранится порядок фрагментов, он имеет заданную длину. Клиент скачивает с сервера индексный файл и доступные на данный момент фрагменты видео. Индексный файл содержит ссылки на несколько последних фрагментов. При повторном обращении к индексному файлу ссылки будут в нём обновляться на новые доступные фрагменты. Зная последовательность фрагментов из индексного файла и имея несколько последних, браузер (плеер) добавляет эти фрагменты в буфер воспроизведения в необходимом порядке. Аналогично работает доставка видео по протоколу DASH.

Измерение задержки на прямой трансляции

В данном случае используется Ubuntu server, на который установлен веб-сервер NGINX. Для обработки видеопотока используется NGINX-RTMP-модуль, который позволяет принимать по RTMP протоколу видео, обрабатывать его, и отправлять пользователям в браузер по протоколу HLS или DASH с различными настройками. Больше информации о возможных настройках и параметров можно узнать на сайтах [3] и [4]. Ниже показаны настройки сервера, а на рисунке 3 приведен программный код для работы плеера в браузере.

```
GNU nano 6.2 nginx.conf
worker_processes auto;
events {
    worker_connections 1024;
}

# RTMP configuration
rtmp {
    server {
        listen 1935; # Listen on standard RTMP port
        chunk_size 4096;

        application show {
            live on;
            # Turn on HLS
            hls on;
            hls_path /nginx/hls/;
            hls_fragment 2;
            hls_playlist_length 4;
        }
    }
}
```

Рисунок 2 – Настройки nginx-rtmp-модуля

```
function vvv()-{
    if (Hls.isSupported()){
        var video = document.getElementById('video');
        var hls = new Hls();
        hls.lowLatencyMode = true;
        hls.loadSource('http://192.168.0.171:8080/hls/test.m3u8');
        hls.attachMedia(video);
        hls.on(Hls.Events.MANIFEST_PARSED, function()-{ video.play(); });
    }
}
```

Рисунок 3 – Настройка плеера в браузере

При настройках, указанных на рисунке 2, задержка составляет 5,15 секунд, и трансляция работает стабильно. Настройки прямой трансляции вещающего в программе OBS:

- разрешение 1280x720,
- 30 кадров в секунду,
- битрейт 3000 Мбит/сек,
- ключевой кадр каждые 2 сек.

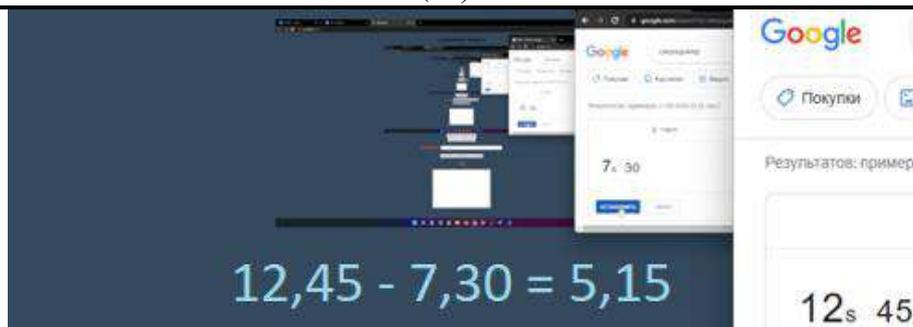


Рисунок 4 – Задержка 5,15 сек

При настройках (hls_fragment 1, hls_playlist_length 2), задержка составляет 3,54 секунд, но возможны появления “подгрузок” видео, которые скорее всего связаны с малой мощностью используемого сервера, в данном случае сервер был установлен на виртуальной машине. Настройки прямой трансляции вещающего в программе OBS:

- разрешение 1280x720,
- 30 кадров в секунду,
- битрейт 3000 Мбит/сек,
- ключевой кадр каждую 1 сек.

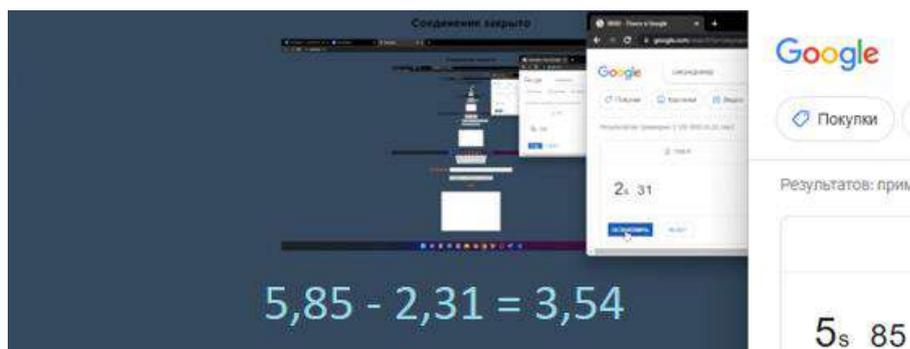


Рисунок 5 – Задержка 3,54 сек

С помощью каких команд можно обработать видео на сервере можно узнать на этом сайте [5]. В данном случае изменения видео на сервере не происходит и получаемое видео без изменений его параметров, например, битрейта будет отправляться зрителю, чтобы снизить время задержки на трансляции.

Заключение

В итоге мы смогли создать прямую трансляцию используя бесплатные инструменты. Провести тесты времени задержки и подобрать значения параметров на стороне сервера и вещающего для уменьшения задержки на трансляции.

Список литературы

1. Как делать прямые трансляции? Протоколы, кодирование, CDN. [Электронный ресурс] – Режим доступа: <https://stream-park.ru/blog/kak-delat-pryamyie-translyatsii-terminy-protokoly-kodirovanie-cdn/>

2. NGINX + rtmp. Трансляция видео с веб-сервера. Установка и настройка nginx-rtmp-module. [Электронный ресурс] – Режим доступа: <https://www.dmosk.ru/instruktions.php?object=nginx-rtmp>
3. arut/nginx-rtmp-module: NGINX-based Media Streaming Server. [Электронный ресурс] – Режим доступа: <https://github.com/arut/nginx-rtmp-module>
4. Directives · arut/nginx-rtmp-module Wiki. [Электронный ресурс] – Режим доступа: <https://github.com/arut/nginx-rtmp-module/wiki/Directives>
5. Онлайн вещание через Nginx-RTMP: несколько готовых рецептов / Хабр. [Электронный ресурс] – Режим доступа: <https://habr.com/ru/articles/174089/>

References

1. How to make live broadcasts? Protocols, coding, CDN. [Electronic resource] – Access mode: <https://stream-park.ru/blog/kak-delat-pryamyie-translyatsii-terminy-protokoly-kodirovanie-cdn/>
 2. NGINX + rtmp. Broadcast video from a web server. Installing and configuring nginx-rtmp-module. [Electronic resource] – Access mode: <https://www.dmosk.ru/instruktions.php?object=nginx-rtmp>
 3. arut/nginx-rtmp-module: NGINX-based Media Streaming Server. [Electronic resource] – Access mode: <https://github.com/arut/nginx-rtmp-module>
 4. Directives arut/nginx-rtmp-module Wiki. [Electronic resource] – Access mode: <https://github.com/arut/nginx-rtmp-module/wiki/Directives>
 5. Online broadcasting via Nginx-RTMP: several ready-made recipes / Sudo Null IT News [Electronic resource] – Access mode: <https://habr.com/ru/articles/174089/>
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.9

СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ ДЛЯ АВТОМАТИЗАЦИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Антонов Д.А.

ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова», г. Чебоксары, Россия (428015, г. Чебоксары, Чувашская Республика, Московский просп., 15), e-mail: bydevil21@gmail.com

В статье рассматривается проблема эффективной разработки программного обеспечения. Описываются наиболее распространенные современные инструменты и практики для автоматизации процесса, позволяющие его упростить, повысить качество создаваемых цифровых продуктов и снизить общую стоимость IT-проектов. Целевая аудитория – разработчики, тестировщики, аналитики.

Ключевые слова: Разработка программного обеспечения, инструменты автоматизации, интегрированная среда разработки, искусственный интеллект, машинное обучение, облачные технологии, low-code, no-code, IDE, BaaS, CaaS, FaaS, IaaS, PaaS, SaaS.

MODERN TOOLS FOR AUTOMATING SOFTWARE DEVELOPMENT

Antonov D.A.

S FSBEI of HE "I.N. Ulianov Chuvash State University", Cheboksary, Russia (428015, Cheboksary, Chuvash Republic, Moskovsky Ave., 15), e-mail: bydevil21@gmail.com

The article deals with the problem of effective software development. The most common modern tools and practices for process automation are described, which make it possible to simplify the process, improve the quality of digital products and reduce the overall cost of IT projects. Target audience – developers, testers, analysts.

Keywords: Software development, automation tools, integrated development environment, artificial intelligence, machine learning, cloud technologies, low-code, no-code, IDE, BaaS, CaaS, FaaS, IaaS, PaaS, SaaS.

В процессе создания программной системы каждый разработчик нередко сталкивается с необходимостью применения типовых синтаксических конструкций, стандартных логических шагов и алгоритмов, а также прочих шаблонных взаимодействий. Несмотря на широкие возможности, предоставляемые современными языками программирования высокого уровня, данная проблема остается актуальной даже при использовании различных парадигм и лучших инженерных практик.

Нацеленность на более простое восприятие кода человеком в совокупности с необъятной вариативностью прикладных задач и путей для их решения, приводят к невозможности формализации всех возможных инструкций в универсальный лаконичный формат. Именно эти факторы в значительной мере приводят к необходимости персонализации инструментов для разработки и командного взаимодействия в случае стремления к максимальной эффективности при реализации программных продуктов.

К современным средствам, позволяющим конструировать программные комплексы различных масштабов, в первую очередь, относятся интегрированные среды разработки. Получившие огромную популярность за последнее десятилетие в силу удобства использования и гибкости настройки, они помогают решать большинство прикладных проблем быстро и эффективно. Однако в последние годы также активно применяются специализированные облачные сервисы и инструменты на основе искусственного интеллекта в дополнение к IDE, а также обособлено – для ряда задач.

Выбор наиболее подходящего инструмента обычно зависит от имеющихся у специалиста знаний, навыков и ресурсов, а также целевых задач и потенциальных внешних требований. В данной работе будут рассмотрены перечисленные выше современные технологии, их преимущества в решении задач по реализации необходимой программной функциональности и дальнейшие перспективы. Это позволит сформировать понимание о том, как оставаться конкурентоспособным игроком в стремительно растущей IT-отрасли.

Основная часть

1. Интегрированные среды разработки

Целевая аудитория: разработчики, тестировщики.

В данную категорию входят различные программные средства, предназначенные для разработчиков и выполняющие вспомогательные функции для более быстрого решения задач, связанных с написанием кода. Среди ключевых функций, позволяющих продуктивно работать с системами различных масштабов, можно выделить следующие:

- автоматическое дополнение (в том числе, благодаря инструментам на основе машинного обучения);
- контекстные подсказки, сообщающие о возможных операциях в текущем окружении, наличии ошибок или иных проблемах;
- генераторы шаблонных частей из predetermined заготовок («сниппетов»);
- утилиты, порождающие код из декларативных спецификаций или графических схем.

Довольно длительное время каждый из продуктов, появляющийся на рынке текстовых редакторов и интегрированных сред разработки, стремился охватить наибольшую часть аудитории, предоставляя подобные возможности различного качества на основе внутренних разработок. Однако в процессе развития IT-индустрии, в ходе которого все сильнее проявлялась тенденция глобализации, стратегии присутствующих игроков менялись: все чаще стали предприниматься попытки по достижению технических договоренностей, единым подходам и протоколам взаимодействия.

По этим причинам профессиональные инструменты становились более гибкими, позволяя сторонним разработчикам осуществлять интеграции для расширения встроенной функциональности посредством механизмов плагинов. Также были сделаны серьезные шаги в направлении унификации инженерных соглашений по единым форматам структурирования информации и ее шаблонизации, а также по обмену данными и их обработке.

Это привело к тому, что, в соответствии с современными архитектурными подходами, IDE чаще всего представляют собой модульные системы и обеспечивают различные способы настройки под собственные нужды. Работа, проделанная тысячами высококвалифицированных инженеров отрасли, позволила дать доступ каждому программисту, независимо от уровня его компетенций, к гибкой настройке ежедневно

используемых инструментов. В свою очередь, данный фактор послужил дополнительным импульсом для развития индустрии: она стала расширяться с большей скоростью благодаря улучшению межгруппового и внутрикомандного взаимодействия, росту личной эффективности и снижению порога входа в мир корпоративных систем. Поэтому можно с большой уверенностью считать, что среды интегрированной разработки останутся важнейшими помощниками на ближайшее десятилетие.

2. Облачные технологии

Целевая аудитория – разработчики, тестировщики, аналитики.

Данный подход подразумевает наличие в цепи процесса создания ПО промежуточного звена – облачного провайдера. Разработчик (аналитик, компания) при подобной модели не нуждается в самостоятельном приобретении высокопроизводительной техники для функционирования создаваемых программных систем, поскольку все процессы по обработке информации могут выполняться на удаленных ресурсах, за пользование которыми необходимо осуществлять регулярную оплату, соразмерную объему выполненных операций и мощности арендованных вычислительных машин [1].

При использовании рассматриваемой схемы достигается эффективное использование ресурсов в целевых прикладных задачах благодаря отсутствию необходимости в регулярном решении инфраструктурных проблем. Чаще всего облачные решения используют малочисленные команды и молодые компании, для которых покупка дорогостоящего оборудования является серьезным экономическим испытанием. Однако, стоит отметить, что крупные компании также нередко обращаются к рассматриваемой модели – например, для проведения различных экспериментов отдельными группами разработки.

Несмотря на то, что основные концепции облачных вычислений были опубликованы еще в конце прошлого столетия, активное развитие и распространение облачные технологии получили лишь в течение последнего десятилетия. Это обусловлено, в первую очередь, имеющимися ранее техническими ограничениями, которые удалось преодолеть. Так, например, среди ключевых достижений можно выделить следующие:

1. Широкополосное интернет-подключение – стала возможной быстрая передача данных между удаленными серверами и пользовательскими устройствами.

2. Высокоскоростные сети – оптические сети, обеспечивающие эффективную коммуникацию, привели к возможности создания распределенных дата-центров.

3. Виртуализация – возможность создания виртуальных экземпляров операционных систем, хранилищ данных и иных сетевых ресурсов для эффективного использования физических мощностей с обеспечением изолированности и гибкости настройки.

4. Централизованное управление ресурсами – контроль за вычислительными мощностями и предоставление их по требованию пользователя в режиме реального времени.

5. Автоматизация и оркестрация – позволили создавать гибкую инфраструктуру из физических и виртуальных элементов для автоматизированного масштабирования ресурсов, управления нагрузкой между серверами и реализации эффективного мониторинга.

6. Большие объемы данных (Big Data) – совершенствование подходов по хранению, обработке и анализу данных позволило справляться с непрерывными потоками информации.

Перечисленные достижения научно-технического прогресса в значительной мере способствовали ускоренному совершенствованию существующих подходов в разработке

программного обеспечения и формированию новых. Большинство из них стали фундаментальными для возможности становления облачных технологий и их применения как в профессиональной сфере, так и в повседневной жизни современного человека [2-3].

На сегодняшний день в обширных перечнях облачных услуг, предоставляемых специализированными провайдерами, чаще всего встречаются следующие позиции:

- **ВaaS (Backend-as-a-service – серверная часть, как услуга)** – предоставляется настроенная функциональность и инфраструктура для управления серверной частью приложений;
- **Саas (Containers-as-a-service – контейнеры, как услуга)** – виртуализация на основе контейнеров, позволяющая упростить управление как отдельными микросервисами, так и реализовать оркестрацию над сложными механизмами;
- **Фаas (Function-as-a-service – функция, как услуга)** – возможность «бессерверного» запуска фрагментов кода (н-р, отдельных функций) при наступлении определенных событий в облачной системе;
- **Иаas (Infrastructure-as-a-service – инфраструктура, как услуга)** – гибкая масштабируемая инфраструктура из необходимого количества виртуальных машин и иных вычислительных ресурсов для развертывания приложений с возможностью простого управления;
- **Раas (Platform-as-a-service – платформа, как услуга)** – полноценная платформа для разработки, включающая оборудование, необходимое программное обеспечение с лицензиями, а также настройку и обслуживание облачной инфраструктуры.
- **Саas (Software-as-a-service – программное обеспечение, как услуга)** – возможность аренды лицензионного программного обеспечения и его использования через Интернет без необходимости в самостоятельной настройке и поддержке на собственных мощностях.

Каждая из услуг содержит специализацию под конкретные нужды. Они имеют множество общих преимуществ и недостатков, поскольку базируются на основных принципах облачных технологий. Перечень общих достоинств, не включающий перечисленные ранее достижения НТП, представлен ниже [4-5]:

1. Гибкость и масштабируемость – использование вычислительных ресурсов исключительно по мере необходимости, а также в объеме и производительности в зависимости от потребностей и нагрузки системы.

2. Упрощение управления и снижение затрат – отсутствие необходимости в формировании и полного обслуживания собственной инфраструктуры, автоматизация различных процессов управления, удобство настройки через графический пользовательский интерфейс.

3. Высокий уровень доступности и отказоустойчивости – специализация центров обработки данных в процессах распределения ресурсов, репликации и защиты данных на множестве физических машин.

4. Повышение эффективности – необходимость в меньшей численности команды с фокусом на разработку для качественного улучшения программного продукта.

Ключевые недостатки облачных услуг:

1. Потенциальные проблемы с безопасностью и конфиденциальностью данных, требующие доверия и гарантий со стороны провайдера, особенно в случаях, когда взаимодействие происходит через сторонние серверы или страны.

2. Риск возникновения проблем с производительностью, доступностью и иных технических сложностей в случае сбоев у поставщика, на которые нельзя повлиять самостоятельно.

3. Зависимость от поставщика – ограничения в настройке инфраструктуры и других частей, которые могут затруднить адаптацию некоторых приложений и ресурсов. Возможные проблемы с совместимостью при миграции между различными облачными платформами.

Таким образом, рассматриваемый подход имеет огромные перспективы по улучшению и большему распространению в разных областях. В большей степени, это связано с активным развитием технологий и цифровизацией человеческой деятельности. Исходя из этого, можно ожидать, что в ближайшее десятилетие роль облачных технологий станет еще более значимой [6].

3. Инструменты на основе машинного обучения

Целевая аудитория – программисты, тестировщики.

Искусственный интеллект и его применение в различных прикладных областях становятся все более распространенными в последние годы, и одной из таких сфер является разработка программного обеспечения. Современные методы и технологии машинного обучения позволяют автоматизировать процессы написания текстов программ, повысить эффективность и качество разработки, а также ускорить время выхода на рынок программных продуктов.

Одной из ключевых возможностей, которую предоставляют «умные» инструменты для написания программного кода, является автоматическое дополнение. Благодаря анализу больших объемов кодовых баз, подобные утилиты могут предлагать разработчику подсказки в процессе работы с текстами программ. Это упрощает специалисту работу, снижает вероятность ошибок и позволяет быть более эффективным при решении задач. Данная функция успешно используется в современных интегрированных средах разработки уже в течение длительного периода, что было отмечено ранее.

Следующим важным аспектом применения инструментов на основе машинного обучения является автоматическое обнаружение и исправление ошибок. Специализированные алгоритмы позволяют анализировать код и выявлять потенциальные проблемы: неправильное использование переменных, несоответствие синтаксису или возможные уязвимости. После обнаружения ошибок утилита может предложить перечень необходимых правок или самостоятельно внести изменения для более эффективного решения проблем.

Инструменты на основе искусственного интеллекта также предоставляют возможности по генерации кода на основе заданных требований. С помощью методов глубокого обучения и генеративных моделей утилита может создавать код, соответствующий определенным спецификациям и шаблонам. Это особенно полезно в случаях, когда требуется большой объем повторяющихся частей или при разработке прототипов, когда нужно быстро получить некоторую функциональность [7-8].

Анализ и оптимизация существующего кода также являются одним из возможных применений инструментов рассматриваемого типа. Алгоритмы машинного обучения и

статистические методы позволяют проводить статический анализ кода, идентифицировать узкие места и неэффективные алгоритмы. Помимо этого, подобные утилиты могут предлагать оптимизированные варианты, которые повысят производительность программы, снизят потребление ресурсов или улучшат общее качество кода.

Последняя ключевая прикладная помощь – возможность автоматического создания документации к коду. Анализируя комментарии, описания и структуру программы, инструмент может автоматически генерировать читаемую и информативную документацию для упрощения понимания и использования кода другими разработчиками.

В качестве обобщения следует отметить, что применение инструментов на основе искусственного интеллекта открывает широкий спектр возможностей для улучшения эффективности, качества и скорости. Несмотря на то, что, на сегодняшний день генерируемые фрагменты не всегда являются полностью готовыми к непосредственному использованию, прослеживается тенденция на совершенствование: определенные утилиты периодически генерируют программный код лучше специалистов среднего уровня. Это значительный прогресс, демонстрирующий, как можно использовать результаты машинного обучения в процессе разработки для более быстрого решения проблем [9].

Заключение

Рассмотренные в данной статье подходы по автоматизации разработки программного обеспечения являются передовыми на сегодняшний день и имеют большие перспективы на улучшение и более широкое распространение на ближайшем этапе развития информационных технологий. Особое внимание следует уделить применению различных облачных услуг и инструментов на основе машинного обучения, чтобы повысить собственную эффективность, снизить стоимость создания программных продуктов и не отставать от технического прогресса, набирающего все большую скорость с каждым годом.

Список литературы

1. Арутюнов, Г. А. Большие трансформеры для генерации кода. / Г. А. Арутюнов, С. М. Авдошин. - Текст : электронный // Труды института системного программирования РАН. - 2022. - № 4 (34). - С. 79-88. URL: <https://elibrary.ru/item.asp?id=50005199> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
2. Ванясин, Н. В. Архитектура интегрированной среды разработки программного обеспечения с поддержкой структурного редактирования / Н. В. Ванясин, И. Г. Сидоркина, В. И. Поляков. - Текст : электронный // Научно-технический вестник информационных технологий, механики и оптики. - 2019. - № 6 (19). - С. 1079-1085. URL: <https://www.elibrary.ru/item.asp?id=41559161> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
3. Воронцов, А. И. Анализ различных инструментов управления и мониторинга облачной инфраструктурой / А. И. Воронцов, А. А. Бусенков, О. Д. Куприков. - Текст : электронный // Экономика и качество систем связи. - 2022. - № 2 (24). - С. 65-71. URL: <https://www.elibrary.ru/item.asp?id=48591219> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.

4. Гончаренко, В. А. Актуальные проблемы моделирования конфигураций объектов виртуальной среды единого информационного пространства / В. А. Гончаренко, Д. И. Казанцев. - Текст : электронный // Информация и космос. - 2018. - № 3. - С. 89-95. URL: <https://www.elibrary.ru/item.asp?id=35785169> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
5. Какутин, Д. Ю. Обзор вспомогательных инструментов на основе машинного обучения для написания исходного кода программ / Д. Ю. Какутин, А. С. Дмитриев, И. А. Абрамов. - Текст : электронный // Электронный научный журнал «Инженерный вестник Дона». - 2022. - № 5 (89). - С. 27-33. URL: <https://www.elibrary.ru/item.asp?id=48925589> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
6. Матвеев, А. О. Разработка программных средств для улучшения работы механизма автодополнения кода с использованием алгоритмов машинного обучения в интегрированной среде разработки для языка Python / А. О. Матвеев, А. В. Быстров, В. И. Бибаев, Н. И. Поваров. - Текст : электронный // Вестник Новосибирского государственного университета. Серия: Информационные технологии. - 2020. - № 2 (18). - С. 62-75. URL: <https://www.elibrary.ru/item.asp?id=43848163> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
7. Мейкшан, В. И. Выбор оптимального размещения данных при использовании облачной инфраструктуры / В. И. Мейкшан, Н. Б. Тесля. - Текст : электронный // Журнал "Доклады Академии наук высшей школы Российской Федерации" - содержание выпуска № 2(51) за 2021 год. - 2021. - № 2 (51). - С. 34-42. URL: <https://www.elibrary.ru/item.asp?id=46311534> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
8. Минакова, О. В. Разработка программных инструментов на базе расширяемых платформ с открытым исходным кодом / О. В. Минакова, Н. В. Акамсина, О. В. Курипта. - Текст : электронный // Вестник Воронежского государственного технического университета. - 2022. - № 4 (18). С. 56-63. URL: <https://www.elibrary.ru/item.asp?id=49369730> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
9. Мурат, Е. П. Внедрение облачных технологий как вектор развития компании / Е. П. Мурат. - Текст : электронный // Вестник Академии знаний. - 2020. - № 2 (37). - С. 205-211. URL: <https://cyberleninka.ru/article/n/vnedrenie-oblachnyh-tehnologiy-kak-vektor-razvitiya-kompanii> (дата обращения: 02.06.2023). - Режим доступа: Научная электронная библиотека «КиберЛенинка».

References

1. Arutyunov, G. A. Large transformers for code generation. / G. A. Arutyunov, S. M. Avdoshin. - Text: electronic // Proceedings of the Institute for System Programming of the Russian Academy of Sciences. - 2022. - No. 4 (34). - S. 79-88. URL: <https://elibrary.ru/item.asp?id=50005199> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
2. Vanyasin, N.V., Sidorkina, I.G., Polyakov, V.I. Architecture of an integrated software development environment with structural editing support. - Text: electronic // Scientific and

- technical bulletin of information technologies, mechanics and optics. - 2019. - No. 6 (19). - S. 1079-1085. URL: <https://www.elibrary.ru/item.asp?id=41559161> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
3. Vorontsov, A. I., Busenkov, A. A., Kuprikov, O. D. Analysis of various tools for managing and monitoring cloud infrastructure. - Text: electronic // Economics and quality of communication systems. - 2022. - No. 2 (24). - S. 65-71. URL: <https://www.elibrary.ru/item.asp?id=48591219> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 4. Goncharenko, V. A. Actual problems of modeling the configurations of objects of the virtual environment of a single information space / V. A. Goncharenko, D. I. Kazantsev. - Text: electronic // Information and space. - 2018. - No. 3. - S. 89-95. URL: <https://www.elibrary.ru/item.asp?id=35785169> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 5. Kakutin, D. Yu., A. S. Dmitriev, I. A. Abramov, A review of auxiliary tools based on machine learning for writing program source code. - Text: electronic // Electronic scientific journal "Engineering Bulletin of the Don". - 2022. - No. 5 (89). - S. 27-33. URL: <https://www.elibrary.ru/item.asp?id=48925589> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 6. Matveev, A. O. Development of software tools for improving the code completion mechanism using machine learning algorithms in an integrated development environment for the Python language / A. O. Matveev, A. V. Bystrov, V. I. Bibaev, N. I. Povarov. - Text: electronic // Bulletin of the Novosibirsk State University. Series: Information technologies. - 2020. - No. 2 (18). - S. 62-75. URL: <https://www.elibrary.ru/item.asp?id=43848163> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 7. Meikshan, V. I. The choice of optimal data placement when using cloud infrastructure / V. I. Meikshan, N. B. Teslya. - Text: electronic // Journal "Reports of the Academy of Sciences of the Higher School of the Russian Federation" - content of issue No. 2 (51) for 2021. - 2021. - No. 2 (51). - S. 34-42. URL: <https://www.elibrary.ru/item.asp?id=46311534> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 8. Minakova, O. V. Development of software tools based on extensible open source platforms / O. V. Minakova, N. V. Akamsina, O. V. Kuripta. - Text: electronic // Bulletin of the Voronezh State Technical University. - 2022. - No. 4 (18). pp. 56-63. URL: <https://www.elibrary.ru/item.asp?id=49369730> (date of access: 06/02/2023). - Access mode: Scientific electronic library eLIBRARY.RU.
 9. Murat, E. P. Implementation of cloud technologies as a vector of company development / E. P. Murat. - Text: electronic // Bulletin of the Academy of Knowledge. - 2020. - No. 2 (37). - S. 205-211. URL: <https://cyberleninka.ru/article/n/vnedrenie-oblachnyh-tehnologiy-kak-vektor-razvitiya-kompanii> (date of access: 06/02/2023). - Access mode: Scientific electronic library "KiberLeninka".
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

¹Андреева Я.А., ²Василевский К.А.

Ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики» (МТУСИ), Москва, Россия (123423, Москва, ул. Народного Ополчения, 32), e-mail: ¹andreevaya.00@mail.ru, ²alaxtver@yandex.ru.

В настоящее время, параллельно со стремительным развитием технологий постоянно растет количество различного рода атак злоумышленников, а также скорость генерации новых способов проникновения в системы. Злоумышленники постоянно разрабатывают новые механизмы вторжения и вредоносные программы, а это значит, что вопрос обеспечения информационной безопасности останется актуальным еще долгое время. На данный момент ключевым элементом обеспечения информационной безопасности являются системы обнаружения вторжений (СОВ). В данной статье представлен обзор архитектуры современных СОВ, а также дан сравнительный анализ некоторых открытых средств обнаружения вторжений.

Ключевые слова: информационная безопасность, вторжения, системы обнаружения вторжений, СОВ.

ANALYSIS OF MODERN INTRUSION DETECTION SYSTEMS

¹Andreeva Ya.A., ²Vasilevsky K.A.

MTUCI, Moscow, Russia (123423, Moscow, Narodnogo Opolcheniya st., 32), e-mail: ¹andreevaya.00@mail.ru, ²alaxtver@yandex.ru.

Nowadays, in parallel with the rapid development of technology, the number of various kinds of attacks by intruders is constantly growing, as well as the speed of generating new ways to penetrate systems. Attackers are constantly developing new intrusion mechanisms, which means that the issue of ensuring information security will remain relevant for a long time. At the moment, intrusion detection systems (IDS) are a key element of ensuring information security. This article provides an overview of the architecture of modern IDS, as well as a comparative analysis of some open intrusion detection tools.

Keywords: information security, intrusions, intrusion detection systems, IDS.

Программные продукты всех производителей имеют уязвимости, которые могут представлять угрозу информационной безопасности. Вредоносное программное обеспечение используется в качестве основного инструмента для эксплуатации этих уязвимостей.

В наши дни скорость генерации вредоносных программ очень высока. Это связано с тем, что злоумышленники владеют различными механизмами, позволяющими им генерировать новые варианты вредоносных программ, то есть создавать мутации. Например, полиморфные и метаморфические механизмы модифицируют некоторые части исходного кода вредоносного ПО, вследствие чего антивирусное программное обеспечение не в состоянии его обнаруживать.

Исторически люди использовали системы обнаружения вторжений (СОВ) для защиты своих сетей от злонамеренных воздействий. Традиционные системы обнаружения вторжений включают в себя мониторинг сети и обнаружение сетевых атак с помощью сигнатур. Такие СОВ успешно справляются с задачей обнаружения известных атак, но терпят неудачу в случае возникновения новых. Кроме того, появление новых шаблонов требует обновления базы данных сигнатур, содержащей определение атак, что увеличивает потенциальное окно злонамеренного воздействия.

В методическом документе ФСТЭК России представлено следующее определение СОВ: «система обнаружения вторжений — программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней [1]».

Другими словами, системы обнаружения вторжений (англ. Intrusion Detection System (IDS)) — это программные или аппаратные средства, которые позволяют обнаруживать и реагировать на попытки несанкционированного доступа к компьютерной системе или сети.

IDS-системы бывают двух типов: сетевые IDS и хост-IDS. Сетевые IDS используются для мониторинга трафика на сетях. Они работают, просматривая пакеты данных, которые передаются по сети, и обнаруживая аномалии в этом трафике. Сетевые IDS могут быть установлены на маршрутизаторах или коммутаторах, чтобы мониторить весь трафик, проходящий через них. Также могут быть установлены на специальном сервере, который будет мониторить весь трафик в сети. Хост-IDS работают на уровне операционной системы и отслеживают активность на конкретном компьютере. Они могут обнаруживать попытки взлома, вирусы, трояны и другие виды вредоносного программного обеспечения, которые могут появиться на компьютере. IDS-системы могут быть настроены на обнаружение различных типов атак: попытки взлома паролей, DoS-атаки, сканирование портов и другие. Когда IDS обнаруживает атаку, он может сгенерировать оповещение администратору системы или автоматически запустить процедуры реагирования на эту атаку.

IDS-системы являются важной частью защиты компьютерных систем и сетей от кибератак. Они позволяют быстро обнаруживать аномалии в трафике и предпринимать соответствующие меры для защиты системы.

Анализ обобщенной архитектуры СОВ

На рисунке 1 представлена обобщенная структура СОВ.

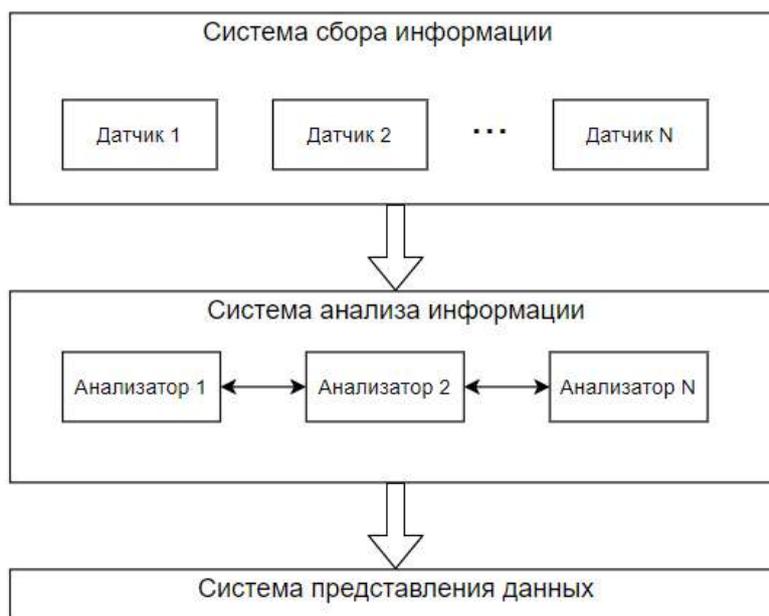


Рисунок 1 – Структурная схема СОВ

В структуре современных СОВ выделяют три главных элемента, представленных на рисунке 2.



Рисунок 2 – Основные элементы СОВ

Система сбора информации собирает информацию о работе объекта защиты. Для сбора информации используются автономные модули – датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы.

Система анализа состоит из одного или более модулей анализа, которые принято называть анализаторами. Для повышения эффективности обнаружения вторжений, в некоторых системах применяется несколько различных анализаторов.

В качестве входных данных анализаторов выступает информация из системы сбора информации или от других анализаторов.

Результатом работы системы анализа информации является индикация о состоянии защищаемой системы. В случае, если анализатором обнаружено злонамеренное действие, на его выходе появляется некоторая дополнительная информация о зафиксированном нарушении.

Подсистема представления данных выполняет функцию информирования пользователей СОВ о состоянии объекта защиты.

Таким образом, анализаторы являются ключевыми элементами СОВ, которые выполняют роль классификаторов входных данных. Именно анализаторы принимают решение об отнесении поданной на вход информации к какому-либо классу.

Обзор открытых средств обнаружения вторжений

Рассмотрим некоторые СОВ с открытым исходным кодом.

Несмотря на широкое распространение и возрастающую потребность в защите информации, открытых систем обнаружения вторжений крайне мало.

Всего будет рассмотрено 6 наиболее распространенных открытых СОВ. Их краткое описание представлено в таблице 1.

Таблица 1 – Краткое описание открытых СОВ

Наименование СОВ	Ссылка
AAFID	http://www.cs.purdue.edu/coast/projects/autonomousagents.html
ASAX	http://www.ja.net/CERT/Software/asax/
NetSTAT	http://www.cs.ucsb.edu/~kemm/netstat.html/
Prelude	http://www.prelude-ids.org/
SHADOW	http://www.nswc.navy.mil/ISSEC/CID
Snort	http://www.snort.org/

Важнейшим критерием оценки СОВ в рамках данного сравнения является адаптивность к неизвестным атакам. Этот критерий определяет способность СОВ обнаруживать атаки «нулевого дня».

Адаптивность к неизвестным атакам, как и эффективность СОВ зависит от применяемых методов анализа полученной информации.

Большинство существующих систем используют эвристические методы обнаружения атак, которые позволяют детектировать и производить классификацию атак, опираясь на неполные данные и порой неверную классификацию.

Системы, рассмотренные в рамках данного сравнительного анализа, применяются для выявления различного класса атак. Некоторые из них подходят для обнаружения локальных атак и применяют в этих целях журналы систем аудита, журналы регистрации приложений, ОС. К такому типу СОВ относятся AAFID и ASAX.

Для обнаружения сетевых атак наиболее подходящими будут системы, которые используют в качестве источников сетевой трафик. К системам с данным подходом можно отнести Snort, SnortNet и SHADOW.

Остальные СОВ являются гибридными и способны детектировать как локальные, так и внешние атаки.

AAFID (Advanced Anti-Fraud and Intrusion Detection System) — это полностью распределенная СОВ. Система включает ряд агентов, которые для выявления вторжений используют характеристики атак, заданные вручную. Агенты – это программные модули с четко описанными признаками атак, для обнаружения которых они предназначены,

написанные на алгоритмическом языке общего назначения. Отсюда следует, что подобная организация трудно расширяемая и не подходит для обнаружения неизвестных атак.

Агенты могут применять фильтры для аккумуляции данных о поведении объектов.

В своей работе система использует современные методы машинного обучения и анализа данных, которые позволяют ей анализировать большие объемы данных и выявлять аномалии в поведении пользователей и устройств в сети. Она также использует технологии искусственного интеллекта для автоматического обнаружения новых угроз и атак.

AAFID имеет модульную структуру, которая позволяет ей работать с различными типами устройств и операционных систем. Она может быть настроена для работы с любыми типами данных и протоколов связи.

СОВ AAFID имеет широкий спектр функций, включая мониторинг сетевой активности, обнаружение вторжений, предотвращение атак, реагирование на инциденты и генерацию отчетов. Она также может интегрироваться с другими системами безопасности и управления рисками.

В целом, система AAFID является одной из самых передовых систем обнаружения вторжений, которая обеспечивает высокий уровень защиты компьютерных систем от кибератак.

В работе системы обнаружения вторжений ASAX применяется язык описания сценариев атак, эквивалентный по описательной мощности алгоритмическому языку C [2].

NetSTAT (Network Statistics) — это утилита командной строки в операционных системах Windows и Unix, которая позволяет отображать информацию о сетевых соединениях, портах и протоколах. С помощью NetSTAT можно узнать, какие сетевые соединения установлены на компьютере, какие порты используются и какой статус имеет каждое соединение.

С помощью NetSTAT можно выполнить следующие задачи:

- отобразить список всех открытых сетевых соединений на компьютере, включая IP-адреса, порты и статусы соединений;
- отобразить список всех открытых портов на компьютере, включая номер порта, протокол и приложение, которое использует этот порт;
- отобразить статистику использования сетевых интерфейсов, такую как количество отправленных и полученных пакетов данных.

NetSTAT может быть полезен для диагностики сетевых проблем, таких как блокировки портов или неправильно настроенные сетевые соединения. Кроме того, NetSTAT может использоваться для обнаружения вредоносных программ, которые могут использовать открытые порты для передачи данных или получения удаленного доступа к компьютеру. [3].

Система Prelude работает с базой сигнатур известных сетевых атак и с журналами. Для анализа сетевого трафика имеется возможность импорта системы Snort. Также система позволяет интегрировать набор специализированных модулей для детектирования таких атак, как сканирование портов, некорректные ARP-пакеты.

Система обнаружения вторжений SHADOW состоит из двух основных типов компонентов – сенсоров сетевого трафика и анализаторов. СОВ использует язык Perl для описания различных фильтров. В анализаторах системы хранится база знаний разработчиков системы о том, какие пакеты могут свидетельствовать о наличии атаки.

Одной из самых популярных систем обнаружения вторжений является утилита Snort. Snort — это бесплатная и открытая СОВ, которая используется для мониторинга сетевого

трафика и обнаружения потенциальных угроз безопасности. Она может работать на различных операционных системах, включая Windows, Linux и macOS.

С помощью Snort можно настраивать правила, определяющие типы атак, которые нужно обнаруживать. Эти правила могут быть созданы самостоятельно или загружены из общедоступных баз данных, таких как OpenAppID и Emerging Threats.

Snort может работать в режиме обнаружения вторжений (IDS) и в режиме предотвращения вторжений (IPS), что позволяет не только обнаруживать угрозы, но и блокировать их.

Кроме того, Snort имеет множество дополнительных модулей и расширений, которые позволяют расширить его функциональность, такие как Snorby, Barnyard2 и PuledPork.

Snort является одним из самых популярных инструментов IDS в мире и широко используется в крупных организациях и правительственных учреждениях для защиты своих сетей.

В работе [5] было впервые предложено использовать деревья решений вместо обычного модуля обнаружения в системе Snort. Эксперименты были проведены на устаревшем датасете DARPA [6]. В данном исследовании авторы смогли доказать, что использование деревьев решений дает возможность увеличить скорости обработки сетевых пакетов более чем на 40%.

Другими широко применяемыми подходами машинного обучения являются алгоритмы кластеризации и регрессии.

В исследовании [7] автор анализирует вопросы, связанные с эффективностью применения систем машинного обучения для задач обнаружения атак «нулевого дня». Автор высказал предположение, что сочетание методов классификации и кластеризации способно привести к лучшим результатам и защитит от ложноположительных срабатываний.

В 2009 году авторы исследования [8] предложили модель нейронной сети с прямой связью для создания СОВ, которая для обучения использует алгоритм обратного распространения ошибки. Авторы также провели тестирование на датасете DARPA KDD'98. По результатам тестирования сеть имела точность 76% на тестовом наборе данных, состоящем из 100 экземпляров.

В исследовании [9] авторы проверили потенциальную возможность применения глубокой нейронной сети в качестве классификатора различных типов атак. Для этой задачи многослойная нейронная сеть прямой связи была обучена с использованием набора данных KDD. В исследовании сообщается о точности обучения составила 99%.

В работе [10] построили классификатор на основе модели глубокой нейронной сети для системы обнаружения вторжений в среде SDN и обучили модель с помощью набора данных NSL-KDD. Исследователи ограничили признаковое пространство до 6 признаков. Результаты показали, что нейронные сети позволяют получить приемлемую скорость обнаружения вторжений только с использованием ограниченного числа признаков.

Выводы

В данной статье представлен обзор обобщенной архитектуры средств обнаружения вторжений, из которого видно, что ключевым элементом СОВ являются анализаторы, которые выполняют роль классификаторов входных данных. Именно анализаторы принимают решение об отнесении поданной на вход информации к какому-либо классу.

Стоит отметить, что СОВ не являются идеальным решением для защиты от всех видов атак. Некоторые виды атак могут обойти СОВ, например, если они используют шифрование или маскировку. Кроме того, системы обнаружения вторжений могут давать ложные срабатывания, что может приводить к перегрузке системы уведомлениями о ложных атаках.

Для максимальной эффективности, СОВ должны быть использованы в сочетании с другими средствами защиты, такими как брандмауэры, антивирусное программное обеспечение и системы аутентификации. Это позволяет создать комплексную систему защиты, которая будет максимально эффективна против различных типов атак.

В целом, IDS-системы являются неотъемлемой частью безопасности компьютерных систем и сетей. Они позволяют быстро обнаруживать и реагировать на атаки, что позволяет минимизировать возможный ущерб и сохранить целостность системы. Поэтому, при разработке системы безопасности, следует уделить особое внимание выбору и настройке СОВ.

Проведенный анализ нескольких распространенных систем обнаружения вторжений с открытым исходным кодом показал, что на сегодняшний день нет открытой и общедоступной СОВ, которая могла бы в режиме реального времени адаптироваться к неизвестным атакам. Наиболее распространенные методы обнаружения вторжений способны обнаружить неизвестные атаки лишь после явного указания их описания в базе знаний системы. Еще одним недостатком рассмотренных систем является необходимость в их постоянной поддержке.

На основании проведенного обзора можно сделать вывод, что наиболее перспективными в сфере обнаружения вторжений являются методы машинного и глубокого обучения, а разработка системы обнаружения вторжений в компьютерную сеть, способной обнаруживать неизвестные ранее аномалии, является актуальной и востребованной задачей.

Список литературы

1. ИТ.СОВ.У5.ПЗ. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты“ (утв. ФСТЭК России 06.03.2012).
2. Mounji A. “Languages and Tools for Rule-Based Distributed Intrusion Detection“ / A. Mounji // Computer Science - 1997.
3. Khraisat A. “Survey of Intrusion Detection Systems: tTechniques, Datasets and Challenges“ / A. Khraisat, I. Gondal, P. Vamplew // Cybersecurity – 2019.
4. Zhang, “Research on IDS Snort Based on Classic Clustering Algorithm“ / Zhang, Gongguo, Li // International Conference on Urban Engineering and Management Science (ICUEMS) – 2020 – PP. 673-676.
5. Kruegel C. “Using Decision Trees to Improve Signature-Based Intrusion Detection“ / C. Kruegel, T. Toth // Recent Advances in Intrusion Detection - 2003 -PP. 173–191.
6. “DARPA Intrusion Detection Data Sets“ (Интернет ресурс, дата обращения 26.04.2022) - [<https://www.ll.mit.edu/ideval/data>].
7. Miller M. “Are we protected yet? developing a machine learning detection system to combat zero-day malware attacks” / M. Miller // IEEE International Conference on Big Data (Big Data) - 2018.
8. Shun J. “Network Intrusion Detection System Using Neural Networks” / J. Shun, A. Malki // Fourth Int. Conf. Nat. Comput. - 2009 - vol. 5 - PP. 242–246.

9. Roy S. “A deep learning based artificial neural network approach for intrusion detection,” / S. Roy, A. Mallik, R. Gulati // Communications in Computer and Information Science - 2017.
10. Tang T. “Deep learning approach for Network Intrusion Detection in Software Defined Networking” / T. Tang, L. Mhamdi, D. McLernon // International Conference on Wireless Networks and Mobile Communications, WINCOM – 2016

References

1. IT.SOV.U5.PZ. Methodological document of the FSTEC of Russia. Protection profile of intrusion detection systems at the node level of the fifth protection class” (approved by the FSTEC of Russia on 03/06/2012).
 2. Mounji A. “Languages and Tools for Rule-Based Distributed Intrusion Detection“ / A. Mounji // Computer Science - 1997.
 3. Khraisat A. “Survey of Intrusion Detection Systems: tTechniques, Datasets and Challenges“ / A. Khraisat, I. Gondal, P. Vamplew // Cybersecurity - 2019.
 4. Zhang, “Research on IDS Snort Based on Classic Clustering Algorithm“ / Zhang, Gongguo, Li // International Conference on Urban Engineering and Management Science (ICUEMS) – 2020 – PP. 673-676.
 5. Kruegel C. “Using Decision Trees to Improve Signature-Based Intrusion Detection“ / C. Kruegel, T. Toth // Recent Advances in Intrusion Detection - 2003 - PP. 173–191.
 6. “DARPA Intrusion Detection Data Sets“ (Internet resource, accessed 26.04.2022) - [<https://www.ll.mit.edu/ideval/data>].
 7. Miller M. Are we protected yet? developing a machine learning detection system to combat zero-day malware attacks” / M. Miller // IEEE International Conference on Big Data (Big Data) - 2018.
 8. Shun J. “Network Intrusion Detection System Using Neural Networks” / J. Shun, A. Malki // Fourth Int. Conf. Nat. Comput. - 2009 - vol. 5-PP. 242–246.
 9. Roy S. “A deep learning based artificial neural network approach for intrusion detection,” / S. Roy, A. Mallik, R. Gulati // Communications in Computer and Information Science - 2017.
 10. Tang T. “Deep learning approach for Network Intrusion Detection in Software Defined Networking” / T. Tang, L. Mhamdi, D. McLernon // International Conference on Wireless Networks and Mobile Communications, WINCOM – 2016
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 65.011.56

АНАЛИЗ БОЛЬШИХ ДАННЫХ НА ПРОМЫШЛЕННОМ ПРЕДПРИЯТИИ

Дементьев С.Ю., ¹Роза М.П.

ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», Красноярск, Россия (660037, Красноярский край, город Красноярск, проспект имени газеты «Красноярский рабочий», д. 3), e-mail: ¹super.wark@mail.ru

Анализ больших данных становится все более важным в современном промышленном секторе, поскольку предприятия стремятся использовать возможности больших объемов данных, генерируемых из различных источников. В этой статье рассматривается применение анализа больших данных на промышленном предприятии и выделяются его потенциальные преимущества. В исследовании рассматриваются проблемы, с которыми пришлось столкнуться, используемые методологии и результаты, достигнутые благодаря анализу больших данных. Используя передовые методы аналитики, промышленные предприятия могут принимать решения на основе данных, оптимизировать операции и повышать общую эффективность. Полученные результаты демонстрируют преобразующий потенциал анализа больших данных и его способность стимулировать инновации и конкурентоспособность в промышленном секторе.

Ключевые слова: Анализ больших данных, промышленное предприятие, решения на основе данных, оптимизация, эффективность.

BIG DATA ANALYSIS IN AN INDUSTRIAL ENTERPRISE

Dementev S.Y., ¹Roza M.P.

Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia (660037, Krasnoyarsk Krai, Krasnoyarsk city, prospect named after the newspaper "Krasnoyarsk worker", 3), e-mail: ¹super.wark@mail.ru

Big data analysis has become increasingly vital in the modern industrial landscape, as enterprises seek to harness the power of large volumes of data generated from various sources. This article explores the application of big data analysis in an industrial enterprise and highlights its potential benefits. The study investigates the challenges faced, methodologies employed, and results achieved through big data analysis. By leveraging advanced analytics techniques, industrial enterprises can make data-driven decisions, optimize operations, and improve overall efficiency. The findings demonstrate the transformative potential of big data analysis and its ability to drive innovation and competitiveness in the industrial sector.

Keywords: Big data analysis, industrial enterprise, data-driven decisions, optimization, efficiency.

In today's digital age, industrial enterprises generate vast amounts of data from various sources, such as sensors, machines, supply chains, and customer interactions. This explosion of data offers unprecedented opportunities for enterprises to gain valuable insights and improve their operations. Big data analysis, which involves extracting actionable information from large and complex datasets, has emerged as a powerful tool for industrial enterprises. By leveraging big data analytics, enterprises can optimize processes, enhance productivity, and unlock new avenues for

growth. This article delves into the application of big data analysis in an industrial enterprise, examining its benefits, methodologies, and outcomes.

One of the important aspects of big data analysis in industrial enterprises is to increase the efficiency of the decision-making process. Big data analysis enables industrial enterprises to make data-driven decisions by providing comprehensive insights into operational processes, market trends, and customer preferences. This data-driven decision-making approach helps in identifying opportunities, mitigating risks, and improving overall business performance [1].

The next aspect of big data analysis in industrial enterprises is Optimization of Operations. By analyzing large datasets, industrial enterprises can identify bottlenecks, inefficiencies, and areas for improvement in their operations. Through advanced analytics techniques, such as predictive modeling and machine learning algorithms, enterprises can optimize production processes, reduce downtime, and enhance resource utilization.

The end aspect of big data analysis in industrial enterprises is Improved Supply Chain Management. Big data analysis facilitates real-time monitoring of the supply chain, enabling enterprises to identify potential disruptions, forecast demand, and optimize inventory levels. By integrating data from suppliers, manufacturers, and distributors, enterprises can achieve greater supply chain visibility, streamline logistics, and improve customer satisfaction [2].

The Methodologies for Big Data Analysis in Industrial Enterprises in industrial enterprises consists of 4 stages. These steps are Data Collection and Integration, Data Preprocessing and Cleansing, Exploratory Data Analysis and Advanced Analytics Techniques. Let's look at these steps in more detail [2]:

1. Data Collection and Integration. Industrial enterprises need to collect data from various sources, including sensors, production systems, and external databases. This data is then integrated into a centralized repository for further analysis. Advanced data integration techniques, such as data virtualization or data lakes, allow enterprises to merge heterogeneous datasets and eliminate data silos.

2. Data Preprocessing and Cleansing. Before analysis, raw data often requires preprocessing and cleansing to remove errors, outliers, and irrelevant information. Techniques like data normalization, outlier detection, and missing data imputation ensure the quality and integrity of the dataset.

3. Exploratory Data Analysis. Exploratory data analysis involves performing initial investigations to uncover patterns, relationships, and anomalies in the data. Visualizations, statistical summaries, and data profiling techniques aid in understanding the characteristics of the dataset and guide further analysis.

4. Advanced Analytics Techniques. Industrial enterprises employ various advanced analytics techniques, such as machine learning, predictive modeling, and optimization algorithms, to extract insights from big data. These techniques enable enterprises to predict equipment failures, optimize maintenance schedules, and forecast demand more accurately.

Several technologies are associated with big data analysis in an industrial enterprise. Here are some of the key technologies commonly used [3]:

1. Distributed File Systems. Distributed file systems, such as Apache Hadoop HDFS (Hadoop Distributed File System) and Apache HBase, are fundamental for storing and managing large volumes of data in a distributed computing environment. These file systems allow enterprises to scale storage capacity and handle massive datasets across clusters of commodity hardware.

2. **Data Processing Frameworks.** Data processing frameworks provide the computational power needed to analyze and extract insights from big data. Apache Hadoop, Apache Spark, and Apache Flink are widely used frameworks that offer distributed processing capabilities. These frameworks allow enterprises to parallelize computations and execute complex data analysis tasks on large datasets efficiently.

3. **Data Integration and ETL Tools.** Data integration and Extract, Transform, Load (ETL) tools are essential for ingesting, cleansing, and transforming data from various sources before analysis. Tools like Apache Nifi, Talend, and Informatica enable enterprises to extract data from different systems, integrate it into a unified format, and prepare it for analysis.

4. **Distributed Databases.** Distributed databases, such as Apache Cassandra, Apache HBase, and Amazon DynamoDB, are designed to handle large-scale data storage and retrieval in a distributed environment. These databases offer high scalability, fault tolerance, and low-latency access, enabling efficient storage and retrieval of big data for analysis.

5. **Machine Learning and Predictive Analytics.** Machine learning algorithms and predictive analytics techniques play a crucial role in extracting insights and making predictions from big data. Technologies such as Python's scikit-learn, TensorFlow, and Apache Mahout provide libraries and frameworks for implementing machine learning models and predictive analytics algorithms on large datasets.

6. **Data Visualization Tools.** Data visualization tools help in presenting complex data analysis results in a visually appealing and understandable manner. Tools like Tableau, Power BI, and D3.js allow enterprises to create interactive charts, graphs, and dashboards, enabling stakeholders to explore and interpret big data analysis outcomes effectively.

7. **Real-time Stream Processing.** Real-time stream processing technologies, such as Apache Kafka and Apache Flink, enable enterprises to process and analyze streaming data in real-time. These technologies support the continuous ingestion, processing, and analysis of data as it flows, allowing for timely insights and quick decision-making.

8. **Cloud Computing.** Cloud computing platforms, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), provide scalable and on-demand computing resources for big data analysis. These platforms offer various managed services, such as Amazon EMR, Azure HDInsight, and Google Cloud Dataproc, which simplify the deployment and management of big data analytics infrastructure.

These technologies, along with others, form the foundation for performing big data analysis in an industrial enterprise. The selection and integration of these technologies depend on the specific requirements, scale, and complexity of the enterprise's big data analytics needs.

There are several real cases of big data analysis being successfully implemented in industrial enterprises. Here are a few examples [4]:

1. **Predictive Maintenance in Manufacturing.** Industrial enterprises have started leveraging big data analytics to implement predictive maintenance strategies. By collecting and analyzing data from sensors embedded in machinery and equipment, enterprises can identify patterns and anomalies that indicate potential failures. This allows them to schedule maintenance proactively, reducing downtime, optimizing maintenance costs, and extending the lifespan of assets. For example, General Electric (GE) uses big data analytics to monitor the performance of jet engines in real-time, predicting maintenance needs and optimizing aircraft operations.

2. **Quality Control and Defect Detection.** Big data analysis helps industrial enterprises improve quality control processes and detect defects in products. By analyzing data from various stages of the manufacturing process, including sensors, machine logs, and inspection records, enterprises can identify deviations from normal operating conditions and detect potential quality issues. This enables them to take corrective actions promptly, reducing waste and improving overall product quality. For instance, a semiconductor manufacturer might analyze sensor data to detect anomalies during the production of microchips, ensuring high-quality output.

3. **Supply Chain Optimization.** Big data analysis plays a crucial role in optimizing supply chain operations. By integrating data from suppliers, manufacturers, logistics providers, and customers, enterprises can gain real-time visibility into their supply chain. This enables them to identify bottlenecks, optimize inventory levels, streamline logistics, and improve demand forecasting. Amazon, for instance, uses big data analytics to analyze customer order patterns, optimize warehouse operations, and facilitate faster deliveries.

4. **Energy Management and Optimization.** Industrial enterprises consume significant amounts of energy in their operations. Big data analysis can help optimize energy usage, reduce costs, and minimize environmental impact. By analyzing energy consumption data from sensors and meters, enterprises can identify energy inefficiencies, implement energy-saving measures, and optimize resource utilization. For example, Google employs big data analytics to optimize the cooling systems in its data centers, resulting in substantial energy savings.

5. **Customer Analytics and Personalization.** Big data analysis enables industrial enterprises to gain insights into customer behavior, preferences, and buying patterns. By analyzing customer data from multiple touchpoints, such as sales transactions, social media interactions, and customer feedback, enterprises can personalize their offerings, tailor marketing campaigns, and improve customer satisfaction. For instance, automotive companies analyze customer data to understand preferences for specific features, enabling them to design and market vehicles that meet customer expectations.

These examples demonstrate the diverse applications of big data analysis in industrial enterprises, showcasing its potential to drive operational efficiency, enhance decision-making, and improve overall business performance. As technology continues to advance, we can expect further innovation and expansion of big data analytics in the industrial sector.

While big data analysis offers numerous benefits, it is essential to consider potential negative effects and challenges associated with its use. One example of a negative effect of big data analysis is the concern related to privacy and data security.

Big data analysis involves the collection, storage, and analysis of vast amounts of personal and sensitive information. As more data is gathered and analyzed, there is an increased risk of privacy breaches and data security incidents. If not handled properly, the misuse or unauthorized access to sensitive data can result in privacy violations, identity theft, or other forms of cybercrime. Moreover, the aggregation of diverse datasets can lead to unintended identification or re-identification of individuals, potentially compromising their privacy rights [5].

For instance, consider a scenario where an industrial enterprise collects and analyzes data from various sources, including employee records, customer transactions, and public data. If the enterprise fails to implement robust security measures, it becomes vulnerable to data breaches, exposing personal information to unauthorized individuals or malicious actors. Such incidents can erode customer trust, damage the reputation of the enterprise, and lead to legal consequences [6].

To mitigate this negative effect, organizations must prioritize data privacy and security. They should implement robust security protocols, employ encryption techniques, and comply with relevant data protection regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Additionally, enterprises must be transparent about their data collection and usage practices, obtain informed consent from individuals, and establish clear policies for data handling and retention [7].

It is important to recognize that while big data analysis offers tremendous potential, organizations must strike a balance between extracting valuable insights and protecting individual privacy and data security. Responsible data governance practices and ethical considerations are essential to address this negative effect and maintain public trust in the use of big data analysis.

Results of Big Data Analysis in Industrial Enterprises include Operational Efficiency. Through big data analysis, industrial enterprises can optimize their production processes, reduce energy consumption, and minimize waste. This optimization leads to improved operational efficiency, increased productivity, and cost savings. The next result is Predictive Maintenance. By leveraging big data analytics, enterprises can implement predictive maintenance strategies. By analyzing sensor data, historical maintenance records, and external factors, enterprises can predict equipment failures, schedule maintenance proactively, and avoid costly unplanned downtime. One of the advantages is Customer Insights and Personalization. Big data analysis helps industrial enterprises gain a deeper understanding of customer behavior, preferences, and buying patterns. By analyzing customer data, such as purchase history, feedback, and social media interactions, enterprises can personalize their offerings, target specific customer segments, and enhance customer satisfaction. Last but not least, the advantage is Risk Mitigation. Big data analysis enables industrial enterprises to identify and mitigate potential risks. By analyzing historical data and external factors, enterprises can develop risk models, detect anomalies, and implement proactive measures to prevent accidents, quality issues, or supply chain disruptions.

Big data analysis holds immense potential for industrial enterprises, offering valuable insights, optimized operations, and improved decision-making capabilities. By leveraging advanced analytics techniques, industrial enterprises can unlock the power of big data and gain a competitive edge in the market. However, the implementation of big data analysis requires careful consideration of data privacy, security, and infrastructure challenges. As technology advances and more sophisticated analytical tools become available, industrial enterprises must adapt and embrace the transformative potential of big data analysis.

Список литературы

1. Chen, M. Big data: A survey / M. Chen, S. Mao, Y. Liu // *Mobile Networks and Applications*. – 2014. – No. 19(2). – pp. 171-209
2. Davenport, T. H. Big data at work: Dispelling the myths, uncovering the opportunities. / T. H. Davenport. – Harvard Business Review Press, 2014. – 121 p.
3. McAfee, A., Big data: The management revolution / A. McAfee, E. Brynjolfsson // *Harvard Business Review*. – 2012. – No. 90(10). – pp. 60-68.
4. Provost, F. Data science for business: What you need to know about data mining and data-analytic thinking / F. Provost, T. Fawcett. - Sebastopol: O'Reilly Media, 2013. - 409 p.
5. Tan, P. N. Introduction to data mining / P. N. Tan, M. Steinbach, V. Kumar. – Pearson, 2018. – 173 p.

6. Dement'ev, S. Ju. Metody avtomaticheskoy gruppirovki dlja povyshenija jekonomicheskoy jeffektivnosti v industrii 4.0 / S. Ju. Dement'ev, M. P. Roza // Jekonomika i predprinimatel'stvo. – 2022. – № 10(147). – pp. 1390-1393. – DOI 10.34925/EIP.2022.147.10.278. – EDN YDFFDH.
7. Wu, X. Data mining with big data / X. Zhu, G. Q. Wu, W. Ding // IEEE Transactions on Knowledge and Data Engineering. – 2014. – No. 26(1). – pp. 97-107

References

1. Chen, M. Big data: A survey / M. Chen, S. Mao, Y. Liu // Mobile Networks and Applications. – 2014. – No. 19(2). – pp. 171-209
 2. Davenport, T. H. Big data at work: Dispelling the myths, uncovering the opportunities. / T. H. Davenport. – Harvard Business Review Press, 2014. – 121 p.
 3. McAfee, A., Big data: The management revolution / A. McAfee, E. Brynjolfsson // Harvard Business Review. – 2012. – No. 90(10). – pp. 60-68.
 4. Provost, F. Data science for business: What you need to know about data mining and data-analytic thinking / F. Provost, T. Fawcett. - Sebastopol: O'Reilly Media, 2013. - 409 p.
 5. Tan, P. N. Introduction to data mining / P. N. Tan, M. Steinbach, V. Kumar. – Pearson, 2018. – 173 p.
 6. Dement'ev, S. Ju. Metody avtomaticheskoy gruppirovki dlja povyshenija jekonomicheskoy jeffektivnosti v industrii 4.0 / S. Ju. Dement'ev, M. P. Roza // Jekonomika i predprinimatel'stvo. – 2022. – № 10(147). – S. 1390-1393. – DOI 10.34925/EIP.2022.147.10.278. – EDN YDFFDH.
 7. Wu, X. Data mining with big data / X. Zhu, G. Q. Wu, W. Ding // IEEE Transactions on Knowledge and Data Engineering. – 2014. – No. 26(1). – pp. 97-107.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 65.011.56

КИБЕРПРЕСТУПНОСТЬ XXI ВЕКА И ЕЁ ВЛИЯНИЕ НА СОВРЕМЕННОЕ ОБЩЕСТВО

Сулейменова Р.Д., ¹Устюжанина С.П.

ФГБОУ ВО «Оренбургский государственный аграрный университет», Оренбург, Россия, (460014, г. Оренбург, ул. Челюскинцев, 18), e-mail: ¹sofiausuzanina@gmail.com

В данной статье исследуется термин киберпреступности. Рассматриваются виды киберпреступлений в сети, причины роста киберпреступников. А также почему Россия имеет одно из лидирующих мест по росту интернет-преступлений. Нами рассмотрены основные незащищенные слои социума, подвергаемые влиянию хакеров. Выявлены различные виды хакеров и их средства и возможности хищения информации. В работе проведен анализ влияния преступлений на современное общество. Нами обосновано положение о том, что правоохранительные органы должны быть всегда на шаг впереди преступников, о том как люди встают на путь киберпреступлений, а так же должны быть предупреждены о целях их преступлений

Ключевые слова: Киберпреступления, компьютерная преступность, киборугрозы, информационная безопасность, всемирная интернет паутина, интрнет-преступления.

CYBERCRIME OF THE XXI CENTURY AND THEIR IMPACT ON MODERN SOCIETY

Suleimenova R.D., ¹Ustyuzhanina S.P.

FSBEI HE "Orenburg State Agrarian University", Orenburg, Russia, (460014, Orenburg, Chelyuskintsev str., 18), e-mail: ¹sofiausuzanina@gmail.com

This article explores the term cybercrime. The types of cybercrimes in the network, the reasons for the growth of cybercriminals are considered. And also why Russia has one of the leading places in the growth of Internet crimes. We have considered the main unprotected layers of society exposed to the influence of hackers. Various types of hackers and their means and possibilities of information theft have been identified. The paper analyzes the impact of crimes on modern society. We have substantiated the position that law enforcement agencies should always be one step ahead of criminals, about how people embark on the path of cybercrime, and should also be warned about the goals of their crimes.

Keywords: Cybercrime, computer crime, cyber threats, information security, the world wide web, internet crimes.

Развитие Всемирной интернет паутины привело к тому, что стерлись все возможные границы общения. Распространение информации на данный момент не представляет никаких трудностей - один клик и сообщение отправлено! Но вместе с положительным влиянием интернета, всегда бок о бок шло и отрицательное.

В Доктрине информационной безопасности РФ информационная безопасность РФ определяется как состояние защищенности еенациональных интересов в информационной сфере[2, с. 210].

Киберпреступность плотно вжилась в современных реалиях. С каждым годом число киберпреступлений растёт и вместе с тем растёт и число пострадавших.

Если просмотреть международную статистику по интернет-преступлениям, то можно сделать вывод, что Россия занимает лидирующее место. Этому могут служить следующие предпосылки:

- трудность расследования преступлений в сфере IT;
- слабая законодательная база в сфере информационной безопасности;
- отсутствие монолитной борьбы с киберпреступлениями.

В 2022 году было совершено порядка 500 тысяч киберпреступлений. Такие цифры назвал представитель Следственного комитета Тамирлан Салихов.

Компьютерная преступность – представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом компьютерная информация является предметом или средством совершения преступления[3, с. 265].

Киберпреступления в России имеют различные формы и проявления. Одним из наиболее распространенных видов киберпреступлений является хакерство. Хакеры могут получать несанкционированный доступ к компьютерам и сетям, кражу личных данных, финансовых средств и другой конфиденциальной информации. Также киберпреступники могут использовать вирусы и другие вредоносные программы для атак на компьютеры и сети.

К компьютерным преступлениям в широком смысле мы будем относить:

- доведение до самоубийства через сеть «Интернет»;
- незаконный сбыт оружия через сеть «Интернет»;
- незаконный сбыт наркотиков через сеть «Интернет»;
- распространение экстремистской и террористической информации через сеть «Интернет»;
- незаконный сбыт контрафактной продукции через сеть «Интернет»;
- правонарушения с использованием компьютерной информации и сети «Интернет» (киберпреступления) [1, с. 60].

Еще одним видом киберпреступлений является фишинг. Фишинг - это метод мошенничества, при котором злоумышленники отправляют электронные письма, которые выглядят как официальные сообщения от банков, сервисов и других организаций. Пользователи, получившие такие письма, могут быть вынуждены вводить свои личные данные и банковские реквизиты, что может привести к краже денег и личных данных. Также киберпреступники могут использовать социальные сети и мессенджеры для распространения фейковых новостей и информации. Это может привести к массовой панике и распространению ложной информации.

Утечка личных данных может произойти с любого незащищенного телефона или компьютера, однако злоумышленники охотятся, как правило, не за личной, а за платежной информацией или паролями» [6, с.34].

Рассмотрим компьютерные преступления в узком смысле. В узком смысле - это те преступления, которые предусмотрены УК РФ, а именно:

- неправомерный доступ к информации (ст. 272 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ);

- создание, распространение вредоносных программ (ст. 273 УК РФ);
- неправомерное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ) [4, с. 126].

Одной из основных причин роста киберпреступности в России является недостаток законодательства в области кибербезопасности. Существующие законы не отвечают на современные вызовы и не позволяют эффективно бороться с киберугрозами. Необходимо улучшить законодательство, чтобы обеспечить более жесткое наказание для киберпреступников и защитить права жертв киберпреступлений.

Еще одна причина роста компьютерных преступлений - это нехватка специалистов. С февраля 2022 года большинство специалистов начали уезжать работать за пределы РФ, объясняя это тем, что там зарплата больше, или переходя на «тёмную» сторону, т. е. становились хакерами [5, с. 210].

Киберпреступность является одной из наиболее актуальных проблем в современном мире. Каждый год количество киберпреступлений растет, и становится все более сложным для правоохранительных органов бороться с этим явлением. Но как люди становятся киберпреступниками?

Во-первых, многие киберпреступники начинают свой путь с маленьких нарушений, таких как незаконное скачивание программного обеспечения или музыки. Эти нарушения могут привести к более серьезным преступлениям, таким как взломы и кражи личных данных.

Во-вторых, некоторые люди становятся киберпреступниками из-за финансовых проблем. Они видят в киберпреступности способ заработать деньги, например, продавая украденные данные или запрашивая выкуп после взлом.

В-третьих, некоторые люди становятся киберпреступниками из-за желания получить доступ к запрещенной информации. Например, хакеры могут взламывать государственные сайты, чтобы получить доступ к секретной информации.

В-четвертых, некоторые люди становятся киберпреступниками из-за желания получить известность. Они могут взламывать сайты и размещать на них свои сообщения или даже создавать вирусы, чтобы привлечь внимание к своим способностям.

Наконец, некоторые люди становятся киберпреступниками просто потому, что им нравится чувствовать себя властными и контролировать других людей. Они могут взламывать компьютеры и устройства других людей, чтобы получить доступ к их личной информации или просто для того, чтобы навредить им.

Однако, не только законодательство может помочь в борьбе с киберпреступлениями. Важную роль играет повышение осведомленности населения о киберугрозах. Люди должны знать, какие меры безопасности необходимо принимать при работе в Интернете, какие угрозы могут возникнуть и как им можно предотвратить. Поэтому, государство должно проводить информационные кампании и обучать население основам информационной безопасности.

Также, необходимо развивать технические средства защиты информации. Новые технологии могут помочь в борьбе с киберпреступлениями, но для этого необходимо инвестировать в разработку и внедрение новых систем защиты. Компании и государственные организации должны использовать современные технологии защиты информации, чтобы предотвратить утечки данных и другие киберугрозы.

В целом, борьба с киберпреступлениями в России требует комплексного подхода. Необходимо улучшать законодательство, повышать осведомленность населения о

киберугрозах и развивать технические средства защиты информации. Только таким образом можно обеспечить безопасность в Интернете и защитить интересы частных лиц.

В настоящее время киберпреступности стали одной из самых актуальных проблем в России. Рост количества кибератак и киберугроз угрожает безопасности государства, бизнесу и частным лицам. Одной из основных причин роста киберпреступности является недостаток законодательства в области кибербезопасности. Необходимо улучшить законодательство, повысить осведомленность населения о киберугрозах и развивать технические средства защиты информации. Только комплексный подход может обеспечить безопасность в Интернете и защитить интересы государства и частных лиц.

Список литературы

1. Барышев В.А. Сулейменова Р.Д. Кибермошенничество как угроза населению России: Интернаука. 2022. №20-1 (243). С. 60 – 62.
2. Драпезо, Р. Г. Информационные технологии в юридической деятельности: учебное пособие / Р. Г. Драпезо, Ю. Г. Волгин. — Кемерово : КемГУ, 2020. — ISBN 978-5-8353-2615-0. — Текст : электронный // Лань : электронно-библиотечная система — URL: <https://e.lanbook.com/book/156105> (дата обращения: 06.02.2023).
3. Ильницкий, А. А. Компьютерная преступность. Основные проблемы раскрываемости киберпреступлений / А. А. Ильницкий, Д. А. Шичкин. — Текст : непосредственный // Молодой ученый. — 2022. — № 19 (414). — С. 265-267.
4. Лагутин, П. Д. Киберпреступность как актуальная угроза обществу / П. Д. Лагутин, Т. А. Миханова. — Текст: непосредственный // Молодой ученый. — 2018. — № 42 (228). — С. 108-109.
5. Ломакин Д.Н., Козлов Д.А. Компьютерная криминалистика «Форензика» и киберпреступления в России в период пандемии: Молодой ученый. 2022. №17 (412). С. 210 – 212.
6. Панин О. Н., Сулейменова Р. Д. Угрозы безопасности цифрового профиля гражданина РФ: Молодой ученый. 2022. № 16 (411). С.34 – 35.

References

1. Baryshev V.A. Suleimenova R.D. Cyber fraud as a threat to the population of Russia: Internauka. 2022. No.20-1 (243). pp. 60 – 62.
 2. Drapezo, R. G. Information technologies in legal activity: textbook / R. G. Drapezo, Yu. G. Volgin. — Kemerovo : KemSU, 2020. — ISBN 978-5-8353-2615-0. — Text : electronic // Lan : electronic library system — URL: <https://e.lanbook.com/book/156105> (accessed: 06.02.2023).
 3. Ilnitsky, A. A. Computer crime. The main problems of detection of cybercrimes / A. A. Ilnitsky, D. A. Shichkin. — Text : direct // Young scientist. — 2022. — № 19 (414). — pp. 265-267.
 4. Lagutin, P. D. Cybercrime as an actual threat to society / P. D. Lagutin, T. A. Mikhanova. — Text: direct // Young scientist. — 2018. — № 42 (228). — pp. 108-109.
 5. Lomakin D.N., Kozlov D.A. Computer forensics "Forensics" and cybercrime in Russia during the pandemic: A young scientist. 2022. No.17 (412). pp. 210-212.
 6. Panin O. N., Suleimenova R. D. Threats to the security of the digital profile of a citizen of the Russian Federation: A young scientist. 2022. No. 16 (411). pp.34-35.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004

АНАЛИЗ СУЩЕСТВУЮЩИХ ИНСТРУМЕНТОВ КОНФИГУРАЦИИ И ВЕРИФИКАЦИИ ФАЙЛОВ SCL ЦПС

¹Сидоров В.А., Алиусманов Г.Э., Антонов Р.Б., Климчук И.В., Медведев М.С.
ФГБОУ ВО "Национальный исследовательский университет "МЭИ", Москва, Россия (111250,
г.Москва, Красноказарменная ул., 14, стр.1), e-mail: ¹SidorovVaAl@yandex.ru

В данном исследовании произведен обзор существующих отечественных и зарубежных программных комплексов для конфигурации и верификации электронной документации на языке SCL, разрабатываемой при проектировании цифровых подстанций.

Ключевые слова: Цифровая подстанция (ЦПС), МЭК 61850, интеллектуальное электронное устройство (ИЭУ), электронная документация (ЭД), Substation Configuration description Language (SCL).

ANALYSIS OF EXISTING TOOLS FOR CONFIGURATION AND VERIFICATION OF SCL FILES OF THE CPS

¹Sidorov V.A., Aliusmanov G.E., Antonov R.B., Klimchuk I.V., Medvedev M.S.
"National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya
st., 14, bild.1), e-mail: ¹ SidorovVaAl@yandex.ru

This study provides an overview of existing national and foreign software systems for the configuration and verification of electronic documentation in the SCL language developed in the design of digital substations.

Keywords: Digital substation (DS), IEC 61850, intelligent electronic device (IED), electronic documentation (ED), Substation Configuration description Language (SCL).

В соответствии с приоритетами, обозначенными Президентом Российской Федерации, и положениям утвержденной в 2017 году национальной программы «Цифровая экономика Российской Федерации» Минэнерго России при активном участии компаний ТЭК сформирован ведомственный проект «Цифровая энергетика». Проект направлен на преобразование энергетической инфраструктуры России и ее цифровизацию [1].

В рамках данного проекта предусмотрено также создание цифровых подстанций. Опыт разработки проектной документации РЗА ЦПС говорит о несовершенстве процесса работы с файлами формата SCL, предусмотренным стандартом МЭК 61850. Особенно часто встречаются проблемы, связанные с неправильной конфигурацией и отсутствием верификации файлов ЭД. Поэтому необходимо производить комплексную проверку файлов ЭД уже на фазе проектирования для предотвращения ошибок на последующих этапах жизни ЦПС, что в свое время ускорит процесс ввода подстанции в эксплуатацию.

Автоматическое выполнение требуемых проверок с помощью специализированных программ значительно ускоряет этот процесс и снижает вероятность ошибки, исключая человеческий фактор.

Оформление проектной документации предполагает разработку принципиальных и монтажных схем [2]. Часть современной проектной документации формируется с использованием файлов конфигурации SCL. Вся информация о применении цифровых технологий на подстанции должна быть интегрирована в соответствующие тома проектной документации (ПД) и комплекты рабочей документации (РД) [3].

Первичная схема энергообъекта, реализуемые на нем функции, конфигурации ИЭУ и информационного обмена между ними на цифровых подстанциях описывается на языке Substation Configuration description Language (SCL), созданном на основе расширенного языка разметки XML (eXtensible Markup Language), согласно МЭК 61850-6 [4]. Язык SCL был разработан для эффективного обмена информацией между устройствами ЦПС различных производителей и для формального описания этого обмена. Данный язык включает описание моделей терминалов и информацию о сетевых отношениях между устройствами, в том числе между терминалами и первичным оборудованием.

Стандарт МЭК определяет шесть типов конфигурационных файлов на языке SCL, создание которых производится на этапе проектирования:

- ICD (IED Capability Description) содержит описание всех логических устройств, логических узлов, объектов и атрибутов данных, входящих в состав описываемого физического устройства, а также описание возможностей осуществления коммуникаций;
- IID (Instantiated IED Description) содержит предварительно сконфигурированную информационную модель ИЭУ, а также предустановленные коммуникации;
- SSD (System Specification Description) содержит описание однолинейной схемы и функций подстанции, а также требуемые логические узлы;
- SCD (System Configuration Description) служит для описания конфигурации цифровой подстанции, описывает все коммуникации на ней;
- CID (Configured IED Description) содержит описание сконфигурированного ИЭУ;
- SED (System Exchange Description) содержит описания межсистемного обмена и описывает коммуникационные связи между отдельными системами, описанными в виде SCD-файлов.

Таким образом, XML-подобный язык SCL удобен при описании структурированной информации и в некоторой степени остается воспринимаемым человеком. Однако на практике файлы SCL содержат огромное количество кода, поэтому полное и точное понимание и анализ этих файлов человеком не представляется возможным.

Верификация является базовым и обязательным этапом проверки электронной проектной документации на языке SCL. Схема SCL как часть стандарта МЭК 61850 распространяется Международной Электротехнической Комиссией вместе со стандартом в виде набора файлов XSD, которые и используются для верификации. Сегодня существуют несколько версий схем SCL, которые могут быть использованы для ее верификации: схемы редакций 1, 2 и 2.1 стандарта МЭК 61850.

Иногда производители вносят изменения в набор файлов, чтобы произвести согласование со своими конфигурационными файлами, что в перспективе приводит к функциональной несовместимости [5]. К тому же вследствие отсутствия четкого нормативного регламента, большинство производителей оборудования программно-аппаратного комплекса ЦПС имеют собственное программное обеспечение для создания и конфигурации SCL-файлов, заточенное конкретно под свое оборудование. Это, в свою очередь, связано с тем, что некоторые пункты стандарта МЭК 61850 описаны лишь в общих чертах и оставлены на усмотрение производителя, поэтому конфигурация некоторых параметров разнится от производителя к производителю [6].

Таким образом, электронную документацию (ЭД) необходимо проверять на стадии проекта, ведь подобная ошибка выявится на стадии пуско-наладки и приведет к затягиванию работ. Проверка ЭД для человека была бы крайне трудоемким процессом, к тому же велика вероятность ошибок, поэтому необходимо использовать программные комплексы для автоматической проверки ЭД.

Для верификации проектной документации наилучшим решением будет использование независимого ПО. Такой подход позволит автоматически выявлять несоответствие документации стандарту МЭК и избежать несовместимости. Особенно актуально это в проектах, где используется ИЭУ различных производителей.

На данный момент существует ряд программных комплексов для осуществления проверок на разных стадиях жизненного цикла ЦПС, выполняющих спектр различных задач.

- Программный комплекс «SCADA Studio – Симулятор устройств»

SCADA Studio — это модульный программный продукт, представляющий собой единую платформу для параметрирования и наладки систем автоматизации на базе стандарта МЭК 61850.

Программный комплекс SCADA Studio включает в себя конфигуратор SCL/CIM, который предназначен для автоматизированного проектирования коммуникационных сетей и систем подстанций (в том числе цифровых) в соответствии со стандартом МЭК 61850-6 (SCL) [7].

- Программный комплекс «Test Suite Pro»

«Test Suite Pro» — это приложение Windows, содержащее инструменты, необходимые для тестирования и устранения неисправностей по стандарту МЭК 61850 в лаборатории, во время процесса ввода в эксплуатацию и текущего обслуживания на подстанции от компании Triangle MicroWorks.

Приложение «Test Suite Pro» предоставляет возможности тестирования новой реализации МЭК 61850, индивидуального тестирования и валидации ИЭУ, помощи в подготовке к формальному тестированию соответствия. Программа реализует следующие функции: автоматизированное тестирование с помощью упорядоченных тестов, визуализация потоков сигналов и их синхронизации в сети, быстрый поиск и устранение системных ошибок из-за устаревших конфигурационных файлов, а также проверка файлов SCL.

С помощью инструмента «SCL Verify» возможно проводить проверку совместимости файлов SCL, идентификацию отсутствующих/неверных параметров файла. В результате работы программы отображаются предупреждения или ошибки [8].

- Программный комплекс «ASE 61850 Suite»

«ASE 61850 Suite» — это программный комплекс на базе Windows, содержащий инструменты для тестирования файлов МЭК 61850, который обеспечивает эксплуатацию и обслуживание цифровых подстанций. Программный комплекс позволяет сканировать сеть или загружать в нее инженерные модели, идентифицировать, подключать и обнаруживать модели данных ИЭУ, а также отслеживать и контролировать их состояния.

«ASE 61850 Suite» поддерживает моделирование стандартных файлов SCL, одновременное моделирование нескольких ИЭУ, а также способен связывать различные интеллектуальные электронные устройства и их логические функции со спецификациями подстанции [9].

- Программный комплекс контроля жизненного цикла ЦПС «Теквел Парк»

«Теквел Парк» — это система управления жизненным циклом цифровой подстанции, оказывающая поддержку инженерам на разных стадиях реализации проекта: от проектирования до эксплуатации. «Теквел Парк» является уникальным инструментом для визуализации коммуникаций между устройствами различных фирм-производителей.

Система включает следующие функции: визуализация цифровых коммуникаций на основании файла электронной проектной документации SCD, автоматизированный анализ правильности разработки файлов электронной проектной документации SCD, версионирование файлов электронной проектной документации SCD, анализ соответствия конфигурации и трафика сети на соответствие файлу электронной проектной документации SCD. На стадии проектирования могут быть использованы следующие возможности «Теквел Парк»: хранение SCD-файлов, система контроля версий и организация коллективного доступа к ним, верификации SCL-файлов, проверка целостности конфигурации, анализ на предмет наличия ошибок и недостатков конфигурации, оценка возможности оптимизации итоговой конфигурации.

Несомненным плюсом данного комплекса является возможность развернуть его на большинстве модификаций промышленных серверов [10].

Таким образом, корректность электронной документации при проектировании может быть достигнута посредством применения программных комплексов для автоматической конфигурации ЭД и последующей ее верификации. На данный момент уже существуют отечественные программные комплексы, способные выполнять данные задачи. Это дает несомненное преимущество в проектировании ЦПС в России, так как работа программных комплексов основывается на отечественных стандартах МЭК 61850.

Однако пока не существует полноценного комплекса по автоматизированной проверке правильности проектных решений в части РЗА в соответствии с нормативными документами и техническим заданием. Существующие комплексы способны лишь осуществлять проверку в соответствии с представлениями конкретного тестирующего о правильной работе РЗА, что, в свою очередь, не исключает появления ошибок, связанных с человеческим фактором.

Список литературы

1. Ведомственный проект «ЦИФРОВАЯ ЭНЕРГЕТИКА» [Электронный ресурс]. Режим доступа: <https://minenergo.gov.ru/node/14559> (дата обращения: 05.05.2023).
2. ПАО «ФСК ЕЭС». СТО 56947007-29-240-10-248-2017. Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ, 2017.

3. ПАО "ФСК ЕЭС". STO 56947007-29.240.10.299-2020 "Цифровая подстанция. Методические указания по проектированию ЦПС, 2020.
4. ГОСТ Р МЭК 61850-6-2009. Язык описания конфигурации для связи между интеллектуальными электронными устройствами на электрических подстанциях, 2009.
5. «Проверка электронной проектной документации ЦПС: требования и практический опыт» [Электронный ресурс]. Режим доступа: <https://tekvel.com/ru/web/blog/post/scd-expertise/> (дата обращения: 06.05.2023).
6. Гурьев А.В., Зайцев Н.Ю. Опыт разработки проектной документации цифровой подстанции. Цифровая электротехника: проблемы и достижения. Чебоксары, 2018. С. 51-59.
7. «SCADA Studio» [Электронный ресурс]. Режим доступа: <http://www.epsa-spb.ru/scada-studio/> (дата обращения: 07.05.2023).
8. «61850 Test Suite Pro» [Электронный ресурс]. Режим доступа: <https://61850solutions.com/61850-test-suite-pro/> (дата обращения: 07.05.2023).
9. «Программный комплекс «ASE 61850 Suite» [Электронный ресурс]. Режим доступа: <https://www.ase-systems.com/products/ase61850-suite/> (дата обращения: 08.05.2023).
10. «Программный комплекс «Теквел Парк» [Электронный ресурс]. Режим доступа: <https://tekvel.com/ru/park/#:~:text=> (дата обращения: 08.05.2023)..

References

1. Departmental project "DIGITAL ENERGY" [Electronic resource]. Access mode: <https://minenergo.gov.ru/node/14559> (date of application: 05.05.2023).
 2. PJSC "FGKEES". STO 56947007-29-240-10-248-2017. Norms of technological design of AC substations with a higher voltage of 35-750 kV, 2017.
 3. PJSC "FGKEES". STO 56947007-29.240.10.299-2020 "Digital substation. Methodological guidelines for the design of the DS, 2020.
 4. GOST R IEC 61850-6-2009. Configuration description language for communication between intelligent electronic devices at electrical substations, 2009.
 5. "Verification of electronic project documentation of the DS: requirements and practical experience" [Electronic resource]. Access mode: <https://tekvel.com/ru/web/blog/post/scd-expertise/> (date of reference: 06.05.2023).
 6. Guryev A.V., Zaitsev N.Yu. Experience in developing design documentation for a digital substation. Digital electrical engineering: problems and achievements. Cheboksary, 2018. pp. 51-59.
 7. "SCADA Studio" [Electronic resource]. Access mode: <http://www.epsa-spb.ru/scada-studio/> (accessed: 07.05.2023).
 8. "61850 Test Suite Pro" [Electronic resource]. Access mode: <https://61850solutions.com/61850-test-suite-pro/> (accessed: 07.05.2023).
 9. "ASE 61850 Suite software package" [Electronic resource]. Access mode: <https://www.ase-systems.com/products/ase61850-suite/> (accessed: 08.05.2023).
 10. "Tekvel Park Software package" [Electronic resource]. Access mode: <https://tekvel.com/ru/park/#:~:text=> (accessed 08.05.2023).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004

РОЛЬ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ПОДСТАНЦИЙ В ЦИФРОВИЗАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ

Антонов Р.Б.,¹Сидоров В.А., Медведев М.С., Алиусманов Г.Э., Климчук И.В.
ФГБОУ ВО "Национальный исследовательский университет "МЭИ", Москва, Россия (111250,
г.Москва, Красноказарменная ул., 14), e-mail: ¹SidorovVaAl@yandex.ru

В данном исследовании рассмотрена кибербезопасность цифровых подстанций в парадигме цифровизации электроэнергетики: проанализирована актуальность киберзащиты ЦПС, рассмотрены требования, предъявляемые к кибербезопасности современных ЦПС.

Ключевые слова: Цифровая подстанция (ЦПС), МЭК 61850, кибербезопасность, киберугроза, кибератака.

THE ROLE OF CYBER SECURITY OF DIGITAL SUBSTATIONS IN THE DIGITALIZATION OF THE POWER INDUSTRY

Antonov R.B.,¹Sidorov V.A., Medvedev M.S., Aliusmanov G.E., Klimchuk I.V.
"National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya
st., 14), e-mail: ¹SidorovVaAl@yandex.ru

This study provides an overview of existing national and foreign software systems for the configuration and verification of electronic documentation in the SCL language developed in the design of digital substations.

Keywords: Digital substation (DS), IEC 61850, cybersecurity, cyber threat, cyber attack.

Развитие энергетической системы и ее «цифровизация» требуют создания высокотехнологичных современных объектов для ее управления — цифровых подстанций (ЦПС). Цифровые подстанции представляют собой сложную систему, совмещающую физическую (технологическую) и информационно-управляющую подсистемы. Физическая подсистема включает в себя первичное оборудование, управляемое аналоговыми сигналами, а информационно-управляющая подсистема — цифровые устройства, предназначенные для сбора, обработки и передачи информации в цифровом виде [1].

Постоянное усложнение информационно-управляющей подсистемы, использование на ЦПС сложных интеллектуальных устройств приводят к уязвимости ЦПС для киберугроз. В целях обеспечения надежной работы ЦПС необходима эффективная система информационной безопасности.

Цифровая трансформация электроэнергетики реализуется посредством формирования единой среды на базе национальных стандартов взаимодействия и универсального формата информационного обмена, разрабатываемых с учетом стандартов Международной электротехнической комиссии (МЭК) [2].

В стратегии развития единой энергетической системы (ЕЭС) следующим этапом является создание цифровых электрических сетей. Согласно стандарту ПАО "Россети", цифровые электрические сети представляют собой организационно-технические комплексы, объединяющие электросетевые объекты, которые оборудованы цифровыми системами для измерения параметров режима сети, контроля состояния оборудования и линий электропередачи, защиты и автоматического предотвращения аварий, а также системами управления сетью и объектами. Взаимный информационный обмен между этими компонентами осуществляется по единым протоколам, обеспечивая синхронизацию по времени [3]. Такие цифровые электрические сети обеспечивают тесное информационное взаимодействие между элементами сети, позволяя передавать данные посредством цифрового обмена. Технологическую связь цифровых электрических сетей и передачу по ним данных в данной концепции осуществляют цифровые подстанции. В контексте эволюции энергетической инфраструктуры, сейчас приоритетным направлением является создание ЦПС и повышение эффективности их работы.

Одной из главных задач создания цифровых подстанций является обеспечение технических условий для перехода к автономным подстанциям, где не требуется постоянное присутствие дежурного персонала, а управление осуществляется из диспетчерских центров или центра управления системой (ЦУС). Кроме того, важным аспектом является интеграция подстанций в цифровые электрические сети. Для выполнения поставленных задач цифровые подстанции должны обеспечивать надежное исполнение их основных технологических функций [4].

Согласно стратегическим направлениям государственной политики в области обеспечения безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), ЦПС являются критически важными объектами инфраструктуры Российской Федерации. Нарушение или прекращение их функционирования имеет серьезные последствия, включая потерю управления, разрушение инфраструктуры, необратимые отрицательные изменения или разрушение экономики страны, региона или административно-территориальной единицы, а также значительное ухудшение безопасности жизнедеятельности населения, проживающего на этих территориях, на продолжительное время [5].

Защита и конфиденциальность обмена информацией, как между устройствами, так и между пользователями системы, обеспечиваются системой информационной безопасности (ИБ) цифровых подстанций.

Для определения угроз информационной безопасности необходимо осуществлять оценку потенциала, оборудования и мотивации потенциальных нарушителей, а также изучать предполагаемые уязвимости в оборудовании и терминалах релейной защиты. Важно также анализировать возможные варианты атак на систему информационной безопасности и учитывать результаты нарушения признаков безопасности информации (таких как целостность, доступность и конфиденциальность). Это позволит эффективно управлять рисками и принимать соответствующие меры по обеспечению безопасности информационных систем.

Концепция развития релейной защиты и автоматики электросетевого комплекса от ПАО «Россети» идентифицирует следующие потенциальные и технически реализуемые угрозы информационной безопасности [6]:

- целенаправленное искажение команд управления и другой информации;
- навязывание ложных команд управления или ложной информации, специально созданных злоумышленником;
- несанкционированный доступ к устройствам, изменение конфигурации технических средств;
- перенаправление (изменение маршрутов) потоков данных для деструктивного воздействия;
- вызов сбоев в работе технических средств или создание неисправностей в них;
- умышленное или непреднамеренное уничтожение или изменение данных, системного и прикладного программного обеспечения системы и устройств релейной защиты и автоматики (РЗА);
- кража, разглашение информации, которая может быть использована для нарушения функционирования устройств релейной защиты.
- инфицирование программного обеспечения автоматизированного рабочего места (АРМ) оперативного персонала и АРМ РЗА компьютерными вирусами;
- сканирование сети технологической связи;
- отказ в обслуживании технических средств РЗА.

К непосредственным источникам угроз информационной безопасности можно отнести [6]:

- иностранные разведывательные службы государств, которые проводят враждебную политику в отношении нашей страны и стремятся нарушить функционирование энергетического комплекса в особый период или во время подготовки и ведения войны;
- террористические организации, криминальные структуры и отдельные лица, такие как хакеры, внутренние и другие нарушители, а также группы лиц, которые используют деструктивные информационные методы для реализации своих корыстных или иных интересов в системах оперативно-технологического управления;
- конкурирующие фирмы и организации.

Самым уязвимым к киберугрозам местом в современной электроэнергетике является оборудование на микропроцессорах, легко поддающееся перепрошивке.

Существуют несколько компонентов цифровой подстанции, которые с наибольшей вероятностью могут стать объектами кибератак и привести к нарушению ее функционирования [7]:

- коммуникационные сети энергообъекта, включая коммутаторы и маршрутизаторы, то есть шины процесса и станции в соответствии с МЭК 61850;
- цифровые устройства релейной защиты, противоаварийной автоматики и АСУ ТП;
- внешние цифровые каналы, которые обеспечивают технологическую и оперативную связь с другими энергообъектами и диспетчерскими пунктами.

Объектами защиты для вышеперечисленных компонентов ЦПС являются [8]:

- данные о параметрах и состоянии управляемого объекта или процесса. Такие данные включают в себя входную (выходную) информацию, управляющую (командную)

информацию, контрольно-измерительную информацию и другую критически важную (технологическую) информацию;

- программно-технический комплекс (ПТК), который включает в себя технические средства, такие как АРМы, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры и исполнительные устройства, а также программное обеспечение (ПО), включающее микропрограммное, общесистемное и прикладное программное обеспечение.

В случае, когда все терминалы РЗА будут объединены в единую локальную сеть, результатом кибератаки может стать полная потеря управления энергообъектом или же несанкционированное управление им. После возврата управления над объектом потребуются обширный ряд пусконаладочных работ продолжительностью до нескольких месяцев, поскольку в результате кибератаки возможны изменение конфигураций цифрового оборудования, нарушение работы ПО энергообъекта.

Пусть несколько соседних подстанций станут целью кибератаки. В таком случае, можно ожидать полного отключения электроснабжения для значительной части потребителей, включая критически важные объекты. Кроме того, следует учитывать возможные повреждения первичного оборудования, которое могло получить ущерб вследствие длительного неотключения короткого замыкания в период кибератаки. Важно отметить, что традиционные системы дальнего резервирования на смежных цифровых подстанциях также могут подвергнуться кибератаке.

Таким образом, важно сохранять некоторые управляющие функции на электромеханическом оборудовании, а не переводить их полностью в цифровые системы. Это позволит немедленно восстановить работу электроэнергетических объектов, несмотря на возможные атаки, которые могут повлиять на цифровые устройства. Совместное использование цифрового и электромеханического оборудования является эффективным методом обеспечения информационной безопасности.

Какие требования предъявляются к кибербезопасности современных ЦПС?

Система информационной безопасности ЦПС должна обеспечивать: целостность информации (отсутствие ее противоправного изменения), доступность информации (свободное использование информации при наличии права доступа), неотказуемость (гарантия невозможности отрицания факта выполнения действий пользователем), подотчетность (однозначная прослеживаемость совершенных действий), подлинность (обеспечение идентичности субъекта или ресурса требованиям), конфиденциальность информации [3].

Информационная безопасность должна обеспечиваться на следующих объектах ПТК ЦПС: АРМы, промышленные серверы, сетевое и телекоммуникационное оборудование, узел связи ЦПС и сеть технологической связи, каналы передачи данных, программируемые логические контроллеры, исполнительные устройства с микропрограммным обеспечением, программное обеспечение, средства защиты информации, оборудование видеонаблюдения.

При этом система обеспечения ИБ включает в себя следующий комплекс организационных и технических мер защиты: применение технических устройств на территории цифровой подстанции, использование аппаратно-программных устройств защиты информации, использование программных средств защиты информации, организационные

меры обеспечения защиты, обеспечивающие безопасные условия работы цифровых подстанций.

Данный комплекс мер должен включать в себя:

- идентификацию и аутентификацию;
- управление доступом;
- ограничение программной среды;
- защиту машинных носителей информации;
- аудит безопасности;
- антивирусную защиту;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защиту технических средств и систем;
- защиту автоматизированной системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Процесс "цифровизации" в энергетических системах, применение интеллектуальных технологий и сложного оборудования для обработки информации и коммуникаций, значительно увеличили риски в области кибербезопасности энергетических предприятий, включая цифровые подстанции. Кибератаки на информационно-коммуникационную подсистему ЦПС могут привести к потере и фальсификации информации, что может привести к неправильным управляющим воздействиям и развитию аварийных ситуаций, как на уровне цифровых подстанций, так и в энергосистеме в целом. Поэтому обеспечение киберустойчивости объектов энергетики является критически важной проблемой, которая требует технических и организационных решений, включая повышение квалификации оперативного персонала.

Список литературы

1. Колосок И.Н., Коркина Е.С. Анализ кибербезопасности цифровой подстанции с позиции киберфизической системы [Электронный ресурс]. Режим доступа: <https://cyberleninka.ru/article/n/analiz-kiberbezopasnosti-tsifrovoy-podstantsii-s-pozitsiy-kiberfizicheskoy-sistemy> (дата обращения: 16.06.2023).
2. «Системный оператор: создание Единой цифровой модели ЕЭС – основной итог унификации информационного обмена в электроэнергетике» [Электронный ресурс]. Режим доступа: <https://www.so-ups.ru/news/press-release/press-release-view/news/17771/> (дата обращения: 16.06.2023).
3. СТО ПАО «Россети» Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110- 220 кВ и узловых цифровых подстанций напряжением 35 кВ.

4. Чичёв С. И., Калинин В. Ф., Глинкин Е. И. Методология проектирования цифровой подстанции в формате новых технологий. Москва: Издательский дом «Спектр», 2014, 228 с.
5. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/ons_doc_LAW_150730/ (дата обращения: 18.06.2023).
6. «Приложение №1 к протоколу Правления ПАО «Россети». Концепция развития релейной защиты и автоматики электросетевого комплекса» [Электронный ресурс]. Режим доступа: <https://www.rosseti.ru/upload/iblock/1da/2igtje3suvjhgtr8ubv5v7jauxqinl.pdf> (дата обращения: 18.06.2023).
7. Осак А.Б., Бузина Е.Я. Влияние человеческого фактора при обеспечении кибербезопасности на надежность объектов электроэнергетики и живучесть электроэнергетических систем [Электронный ресурс]. Режим доступа: <https://cyberleninka.ru/article/n/vliyanie-chelovecheskogo-faktora-pri-obespechenii-kiberbezopasnosti-na-nadezhnost-obektov-elektroenergetiki-i-zhivuchest> (дата обращения: 19.06.2023).
8. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» ФСТЭК Приказ от 14 марта 2014 г. N31 [Электронный ресурс]. Режим доступа: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31> (дата обращения: 20.06.2023).

References

1. Kolosok I.N., Korkina E.S. Cybersecurity Analysis of a Digital Substation from the Position of a Cyber-Physical System [Electronic resource]. Access mode: <https://cyberleninka.ru/article/n/analiz-kiberbezopasnosti-tsifrovoy-podstantsii-s-pozitsiy-kiberfizicheskoy-sistemy> (date of access: 06/16/2023).
2. "System Operator: Creation of the Unified Digital Model of the UES - the main result of the unification of information exchange in the electric power industry" [Electronic resource]. Access mode: <https://www.so-ups.ru/news/press-release/press-release-view/news/17771/> (date of access: 06/16/2023).
3. STO PJSC "Rosseti" Digital supply center. Requirements for the technological design of digital substations with a voltage of 110-220 kV and nodal digital substations with a voltage of 35 kV.
4. Chichev S. I., Kalinin V. F., Glinkin E. I. Methodology for designing a digital substation in the format of new technologies. Moscow: Spektr Publishing House, 2014, 228 p.
5. "The main directions of state policy in the field of ensuring the safety of automated control systems for production and technological processes of critically important infrastructure facilities of the Russian Federation" [Electronic resource]. Access mode: https://www.consultant.ru/document/cons_doc_LAW_150730/ (date of access: 06/18/2023).

6. Appendix No. 1 to the minutes of the Management Board of PJSC Rosseti. The concept of development of relay protection and automation of the electric grid complex” [Electronic resource]. Access mode: <https://www.rosseti.ru/upload/iblock/1da/2igrtje3suvjhgtjr8ubv5v7jauxqinl.pdf> (date of access: 06/18/2023).
 7. Osak A.B., Buzina E.Ya. The influence of the human factor in ensuring cybersecurity on the reliability of electric power facilities and the survivability of electric power systems [Electronic resource]. Access mode: <https://cyberleninka.ru/article/n/vliyanie-chelovecheskogo-faktora-pri-obespechenii-kiberbezopasnosti-na-nadezhnost-obektov-elektroenergetiki-i-zhivuchest> (date of access: 06/19/2023).
 8. "On approval of the requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities that pose an increased danger to human life and health and to the environment" FSTEC Order dated March 14, 2014 N31 [Electronic resource] . Access mode: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31> (date of access: 06/20/2023).
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 536.24

ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ ВАКУУМНЫХ КОЛЛЕКТОРОВ ЗА СЧЁТ ИСПОЛЬЗОВАНИЯ ЕСТЕСТВЕННОЙ ЦИРКУЛЯЦИИ

Канарейкин А.И.

ФГБОУ ВО «Российский государственный геологоразведочный университет имени Серго Орджоникидзе (МГРИ)», Москва, Россия, (117485, г. Москва, ул. Миклухо-Маклая, 23), e-mail: kanareykins@mail.ru

Статья посвящена вопросам теплопередачи внутри горизонтальной теплообменной трубы. Предметом исследования является безразмерный коэффициент сопротивления при естественной циркуляции жидкости внутри горизонтальных труб теплообменника. В настоящее время многие жилые здания и предприятия используют солнечные системы водяного отопления. Это экономичный и надежный вид горячего водоснабжения. Нагрев воды для бытовых целей или отопление с использованием солнечной энергии - это естественный и простой метод экономии энергии и сохранения запасов ископаемого топлива. Использование возобновляемых источников энергии актуально для всех стран мира. В статье рассматривается вопрос повышения энергоэффективности системы солнечного теплоснабжения зданий на основе вакуумных коллекторов с естественной циркуляцией теплоносителя

Ключевые слова: Вакуумный коллектор, теплообмен, теплопроводность, естественная циркуляция, естественная конвекция, ламинарное течение.

INCREASING THE ENERGY EFFICIENCY OF VACUUM COLLECTORS THROUGH THE USE OF NATURAL CIRCULATION

Kanareykin A.I.

Sergo Ordzhonikidze Russian State University for Geological Prospecting, Moscow, Russia, (117485, Moscow, st. Miklukho-Maklaya 23), e-mail: kanareykins@mail.ru

The article is devoted to the issues of heat transfer inside a horizontal heat exchange pipe. The subject of the study is the dimensionless coefficient of resistance in the natural circulation of liquid inside the horizontal pipes of the heat exchanger. Currently, many residential buildings and businesses use solar water heating systems. This is an economical and reliable type of hot water supply. Heating water for domestic purposes or heating using solar energy is a natural and simple method of saving energy and preserving fossil fuel reserves. The use of renewable energy sources is relevant for all countries of the world. The article deals with the issue of increasing the energy efficiency of the solar heat supply system of buildings based on vacuum collectors with natural circulation of the coolant.

Keywords: Vacuum collector, heat exchange, thermal conductivity, natural circulation, natural convection, laminar flow.

На сегодня Солнце является самым мощным возобновляемым источником энергии для нашей планеты: количество энергии, падающей на поверхность земли от солнца в день, превышает мировое потребление в год. Солнечную энергию можно использовать как для выработки электроэнергии, так и для отопления и освещения жилых и производственных помещений, нагрева воды [1, 2]. Являясь экологически чистым возобновляемым источником энергии, который не выделяет углекислый газ и не зависит от ископаемых ресурсов, солнечная

энергия способствует диверсификации источников энергии, повышению энергоэффективности и экономии денег и ресурсов.

Существуют различные технологии преобразования и использования солнечной энергии. Солнечные системы теплоснабжения получили масштабное практическое применение для теплоснабжения жилых и общественных зданий [3, 4]. В мировой практике наиболее широко используются плоские и трубчатые вакуумированные солнечные коллекторы.

Несмотря на столь впечатляющий объем внедрения, многие вопросы проектирования и построения вакуумных коллекторов остаются нерешенными по сей день, поскольку действующие нормативные документы и руководства по их проектированию не содержат достаточной информации по их применению и расчету.

Целью работы является повышение эффективности солнечных коллекторов за счет использования естественной циркуляции.

Существуют солнечные коллекторы различных размеров и конструкций в зависимости от их применения. Они могут обеспечивать горячее водоснабжение либо использоваться для предварительного нагрева воды для существующих водонагревателей. Солнечный коллектор - устройство для сбора тепловой энергии Солнца, переносимой видимым светом и ближним инфракрасным излучением. В отличие от солнечных панелей, которые вырабатывают электроэнергию напрямую, солнечный коллектор нагревает охлаждающий материал.

Основным элементом коллектора является поглотитель, представляющий собой пластину из меди или алюминия, зачерненную с одной стороны по специальной технологии. На самом деле это почернение при просмотре "на глаз" может иметь голубоватый оттенок, но способность поглощать необходимый спектр солнечного излучения у такой поверхности во много раз выше, чем при покрытии пластины самой черной из всех возможных красок или пигментов. Кроме того, зачерненная поверхность обязательно должна быть матовой.

В вакуумированных системах с прямой передачей тепла воде вакуумные трубки подсоединены к накопительному баку (рис. 1). Из контура теплообменника вода поступает непосредственно в трубки, нагревается и возвращается обратно. Такие системы также называются термосифонными. К преимуществам этих систем можно отнести прямую передачу тепла воде без участия других элементов. Термосифонные системы работают по принципу естественной конвекции, когда теплая вода поднимается вверх. В термосифонных системах резервуар должен располагаться над коллектором. По мере того как вода в коллекторных трубках нагревается, она становится легче и естественным образом поднимается к верхней части резервуара. Более холодная вода из резервуара стекает вниз по трубам, обеспечивая таким образом циркуляцию по всей системе. Такая система обладает минимальным гидравлическим сопротивлением.

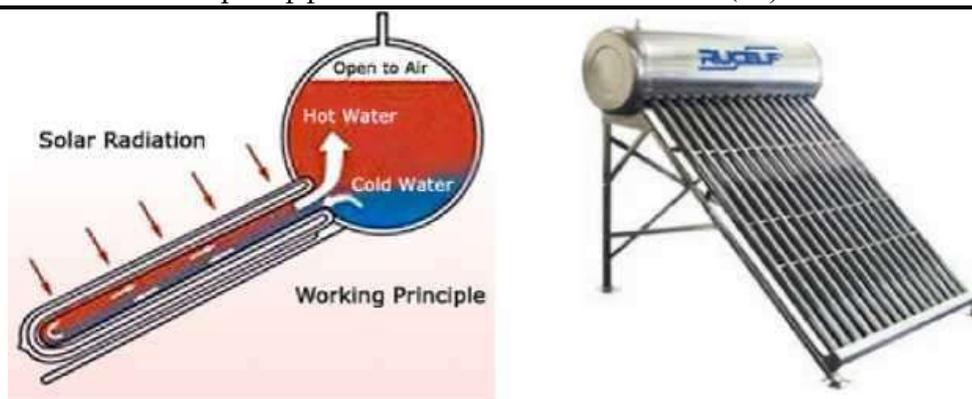


Рисунок 1 – Схема вакуумированного коллектора с прямой передачей тепла воде (а) и его внешний вид (б).

В литературных источниках приводится несколько путей повышения эффективности солнечных коллекторов. В данной работе для этой цели предлагается использовать естественную циркуляцию теплоносителя, которая возникает и развивается при наличии небольших градиентов статического давления, возникающей из-за разной плотности воды в окружающей среде и элементах теплообменника и циркуляционной системы.

Главным же условием свободно конвективного движения является неравномерность распределения плотностей, которая определяется неравномерностью температурного поля [5-11]. Если движение не является в чистом виде естественно-конвективным. В таких случаях говорят о так называемой естественной циркуляции. Её применение имеет ряд важных преимуществ: малый расход энергии на собственные нужды, отсутствие побудителя движения охлаждающей воды [12, 13].

Рассматривая природу происхождения движущей силы, следует отметить, что если ρ_{∞} - плотность холодной невозмущенной жидкости, а ρ - плотность более нагретой жидкости, то подъемная сила, действующая на единицу объема в гравитационном поле, равна $(\rho_{\infty} - \rho)g$, где g - ускорение свободного падения.

Естественная циркуляция воды возникает и развивается при наличии небольших градиентов статического давления, определяемых разницей в гидростатических давлениях, образующихся из-за различной плотности воды в окружающей среде и элементов теплообменника и системы циркуляции [14-19]. Разница в плотности может быть выражена в зависимости от теплового коэффициента объемного расширения жидкости β , который равен

$$\beta = \frac{\rho_{\infty} - \rho}{\rho(T - T_{\infty})} \quad (1)$$

Использование естественной циркуляции обеспечивает ряд важных преимуществ: отсутствие стимула для перемещения охлаждающей воды и, как следствие, отсутствие средств автоматизации, контроля и управления.

В зависимости от условий компоновки или из-за изменения пространственного положения объекта, на котором установлен теплообменник, последний часто может занимать наклонное положение. Это влияет на интенсивность теплообмена при естественной циркуляции воды, а также в случае вязко-гравитационного течения в условиях принудительной циркуляции. В горизонтальной трубе с вязко-гравитационным потоком теплообмен протекает более интенсивно, чем в вертикальной.

В то же время, когда трубы теплообменника наклонены, проекция высоты столба нагретой воды на вертикаль уменьшается, а, следовательно, и приводное давление естественной циркуляции. Результатом этого должно стать снижение скорости потока воды и интенсивности теплообмена, что скажется на энергоэффективности вакуумного коллектора.

Таким образом, в данной работе была рассмотрена возможности применения использования солнечных коллекторов для горячего водоснабжения. Это экономичный и надежный вид горячего водоснабжения. Использование солнечных коллекторов для горячего водоснабжения зданий является перспективной и экономически выгодной. Также было показано, что можно повысить эффективность солнечных коллекторов, используя естественную циркуляцию.

Список литературы

1. Лошкарева Е.А., Канарейкин А.И. Определение температурной зависимости коэффициента заполнения солнечного элемента // В сборнике: научные труды Калужского государственного университета имени К.Э. Циолковского. материалы докладов. Сер. "Естественные и технические науки. 2022" Калуга, 2022. С. 157-162.
2. Канарейкин А.И. О влиянии температурного фактора на эффективность солнечных панелей // Международный журнал информационных технологий и энергоэффективности, 2023. Т. 8. № 1 (27). С. 103-107.
3. Алмаев А. Ю. Лушкин И. А. Использование солнечной энергии для теплоснабжения систем горячего водоснабжения в индивидуальном жилищном строительстве // Вестник НГИЭИ, 2014. № 12 (43). С. 5–9.
4. Петросян А. Л. Использование солнечной энергии и тепловых насосов для теплоснабжения жилых зданий // Сб научн. трудов. Ереванского гос. университета архитектуры и строительства. II том, 2003. С. 122–124.
5. Петухов Б. С. Теплообмен и сопротивление при ламинарном течении жидкости в трубах, «Энергия», 1967. 412с.
6. Мартыненко О.Г., Соковишин Ю.А., «Свободно – конвективный теплообмен»: справочник. Минск: Наука и техника, 1982.
7. Соковишин Ю.А., Мартыненко О.Г., «Введение в теорию свободно – конвективно-го теплообмена». Л.: изд-во ЛГУ, 1982.
8. Петражицкий Г.Б., Ключников Ф.В., Бекнева Е.В. «Численные исследования свободно-конвективных циркуляционных течений и процессов переноса тепла в замкнутых полостях различной конфигурации». М.: Наука, 1975.
9. Берковский Б.М., Полевиков В.К. «Исследования теплообмена в условиях высокоинтенсивной свободной конвекции». В кн.: Теплообмен-1974. М.: Наука, 1975.
10. Петухов Б. С. и Поляков А. Ф. О влиянии свободной конвекции на теплоотдачу при вынужденном течении в горизонтальной трубе, «Теплофизика высоких температур», 1967, т. 5, № 2.
11. Li, Ji Difference Scheme for Hyperbolic Heat Conduction Equation with Pulsed Heating Boundary. Journal of Thermal Science, 20009. (2) pp.152 – 157.
12. Канарейкин А. И. Теплообмен при естественной циркуляции внутри труб теплообменника с вытяжной шахтой при ламинарном течении: дис. канд. техн. наук. Калуга, 2011. 113 с.

13. Канарейкин А. И. Теплообмен при естественной циркуляции внутри труб теплообменника с вытяжной шахтой при ламинарном течении: автореф. дис. канд. техн. наук. Екатеринбург, 2011. 20 с.
14. Мильман О.О., Канарейкин А. И. Исследование теплообмена в области ламинарного течения при естественной циркуляции внутри труб теплообменника с вытяжной шахтой // Вестник Калужского университета. 2008. № 3. С. 9-11.
15. Канарейкин А. И. Решение задачи теплообмена при естественной циркуляции внутри теплообменника с вытяжной шахтой в ламинарной области течения // Вестник Челябинского государственного педагогического университета. Челябинск, 2009. №11. С.328-333.
16. Канарейкин А. И. Определение коэффициента сопротивления внутри горизонтального теплообменника при естественной циркуляции // В сборнике: Научные труды Калужского государственного университета имени К.Э. Циолковского. Региональная университетская научно-практическая конференция. Сер. "Естественные науки" Калужский государственный университет имени К.Э. Циолковского. 2015. С. 200-202.
17. Канарейкин, А. И. Оценка влияния тангенциальной составляющей теплового потока на процесс теплообмена внутри труб при естественной циркуляции // Научный альманах Центрального Черноземья. 2022. № 3-1. С. 18-22.
18. Канарейкин, А. И. Определение сопротивления при естественной циркуляции внутри горизонтальной теплообменной трубы // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8 № 5(31) ч.1 С. 80–84.
19. Канарейкин, А. И. Сравнение процесса теплообмена при естественной конвекции и при естественной циркуляции в ламинарной области течения в круглой трубе при граничных условиях второго рода // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8 № 5(31) ч.1 С. 85–89.

References

1. Loshkareva E.A., Kanarekin A.I. Determination of the temperature dependence of the coefficient of filling of a solar cell // In the collection: Scientific works of Kaluga State University named after K.E. Tsiolkovsky. Materials of the reports. Ser. "Natural and technical sciences. 2022" Kaluga, 2022. pp. 157-162.
2. Kanareykin A.I. On the influence of the temperature factor on the efficiency of solar pan-els // International Journal of Information Technologies and Energy Efficiency, 2023. Vol. 8. No. 1 (27). pp. 103-107.
3. Almaev A. Yu. Lushkin I. A. The use of solar energy for heat supply of hot water supply systems in individual housing construction // Bulletin of NGIEI, 2014. No. 12 (43). pp. 5-9.
4. Petrosyan A. L. The use of solar energy and heat pumps for heat supply of residential buildings // Sb nauchn. works. Yerevan State University. University of Architecture and Construc-tion. Volume II, 2003. pp. 122-124.
5. Petukhov B. S. Heat exchange and resistance during laminar fluid flow in pipes, "Energy", 1967. 412с.
6. Martynenko O.G., Sokovishin Yu.A., "Free –convective heat exchange": reference. Minsk: Science and Technology, 1982.

7. Sokovishin Yu.A., Martynenko O.G., "Introduction to the theory of free-convective heat transfer". L.: LSU Publishing House, 1982.
 8. Petrazhitsky G.B., Klyushnikov F.V., Bekneva E.V. "Numerical studies of free-convective circulation flows and heat transfer processes in closed in areas of various configurations". Moscow: Nauka, 1975.
 9. Berkovsky B.M., Polevikov V.K. "Studies of heat transfer in conditions of high-intensity free convection". In: Heat exchange-1974. Moscow: Nauka, 1975.
 10. Petukhov B. S. and Polyakov A. F. On the effect of free convection on heat transfer during forced flow in a horizontal pipe, "High temperature Thermophysics", 1967, vol. 5, No. 2.
 11. Li, Ji Difference Scheme for Hyperbolic Heat Conduction Equation with Pulsed Heating Boundary. Journal of Thermal Science, 20009. (2) pp.152 – 157.
 12. Kanareykin A. I. Heat exchange during natural circulation inside heat exchanger tubes with exhaust shaft during laminar flow: dis. candidate of Technical Sciences. Kaluga, 2011. 113 p.
 13. Kanarekin A. I. Heat exchange during natural circulation inside the heat exchanger tubes with an exhaust shaft during laminar flow: abstract of the dissertation of the Candidate of Technical Sciences. Yekaterinburg, 2011. 20 p.
 14. Milman O.O., Kanarekin A. I. Investigation of heat exchange in the field of laminar flow with natural circulation inside the pipes of a heat exchanger with an exhaust shaft // Bulletin of Kaluga University. 2008. No. 3. pp. 9-11.
 15. Kanareykin A. I. Solving the problem of heat exchange with natural circulation inside a heat exchanger with an exhaust shaft in the laminar flow region // Bulletin of the Chelyabinsk State Pedagogical University. Chelyabinsk, 2009. No. 11. pp. 328-333.
 16. Kanarekin A. I. Determination of the coefficient of resistance inside a horizontal heat exchanger with natural circulation // In the collection: Scientific works of K.E. Tsiolkovsky Kaluga State University. Regional University scientific and practical conference. Ser. "Natural Sciences" Kaluga State University named after K.E. Tsiolkovsky. 2015. pp. 200-202.
 17. Kanarekin, A. I. Assessment of the influence of the tangential component of the thermal current on the heat exchange process inside pipes during natural circulation // Scientific Alma-na of the Central Chernozem region. 2022. No. 3-1. pp. 18-22.
 18. Kanarekin, A. I. Determination of resistance during natural circulation inside a horizontal heat exchange pipe // International Journal of Information Technologies and Energy Efficiency. 2023. Vol. 8 No. 5(31) part 1 pp. 80-84.
 19. Kanarekin, A. I. Comparison of the heat exchange process with natural convection and with natural circulation in the laminar flow region in a round tube under boundary conditions of the second kind // International Journal of Information Technologies and Energy Efficiency. 2023. Vol. 8 No. 5(31) part 1 pp. 85-89.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 658.26

ЭЛЕКТРОПИТАНИЕ ОБЪЕКТОВ ГАЗОВОЙ ПРОМЫШЛЕННОСТИ ПРИ ЗНАЧИТЕЛЬНОМ УДАЛЕНИИ ОТ ЛИНИЙ ЭЛЕКТРОПЕРЕДАЧ

Кузьмин В.В., ¹Гараев Р.Р.

ФГБОУ ВО «Казанский национальный исследовательский технологический университет», г.
Казань, Россия, (420015, г. Казань, ул. Карла Маркса, 68.), e-mail: ¹garaev.ramis99@yandex.ru

В данной статье будет рассмотрен способ электропитания объектов газовой промышленности при помощи автономного пункта электропитания на базе двигателя Стирлинга. Также будут расписаны технологические режимы работы и типовая конструкция двигателя

Ключевые слова: Электропитание; автономный пункт; двигатель Стирлинга; генератор.

POWER SUPPLY OF GAS INDUSTRY FACILITIES AT A CONSIDERABLE DISTANCE FROM POWER LINES

Kuzmin V.V., ¹Garaev R.R..

"Kazan National Research Technological University", Kazan, Russia, (420015, Kazan, Karl Marx
str., 68.), e-mail: ¹garaev.ramis99@yandex.ru

This article will consider a method for powering gas industry facilities using an autonomous power supply point based on a Stirling engine. Technological modes of operation and a typical engine design will also be described.

Keywords: Power supply; standalone item; Stirling's engine; generator.

Объекты газовой промышленности с каждым годом становятся все больше, так как увеличивается протяжённость магистральных газопроводов. А именно, строятся новые и расширяются уже существующие сети магистральных газопроводов. Это связано с освоением новых месторождений в районах Крайнего Севера, Сибири и Дальнего Востока. С увеличиваем сетей магистральных трубопроводов транспортировки природного газа увеличивается и потребности в облаживающей инфраструктуре. Таких как, запорно-регулирующих пунктах, пунктах телемеханики, станциях управления и связи и т.д. Как правило такие районы труднодоступны, малонаселены, с суровым климатом, и традиционный подход электроснабжения путем подключения к сети линий электропередачи (ЛЭП) требует значительных капитальных затрат.

Одним из альтернативных путей снижения капиталовложения является применение автономных пунктов электроснабжения с надежной транспортной сетью подачи топлива для него, которым выступает сам магистральный газ.

Для применяя в районах вечной мерзлоты с температурой воздуха от минус 55 С до плюс 35 С зимой и летом соответственно, автономные пункты электроснабжения должны

обеспечить бесперебойную работу системы телемеханики и связи за счёт гарантированного электропитания управляющей аппаратуры.

Зачастую, пункты автономного электропитания проектируются для работы без непосредственного присутствия эксплуатирующего персонала, а лишь с удаленным мониторингом с дистанционных пунктов управления. Из-за этого одним из главных функций системы автоматизированного управления (САУ) автономных пунктов электропитания является самодиагностика и перезапуск в автономном режиме без вмешательства человека.

Электронная аппаратура источников электропитания размещаются в блок-боксах. Данной укрытие кроме размещения оборудования применяется так же для временного пребывания обслуживающего персонала и для поддержания оптимального микроклимата для работы оборудования и людей в суровом климате.

Один из вариантов общего вида блок-бокса приведена на рисунке 1.

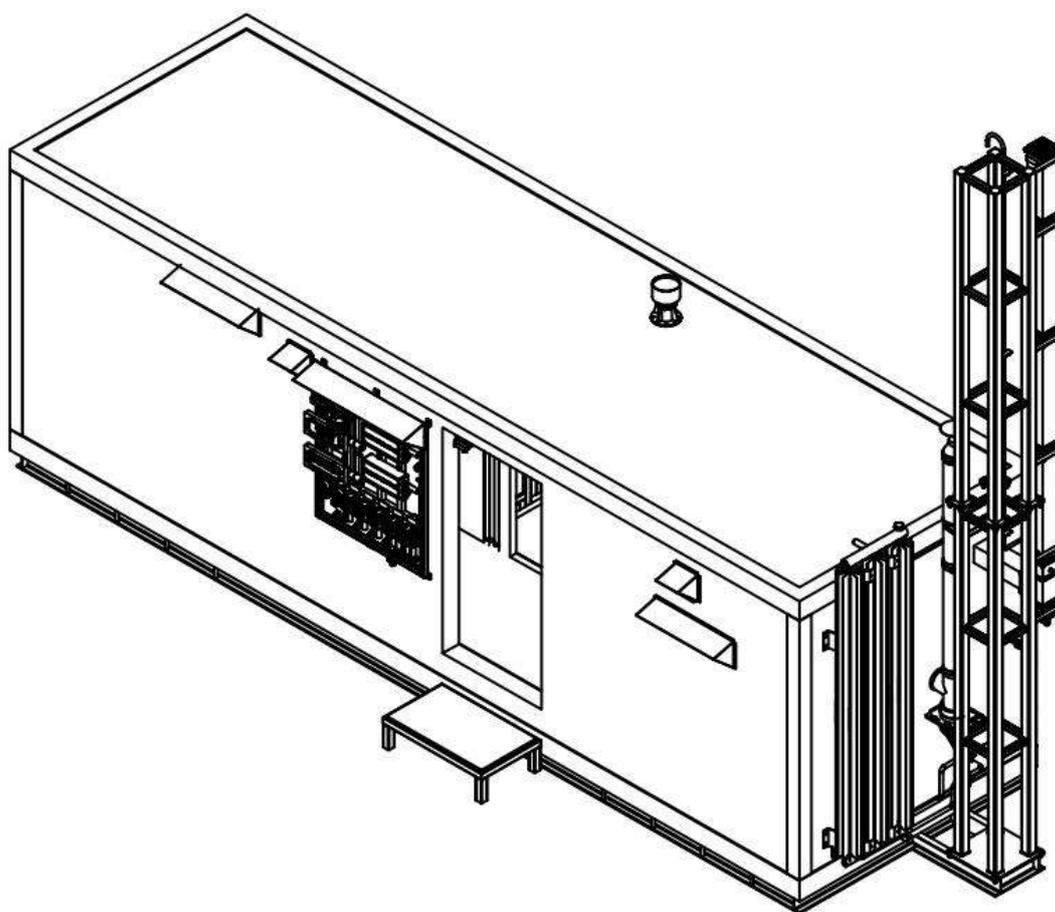


Рисунок 1 – Общий вид блок-бокса автономного пункта электропитания

Блок-бкс автономного пункта электропитания выполнен на рамной конструкции, в пределах которой выполнена сборка всего оборудования, разводка электрической проводки, проложенной в лотках. Установка и обвязка оборудования и приборов в отсеках выполнена с учетом инструкций по установке и эксплуатации производителей.

Конструкция блоков автономного пункта электропитания предусматривает их подъем, передвижение, транспортировку, обеспечивает необходимую прочность и отсутствие повреждений при погрузке, транспортировке, разгрузке и монтаже.

Основным элементом многих автономных пунктов электропитания является газовый генератор, преобразующий тепловую энергию горения газа в электричество. Одним из перспективным представителем газовых генераторов является двигатель Стирлинга. Конструкция двигателя приведена на рисунке ниже:



Рисунок 2 – Устройство двигателя Стирлинга

Двигатель Стирлинга представляет собой термодинамическую систему с внешней подачей тепловой энергии, которая преобразуется в механическую энергию возвратно-поступательного движения поршня. Двигатель имеет две основные движущиеся части: вытеснитель и рабочий поршень, находящийся в замкнутой среде гелия. Благодаря двум температурным зонам, а именно зоне нагрева и зоне охлаждения, гелий перемещается из области высокого давления в область низкого давления генерируя механическую энергию. Цикличность движения рабочего поршня обеспечивается за счет соосно расположенного поршня вытеснителя [1].

Механической энергии движения рабочего поршня превращается в электрическую энергию при помощи однофазного синхронного линейного генератора, индуктор которого присоединен к рабочему поршню. Генератор создает синусоидальное напряжение пропорциональное амплитуде колебания поршня, а частота определяется скоростью движения поршня.

Для поддержания работы двигателя нужно подавать природный газ в горелку с давлением в диапазоне от 1,8...3 кПа. Перед первым пуском отсек, где находится двигатель, должен иметь температуру окружающего воздуха выше 6 °С и поддерживаться в диапазоне до

плюс 30 °С. Чтобы минимизировать возможность конденсатаобразования на линии подача газа в газовый генератор, нужно нагреть газ перед первым пуском двигателя Стирлинга при помощи электрообогревателя до значений плюс 55...60 °С.

Также перед пуском двигателя производится подогрев охлаждающей жидкости. В ходе эксплуатации температура охлаждающей жидкости может быть в диапазоне от плюс 25 до 105 °С. Оптимальным является поддержание температуры на входе в двигатель в районе плюс 55 °С [2]. Для поддержания температуры охлаждающей жидкости в заданном диапазоне излишки тепла используются для нагрева помещений блок-бокса в зимнее время, и внешний теплообменник в летнее время.

Список литературы

1. Источники автономного энергообеспечения [Электронный ресурс]. Режим доступа URL: <https://evogress.com/>
2. Официальный сайт компании Наука Энерготех [Электронный ресурс]. Режим доступа URL: <https://npo-nauka.ru>

References

1. Sources of autonomous power supply [Electronic resource]. URL access mode: <https://evogress.com/>
 2. The official website of the company Nauka Energotech [Electronic resource]. URL access mode: <https://npo-nauka.ru>
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 620.92

НАКОПЛЕНИЕ СОЛНЕЧНОЙ ЭНЕРГИИ В ИОНИСТОРЕ

Канарейкин А.И.

ФГБОУ ВО «Российский государственный геологоразведочный университет имени Серго Орджоникидзе (МГРИ)», Москва, Россия, (МГРИ), г. Москва, Российская Федерация, (117485, г. Москва, ул. Миклухо-Маклая, 23), e-mail: kanareykins@mail.ru

Работа относится к вопросам солнечной энергетики. Объектом исследования является ионистор. В статье предлагается как вариант в качестве накопителя солнечной энергии использовать ионистор. В отличие от аккумулятора, ионистор наиболее эффективно заряжается не постоянным напряжением, а током, причем максимальным, т.е. всем, который только в состоянии отдать источник. Для источника энергии разряженный ионистор представляет собой короткозамкнутую нагрузку. Что приводит к некоторым трудностям его заряда. Так как солнечные элементы могут работать на нулевое сопротивление, то они способны заряжать ионистор с нуля. Проведен анализ проблемы применения данного метода. В статье приведены схемы подключения, а также формулы для расчёта зарядных характеристик.

Ключевые слова: Солнечная энергия, солнечный модуль, ионистор, ток заряда, суперконденсатор, схема включения, шунт.

ACCUMULATION OF SOLAR ENERGY IN AN IONISTOR

Kanareykin A.I.

Sergo Ordzhonikidze Russian State University for Geological Prospecting, Moscow, Russia, (117485, Moscow, st. Miklukho-Maklaya 23), e-mail: kanareykins@mail.ru

The work relates to the issues of solar energy. The object of the study is an ionistor. The article suggests using an ionistor as an option as a solar energy storage device. Unlike a battery, the ionistor is most efficiently charged not with a constant voltage, but with a current, and with maximum, i.e. with every-thing that is only able to give the source. For an energy source, a discharged ionistor is a short-circuited load. Which leads to some difficulties in charging it. Since solar cells can operate at zero resistance, they are able to charge the ionistor with a nula. The analysis of the problem of using this method is carried out. The article provides connection diagrams, as well as formulas for calculating charging characteristics

Keywords: Solar energy, solar module, ionistor, charge current, supercapacitor, switching circuit, shunt.

Сегодня применение солнечных панелей приобретает широкое применение. Увеличение спроса на электроэнергию приводит к быстрому истощению традиционных ископаемых видов топлива и обостряет проблему загрязнения окружающей среды. Поэтому существует необходимость в развитии альтернативных (возобновляемых) источников энергии для обеспечения устойчивых энергопоставок потребителю, а также для уменьшения локальных и глобальных загрязнений окружающей среды [1-3]. В литературных источниках существует много работ посвящённых оптимизации и увеличению эффективности фотоэлектрических преобразователей [4-8].

В таких системах в качестве накопителей выработанной солнечной энергии выступают аккумуляторы. В статье предлагается вместо АКБ использовать ионистор [9].

Ионисторы (суперконденсаторы) – это электрохимические накопители энергии. Функционально ионистор представляет собой гибрид конденсатора и химического источника тока [10-13]. По характеристикам ионистор занимает промежуточное положение между конденсатором и химическим источником тока. Сравнивая ионистор с батареями или аккумуляторами, стоит сказать, что ионисторы имеют низкую плотность заряда и худшие характеристики саморазряда, но все же с точки зрения времени зарядки, срока годности и цикла зарядки они превосходят батареи. В зависимости от наличия тока зарядки, ионисторы могут заряжаться менее чем за минуту, а при правильном обращении они могут работать более десяти лет.

В отличие от аккумуляторов, ионисторы обладают следующими преимуществами:

- имеют практически неограниченное количество циклов,
- могут быть разряжены до нуля, не боятся разряда,
- могут работать при отрицательных температурах,
- могут отдавать очень большие токи, в десятки или даже сотни ампер,
- имеют основной компонент — активированный уголь, который является весьма экологически чистым и «возобновляемым» компонентом.

Ионисторы с большими токами разряда применяются в экспериментальных автобусах с электроприводом (заряд на каждой второй остановке) и электромобилях, а также для сглаживания пиковых нагрузок в автономных электрогенераторах возобновляемых источников энергии. Благодаря уникальным свойствам ионисторы находят применение в различных устройствах. Ёмкость ионисторов может составлять несколько Фарад, а плотность запасенной энергии исчисляется Ваттами на килограмм. На основании статистических и экспериментальных данных ионисторы данного типа имеют наработку на отказ, равную 15000 циклов, при сроке службы не менее 12 лет [14-18].

В связи с этим возникает вопрос о технической возможности запаса солнечной энергии ионистором и дальнейшем использовании запасенной энергии.

Для источника энергии разряженный ионистор представляет собой короткозамкнутую нагрузку. Как следует из вольт-амперной характеристики солнечного модуля существует так называемый ток короткого замыкания (I_{sc}) (рис. 1). Данная характеристика показывает, как меняется ток, который проходит по цепи от напряжения, которое к ней прилагают. Поэтому фотогальванические элементы могут работать на нулевое сопротивление, а значит, способны заряжать ионистор с нуля.

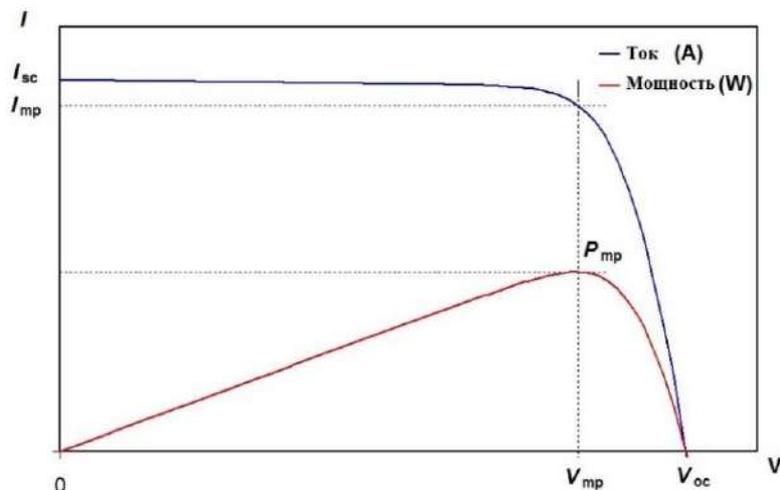


Рисунок 1 – Внешняя характеристика солнечной панели.

В начальный момент напряжение на ионисторе равно 0 В, вследствие чего солнечная батарея замкнута. По мере заряда ионистора ток уменьшается в соответствии с вольт-амперной характеристикой фотогальванического элемента. Если напряжение холостого хода источника энергии превышает рабочее напряжение ионистора, то для его защиты потребуется шунтовый регулятор напряжения. На рисунке 2 показана одна из возможных схем подключения ионистора к солнечной панели.

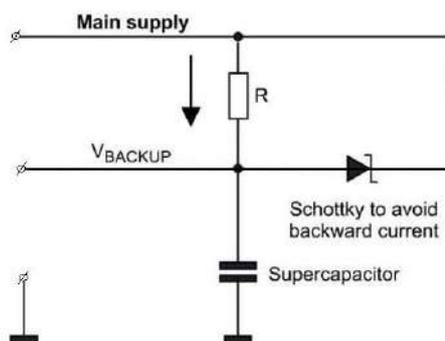


Рисунок 2 – Схема включения ионистора.

Диод Шоттки, который обладает малым падением напряжения при прямом пропускании тока, предохраняет ионистор от разряда через солнечную батарею в темное время суток. В качестве шунта выступает резистор. В таком случае зарядный ток будет равен

$$I = \frac{U}{R} \quad (1)$$

Время заряда τ равно

$$\tau = RC \quad (2)$$

За время t суперконденсатор емкостью C , подключенный последовательно с резистором R , зарядится примерно до $2/3$ (точнее до 63,2%) напряжения питания. За время $5t$ суперконденсатор зарядится до значения очень близкое к напряжению питания (99,3%). Эти

интервалы обусловлены тем, что процесс зарядки конденсатора является не линейной функцией (экспоненциальной). Для определения мгновенного зарядного тока I и мгновенного напряжения U можно использовать следующие формулы:

$$U = U_0 \left(1 - e^{-\frac{t}{RC}} \right) \quad (3)$$

$$I = \frac{U_0}{R} e^{-\frac{t}{RC}} \quad (4)$$

где: U_0 – напряжение заряда.

Ионисторы, представленные на рынке сегодня, обычно рассчитаны на малое напряжения порядка 2,5 В, 2,7 В или 5,5 В. Подобно литиевому элементу, эти конденсаторы должны быть соединены последовательно или параллельно для образования высоковольтных аккумуляторных батарей. Чтобы эффективно запастись необходимой для батарей энергией, необходимо ограничить напряжение заряда ионистора до уровня несколько меньшего, чем его допустимое напряжение. С учетом этого примем необходимое количество ионисторов равно

$$N = \frac{U_0}{U_u} \quad (5)$$

При использовании суперконденсаторов в качестве элементов накопления энергии для питания электронных устройств важно определить энергию, запасенную в ионисторе, чтобы предсказать, как долго устройство может быть запитано. Запасенная энергия равна

$$W = \frac{1}{2} C U_0^2 \quad (6)$$

Теперь, используя это значение, можно вычислить, как долго ионистор может питать устройства мощностью P

$$t = \frac{W}{P} \quad (7)$$

Таким образом, работа была посвящена вопросам запаса солнечной энергии. В качестве аккумулирующего устройства выступает ионистор. Благодаря своим уникальным свойствам ионисторы находят применение в различных устройствах. В работе приведены расчёты необходимых параметров для заряда ионистора от солнечных панелей.

Список литературы

1. Канарейкин А.И. Моделирование кривой мощности солнечного модуля // Электрооборудование: эксплуатация и ремонт, 2021. № 10. С. 31-34.
2. Канарейкин А.И. Моделирование значения шунтирующего сопротивления солнечного элемента на основе световой вольт-амперной характеристики // Наукосфера, 2022. № 3-2. С. 226-230.
3. Удалов Н. С. Возобновляемые источники энергии. Новосибирск: Изд-во НГТУ, 2009. 412 с.
4. Малинин Г.В., Серебрянников А.В. Слежение за точкой максимальной мощности солнечной батареи // Вестник Чувашского университета, 2016. № 3. С. 76–93.

5. Kanareykin A.I. On the correctness of calculating the Fill Factor of the solar module IOP Conf. Series: Earth and Environmental Science 808 (2021) 012018 <https://iopscience.iop.org/article/10.1088/1755-1315/808/1/012018>.
6. Kanareykin A.I. Determination of the shunt resistance of a solar cell from its light volt-ampere characteristic Improving Energy Efficiency, Environmental Safety and Sustainable Development in Agriculture. International Scientific and Practical Conference. IOP Publishing Ltd, Lon-don, 2022. С. 012185. DOI: 10.1088/1755-1315/979/1/012185.
7. Лошкарева Е.А., Канарейкин А.И. Определение температурной зависимости коэффициента заполнения солнечного элемента // В сборнике: Научные труды Калужского государ-ственного университета имени К.Э. Циолковского. материалы докладов. Сер. "Естествен-ные и технические науки. 2022" Калуга, 2022. С. 157-162.
8. Канарейкин А.И. О влиянии температурного фактора на эффективность солнечных панелей // Международный журнал информационных технологий и энергоэффективности, 2023. Т. 8. № 1 (27). С. 103-107.
9. Канарейкин А.И. Осуществление процесса заряда ионистора от солнечной панели // Электрооборудование: эксплуатация и ремонт, 2023. № 6. С. 16-20.
10. Панкрашин А. Ионисторы Panasonic: физика, принцип работы, параметры / А. Панкрашин // Компоненты и технологии, 2006. № 9(62). С. 12–17.
11. Абакумова Ю.П. Химические источники тока. СПб: СПбГУПС, 2004. 26 с.
12. Кашкаров А. Ионистор в автономной электрической цепи // Современная электро-ника, 2014. № 1.
13. Кузнецов В., Панькина О., Мачковская Н. Конденсаторы с двойным электрическим слоем (ионисторы): разработка и производство // Компоненты и технологии, 2005. № 50. С. 12–16.
14. Шурыгина В. Суперконденсаторы помощники или возможные конкуренты батарейным источникам питания/Электроника: Наука, Технология, Бизнес, 2003. №3.
15. Conway, B.E. Electrochemical Supercapacitors: Scientific Fundamentals and Technological Ap-plications / B.E. Conway. Springer, 1999. 698 p.
16. Electrolytes for Electrochemical Supercapacitors / C. Zhong, Y. Deng, W. Hu et al. CRC Press, 2016. 361 p.
17. Frackowiak, E. Carbon Materials for the Electrochemical Storage of Energy in Capacitors / E. Frackowiak, F. Béguin // Carbon, 2001. Vol. 39, Iss. 6. P. 937–950.
18. Zhong C., Deng Y., Hu W., Sun D., Han X., Qiao J., Zhang J. Electrolytes for Electrochem-ical Supercapacitors. CRC Press, 2016, 361 p. DOI: 10.1201/b21497.

References

1. Kanareykin A.I. Modeling of the power curve of the solar module // Electrical equipment: opera-tion and repair, 2021. No. 10. pp. 31-34.
2. Kanareykin A.I. Modeling of the value of the shunting resistance of a solar cell based on the light volt-ampere characteristic // Naukosphere, 2022. No. 3-2. pp. 226-230.
3. Udalov N. S. Renewable energy sources. Novosibirsk: NSTU Publishing House, 2009. 412 p.
4. Malinin G.V., Serebryannikov A.V. Tracking the point of maximum solar battery power // Bulletin of the Chuvash University, 2016. No. 3. pp. 76-93.

5. Kanareykin A.I. On the correctness of calculating the Fill Factor of the solar module IOP Conf. Series: Earth and Environmental Science 808 (2021) 012018 <https://iopscience.iop.org/article/10.1088/1755-1315/808/1/012018>.
 6. Kanareykin A.I. Determination of the shunt resistance of a solar cell from its light volt-ampere characteristic Improving Energy Efficiency, Environmental Safety and Sustainable Development in Agriculture. International Scientific and Practical Conference. IOP Publishing Ltd, Lon-don, 2022. С. 012185. DOI: 10.1088/1755-1315/979/1/012185.
 7. Loshkareva E.A., Kanarekin A.I. Determination of the temperature dependence of the solar cell filling coefficient // In the collection: Scientific works of Kaluga State University named after K.E. Tsiolkovsky. materials of the reports. Ser. "Natural and technical sciences. 2022" Kaluga, 2022. pp. 157-162.
 8. Kanareykin A.I. On the influence of the temperature factor on the efficiency of solar panels // International Journal of Information Technologies and Energy Efficiency, 2023. Vol. 8. No. 1 (27). pp. 103-107.
 9. Kanareykin A.I. Implementation of the ionistor charging process from the solar panel // Electrical equipment: operation and repair, 2023. No. 5. pp. 31-34.
 10. Pankrashin A. Panasonic ionistors: physics, principle of operation, parameters / A. Pankrashin // Components and Technologies, 2006. No. 9(62). pp. 12-17.
 11. Abakumova Yu.P. Chemical current sources. St. Petersburg: SPbGUPS, 2004. 26 p.
 12. Kashkarov A. Ionistor in an autonomous electrical circuit // Modern Electronics, 2014. No. 1.
 13. Kuznetsov V., Pankina O., Machkovskaya N. Capacitors with a double electric layer (ionistors): development and production // Components and technologies, 2005. No. 50. pp. 12-16.
 14. Shurygina V. Supercapacitors assistants or possible competitors to battery power sources/Electronics: Science, Technology, Business, 2003. No. 3.
 15. Conway, B.E. Electrochemical Supercapacitors: Scientific Fundamentals and Technological Applications / B.E. Conway. Springer, 1999. 698 p.
 16. Electrolytes for Electrochemical Supercapacitors / C. Zhong, Y. Deng, W. Hu et al. CRC Press, 2016. 361 p.
 17. Frackowiak, E. Carbon Materials for the Electrochemical Storage of Energy in Capacitors / E. Frackowiak, F. Béguin // Carbon, 2001. Vol. 39, Iss. 6. P. 937–950.
 18. Zhong C., Deng Y., Hu W., Sun D., Han X., Qiao J., Zhang J. Electrolytes for Electrochemical Supercapacitors. CRC Press, 2016, 361 p. DOI: 10.1201/b21497.
-